

STANDARDS

AMERICAN NATIONAL STANDARD

ANSI/BICSI 002-2011

Data Center Design and
Implementation Best Practices



ANSI/BICSI 002-2011

Data Center Design and Implementation Best Practices

Committee Approval: January 2011
First Published: March 2011



BICSI Standards

BICSI standards contain information deemed to be of technical value to the industry and are published at the request of the originating committee. The BICSI International Standards Program has subjected this standard to a rigorous public review and resolution of comments, which is a procedural part of the development of a BICSI standard.

BICSI reviews standards within five years of its last approval date. As necessary, standards are reaffirmed, rescinded, or revised according to submitted updates and assessment of need.

Suggestions for revision should be directed to the BICSI International Standards Program, care of BICSI.

Copyright

This BICSI document is a standard and is copyright protected. Except as permitted under the applicable laws of the user's country, neither this BICSI standard nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission from BICSI being secured.

Requests for permission to reproduce this document should be addressed to BICSI.

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Published by:

BICSI
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA

All rights reserved
Printed in U.S.A.

Notice Of Disclaimer And Limitation Of Liability

BICSI standards and publications are designed to serve the public interest by offering information technology systems (ITS) design guidelines. Existence of such standards and publications shall not in any respect preclude any member or nonmember of BICSI from manufacturing or selling products not conforming to such standards and publications, nor shall the existence of such standards and publications preclude their voluntary use by those other than BICSI members, whether the standard is to be used either domestically or internationally.

By publication of this standard, BICSI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any item mentioned in this standard. Additionally, BICSI does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standard or publication. Users of this standard are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard does not purport to address all safety issues or applicable regulatory requirements associated with its use. It is the responsibility of the user of this standard to review any existing codes and other regulations recognized by the national, regional, local and/or other recognized AHJ in conjunction with the use of this standard. Where differences occur, those items listed within the codes or regulations of the AHJ supersede any requirement or recommendation of this standard.

All warranties, express or implied, are disclaimed, including without limitation, any and all warranties concerning the accuracy of the contents, its fitness or appropriateness for a particular purpose or use, its merchantability and its non-infringement of any third party's intellectual property rights. BICSI expressly disclaims any and all responsibilities for the accuracy of the contents and makes no representations or warranties regarding the content's compliance with any applicable statute, rule or regulation.

BICSI shall not be liable for any and all damages, direct or indirect, arising from or relating to any use of the contents contained herein, including without limitation any and all indirect, special, incidental or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based upon breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. The foregoing negation of damages is a fundamental element of the use of the contents hereof, and these contents would not be published by BICSI without such limitations.

TABLE OF CONTENTS

1 INTRODUCTION.....	1
1.1 GENERAL.....	1
1.2 PURPOSE.....	1
1.2.1 Users within information technology (IT)	1
1.2.2 Users within facilities group	1
1.2.3 Staff outside information technology (IT) and facilities groups	2
1.3 CATEGORIES OF CRITERIA	2
2 SCOPE.....	2
3 REFERENCES.....	2
4 DEFINITIONS, ACRONYMS, ABBREVIATIONS, AND UNITS OF MEASUREMENT	5
4.1 DEFINITIONS	5
4.2 ACRONYMS AND ABBREVIATIONS.....	17
4.3 UNITS OF MEASUREMENT	19
5 SPACE PLANNING	21
5.1 OVERALL FACILITY CAPACITY.....	21
5.2 POWER SYSTEMS.....	21
5.2.1 Introduction	21
5.2.2 Electric utility service feeds.....	22
5.2.3 Generator power	22
5.2.4 Power distribution.....	23
5.3 COOLING CAPACITY.....	25
5.3.1 Introduction	25
5.3.2 Recommendations	25
5.4 DATA CENTER SUPPORTING SPACES.....	25
5.4.1 Adjacencies of functional spaces	25
5.4.2 Security	26
5.4.3 Telecommunications entrance room.....	26
5.4.4 Operations center	27
5.4.5 Helpdesk	27
5.4.6 Print	27
5.4.7 Loading dock	27
5.4.8 Storage.....	28
5.4.9 Engineering offices.....	28
5.4.10 Administrative	28
5.4.11 Waste/recycle.....	29
5.5 NON-IT EQUIPMENT ON ACCESS FLOOR.....	29
5.5.1 Cooling	29
5.5.2 Power distribution.....	29
5.5.3 Fire protection systems	30
5.6 INFORMATION TECHNOLOGY EQUIPMENT PLACEMENT IN A COMPUTER ROOM WITH AN ACCESS FLOOR	30
5.6.1 Telecommunications spaces	30
5.6.2 Racks, frames, and equipment	30
5.6.3 Aisles	32
5.6.4 Power and telecommunications cable distribution.....	34
5.6.5 Airflow circulation and equipment placement coordination.....	35
5.6.6 Information technology (IT) equipment adjacencies	35
5.6.7 Access floor grid layout and reference point	35
5.7 NETWORK ARCHITECTURE.....	36

6 SITE SELECTION.....	37
6.1 INTRODUCTION	37
6.2 NATURAL ENVIRONMENT	37
6.2.1 Seismic activity.....	37
6.2.2 Subsurface stability.....	39
6.2.3 Groundwater.....	39
6.2.4 Wind.....	41
6.2.5 Flood plain/wet lands.....	43
6.2.6 Topographical.....	43
6.2.7 Air quality.....	43
6.2.8 Altitude.....	44
6.2.9 Noise.....	44
6.3 UTILITY ENVIRONMENT.....	44
6.3.1 Power.....	44
6.3.2 Communications.....	47
6.3.3 Water.....	49
6.3.4 Sanitary sewer.....	49
6.3.5 Natural gas.....	50
6.3.6 Other fuel (utility natural gas unavailable).....	50
6.4 TRANSPORTATION	51
6.4.1 Public road access.....	51
6.4.2 Air traffic.....	51
6.4.3 Railways.....	51
6.4.4 Marine.....	51
6.5 REGULATIONS (LOCAL, REGIONAL, FEDERAL)	52
6.5.1 Air quality.....	52
6.5.2 Noise.....	52
6.5.3 Communication towers.....	52
6.5.4 Water tanks/cooling towers.....	52
6.5.5 Fuel tanks.....	52
6.5.6 Generator exhaust.....	52
6.5.7 Generator hours of operation.....	52
6.5.8 Required parking.....	52
6.5.9 Truck traffic.....	52
6.5.10 Setbacks.....	52
6.5.11 Height restrictions.....	52
6.5.12 Environmental assessment.....	53
6.5.13 Sight lines.....	53
6.6 LOCATION ENVIRONMENT	53
6.6.1 Adjacent properties.....	53
6.6.2 Security.....	54
6.6.3 Underground train or public transportation stations.....	54
6.7 COST EVALUATION	55
7 ARCHITECTURAL	57
7.1 FACILITIES PLANNING	57
7.1.1 General overview.....	57
7.1.2 Site selection.....	57
7.1.3 Location within a building.....	58
7.2 GENERAL DESIGN CONCEPTS.....	58
7.2.1 Levels of reliability.....	58
7.2.2 Facility purpose.....	58
7.2.3 Multiuser versus single user groups.....	59
7.2.4 Equipment change cycle.....	59
7.2.5 Occupied versus unoccupied computer rooms.....	59
7.2.6 Data center location within building.....	59
7.2.7 Type of building.....	59

7.2.8 Multitenant buildings.....	60
7.2.9 24/7 operation of data center	60
7.2.10 Temperature and relative humidity control.....	60
7.2.11 Materials.....	60
7.3 DESIGN FOR EFFICIENCY	60
7.3.1 Holistic energy efficient data center design.....	60
7.3.2 Data center efficiency metrics	61
7.3.3 Data center energy saving design opportunities	62
7.4 GENERAL PATHS OF ACCESS.....	63
7.4.1 General access	63
7.4.2 Data center access.....	63
7.4.3 Equipment access	63
7.4.4 Telecommunications access provider entry into computer rooms	63
7.4.5 Vendor access.....	64
7.4.6 Support equipment service access	64
7.5 PROGRAMMING DETAIL	64
7.5.1 Entry	64
7.5.2 Control room and personnel areas	64
7.5.3 Printer room.....	64
7.5.4 Media storage room	64
7.5.5 Restrooms and break rooms.....	64
7.5.6 Computer room.....	65
7.5.7 Entrance rooms	66
7.5.8 Mechanical equipment space.....	66
7.5.9 Electrical room and UPS room	66
7.5.10 Battery room.....	66
7.5.11 Fire suppression room.....	67
7.5.12 Circulation	67
7.5.13 Equipment staging and storage.....	67
7.5.14 Equipment repair room.....	67
7.6 CONSTRUCTION COMPONENTS.....	67
7.6.1 Data center preparation.....	67
7.6.2 Floor slab.....	67
7.6.3 Computer room envelope wall construction	68
7.6.4 Nonrated partitions	68
7.6.5 Vapor/moisture seal.....	68
7.6.6 Door and glazed openings	68
7.6.7 Fire-rated construction.....	69
7.6.8 Access control systems.....	69
7.6.9 Access flooring system.....	70
7.6.10 Ceilings.....	71
7.6.11 Equipment bracing system.....	72
7.6.12 Computer room finishes	72
7.6.13 Roof systems.....	72
8 STRUCTURAL.....	73
8.1 CODE COMPLIANCE AND COORDINATION	73
8.2 IMPACT OF SITE LOCATION ON IMPLEMENTATION OF STANDARDS	73
8.3 TYPES OF LOADING ON THE STRUCTURE.....	73
8.4 STRUCTURAL CONCERNS SPECIFIC TO DATA CENTER DESIGN	73
8.4.1 Floor load.....	73
8.4.2 Wind	74
8.4.3 Earthquake.....	74

9 ELECTRICAL SYSTEMS	75
9.1 OVERVIEW	75
9.1.1 Introduction	75
9.1.2 Requirements	75
9.1.3 Availability and uptime	75
9.1.4 Redundancy	76
9.1.5 Capacity versus utilization efficiency	76
9.1.6 Electrical Class ratings	77
9.2 UTILITY SERVICE	85
9.2.1 Utility service planning	85
9.2.2 Low-voltage utility services	85
9.2.3 Medium-voltage utility services	86
9.2.4 Protective relaying	86
9.3 DISTRIBUTION	86
9.3.1 Requirements	86
9.3.2 UPS rectifier or motor inputs	87
9.3.3 Static switch bypass inputs	87
9.3.4 UPS system bypass	87
9.3.5 Power strips	87
9.3.6 Input source transfer	87
9.3.7 Generator controls and paralleling	89
9.3.8 Unit substations	89
9.3.9 UPS system	90
9.3.10 UPS output distribution	97
9.3.11 Power distribution units (PDUs)	99
9.3.12 Automatic static transfer switches	100
9.3.13 Direct current power systems	100
9.3.14 Computer room equipment power distribution	100
9.3.15 Surge suppression/surge protection devices (SPDs) for ac circuits	110
9.3.16 Emergency power off (EPO) systems	110
9.4 MECHANICAL EQUIPMENT SUPPORT	112
9.4.1 Introduction	112
9.4.2 Requirements	113
9.4.3 Recommendations	113
9.5 UNINTERRUPTIBLE POWER SUPPLY (UPS) SYSTEMS	115
9.5.1 Introduction	115
9.5.2 Sizing and application	115
9.5.3 Technologies	117
9.5.4 Paralleling and controls	118
9.5.5 Batteries and stored energy systems	119
9.6 STANDBY AND EMERGENCY POWER SYSTEMS	123
9.6.1 Sizing and application	123
9.6.2 Starting systems	124
9.6.3 Fuel system	124
9.6.4 Exhaust system	125
9.6.5 Cooling system	125
9.6.6 Mounting	125
9.7 AUTOMATION AND CONTROL	125
9.7.1 Introduction	125
9.7.2 Monitoring	126
9.7.3 Control	126
9.7.4 System integration	127
9.8 LIGHTING	127
9.8.1 Introduction	127
9.8.2 General Recommendations	127
9.8.3 Computer rooms	127
9.8.4 Support areas	128

9.9 BONDING AND GROUNDING	128
9.9.1 Introduction	128
9.9.2 General recommendations	130
9.9.3 Lightning protection	131
9.9.4 Surge protective devices	131
9.9.5 Telecommunications surge protection	132
9.9.6 Building ground (electrode) ring	133
9.9.7 Supplementary bonding and grounding	134
9.9.8 Information technology equipment (ITE) interconnections	139
9.9.9 Power system bonding and grounding	140
9.10 LABELING AND SIGNAGE	147
9.10.1 Introduction	147
9.10.2 Requirements	147
9.10.3 Recommendations	147
9.11 TESTING AND QUALITY ASSURANCE	148
9.11.1 Recommendations	148
9.12 ONGOING OPERATIONS	149
9.12.1 Recommendations	149
9.13 ELECTRICAL SYSTEMS MATRIX	149
10 MECHANICAL	165
10.1 CODE COMPLIANCE AND COORDINATION	165
10.2 TERMINOLOGY DIFFERENCES BETWEEN CODES AND TELECOMMUNICATIONS STANDARDS	165
10.3 ENVIRONMENTAL CONDITIONS	165
10.3.1 Introduction	165
10.3.2 Normal operation versus loss of environmental control	165
10.3.3 Environmental Class definitions	165
10.3.4 Air conditioning	166
10.3.5 Ventilation (outside air)	167
10.3.6 Airborne contaminants (gases and particles)	168
10.3.7 Environmental limits	168
10.3.8 Humidity control	169
10.3.9 Temperature and humidity control—tape media	169
10.3.10 Maximum dewpoint	169
10.3.11 Altitude	169
10.3.12 Noise levels	169
10.3.13 Leak detection	169
10.4 THERMAL MANAGEMENT	170
10.4.1 Introduction	170
10.4.2 Use of operating rather than nameplate load	170
10.4.3 Current equipment heat release and trends	171
10.4.4 Equipment heat release specifications	171
10.4.5 Electronic equipment cooling	171
10.4.6 Humidification and dehumidification equipment	171
10.4.7 Computer room cooling	172
10.4.8 Supplemental cooling	175
10.4.9 Hot and cold equipment aisles	176
10.4.10 Equipment layout	176
10.4.11 Supply air layout	176
10.4.12 Return air layout	176
10.4.13 Cable management	176
10.5 MECHANICAL EQUIPMENT (DESIGN AND OPERATION)	176
10.5.1 General recommendations	176
10.5.2 Computer room air conditioning (CRAC) units	177
10.5.3 Central air handlers	177
10.5.4 Supplemental cooling systems	177
10.5.5 Chilled water systems	178

10.5.6 Chillers	178
10.5.7 Cooling towers.....	178
10.5.8 Thermal Storage	178
10.5.9 Piping and pumps	178
10.5.10 Fuel oil tank and piping	179
10.5.11 Plumbing.....	179
10.5.12 Generator	179
10.6 MATERIALS AND FINISHES.....	179
10.6.1 Introduction	179
10.6.2 Materials in air plenums	180
10.7 REFERENCED STANDARDS AND DOCUMENTS	180
11 FIRE PROTECTION	183
11.1 INTRODUCTION	183
11.2 BASIC DESIGN ELEMENTS	183
11.3 GENERAL REQUIREMENTS AND RECOMMENDATIONS	183
11.3.1 Requirements	183
11.3.2 Recommendations.....	183
11.4 ENCLOSURES - WALLS, FLOORS, AND CEILINGS.....	184
11.4.1 Requirements	184
11.5 HANDHELD FIRE EXTINGUISHERS	184
11.5.1 Requirements	184
11.5.2 Recommendations.....	184
11.6 FIRE PROTECTION.....	184
11.6.1 Water sprinkler system	184
11.6.2 Gaseous fire suppression	185
11.7 FIRE DETECTION	186
11.7.1 Area requirements.....	186
11.7.2 Detector technology.....	187
11.7.3 Early warning detection systems	188
11.8 LABELING AND SIGNAGE.....	188
11.8.1 Requirements	188
11.8.2 Recommendations.....	188
11.9 TESTING AND QUALITY ASSURANCE	188
11.9.1 Requirements	188
11.9.2 Recommendations.....	188
11.10 ONGOING OPERATIONS.....	188
11.10.1 Requirements	188
11.10.2 Recommendations.....	188
11.11 REFERENCE.....	189
12 SECURITY	191
12.1 GENERAL.....	191
12.1.1 Introduction	191
12.1.2 Requirements	191
12.2 PHYSICAL SECURITY PLAN	191
12.2.1 Recommendations.....	191
12.2.2 Additional information	191
12.3 RISK AND THREAT ASSESSMENT	192
12.3.1 Definitions	192
12.3.2 Recommendations.....	192
12.4 REGULATORY REQUIREMENTS AND LEGISLATION	193
12.4.1 Recommendations.....	193
12.4.2 Additional information	193
12.5 DATA CENTER SECURITY PLAN.....	193
12.5.1 Recommendations.....	193

12.6 CRIME PREVENTION THROUGH ENVIRONMENT DESIGN	198
12.6.1 Recommendations.....	198
12.7 ACCESS CONTROL	199
12.7.1 Requirements	199
12.7.2 Recommendations.....	199
12.8 ALARMS.....	205
12.8.1 Introduction	205
12.8.2 Recommendations.....	205
12.9 SURVEILLANCE	207
12.9.1 Introduction	207
12.9.2 Recommendations.....	207
12.10 BARRIERS	209
12.10.1 Introduction	209
12.10.2 Recommendations.....	210
12.11 LIGHTING	219
12.11.1 Introduction	219
12.12 GUARDS.....	219
12.12.1 Introduction	219
12.12.2 Recommendations.....	219
12.13 DISASTER RECOVERY.....	219
12.13.1 Recommendations.....	219
12.14 BUILDING SITE CONSIDERATIONS.....	221
12.14.1 Introduction	221
12.14.2 Recommendations.....	221
12.15 BUILDING SHELL	225
12.15.1 Recommendations.....	225
12.16 DATA CENTER SECURITY DESIGN CONSIDERATIONS.....	226
12.16.1 Recommendations.....	226
13 BUILDING AUTOMATION SYSTEMS	231
13.1 INTRODUCTION	231
13.2 COMPONENTS.....	231
13.2.1 Cabling	231
13.2.2 Hardware	232
13.2.3 Communications.....	232
13.3 CABLING DESIGN CONSIDERATIONS	232
13.3.1 General cabling standards.....	232
13.3.2 Topology.....	233
13.3.3 Media	233
13.3.4 Pathways and spaces.....	234
13.3.5 Cabling management and termination	234
13.3.6 Enclosures.....	234
14 TELECOMMUNICATIONS	235
14.1 ACCESS PROVIDERS AND OUTSIDE PLANT	235
14.1.1 Security of underground telecommunications entrance pathways.....	235
14.1.2 Pathway adjacencies with other systems	235
14.1.3 Entrance facilities	235
14.1.4 Underground pathways.....	236
14.1.5 Access provider coordination	236
14.1.6 Access provider demarcation.....	237
14.1.7 Demarcation of low-speed circuits	237
14.1.8 Demarcation of E-1 and T-1 circuits	237
14.1.9 Demarcation of T-3 and E-3 coaxial cabling circuits	239
14.1.10 Demarcation of optical fiber circuits	239
14.1.11 Aerial service to facility.....	240
14.1.12 Underground pathway types and quantities to facility.....	240

14.1.13 Redundancy of underground pathways.....	240
14.1.14 Security of underground pathways	240
14.2 TELECOMMUNICATIONS SPACES	240
14.2.1 Design and structural considerations	240
14.2.2 Airborne particles created by telecommunications pathways components.....	241
14.2.3 Ramps	241
14.2.4 Computer room space allocation and layout.....	241
14.2.5 Entrances	241
14.2.6 Redundant main distribution area.....	242
14.2.7 Data center redundancy	243
14.2.8 Pathway and equipment support and attachment.....	243
14.2.9 Miscellaneous considerations	243
14.3 TELECOMMUNICATIONS AND COMPUTER CABINETS AND RACKS	243
14.3.1 General	243
14.3.2 Two post racks.....	243
14.3.3 Four post racks.....	244
14.3.4 Cabinets	244
14.3.5 Cabinets and rack configurations.....	244
14.3.6 Product configurations for racks.....	245
14.3.7 Product configurations for cabinets	245
14.3.8 Rack and cabinets installations	252
14.3.9 Rack installations.....	253
14.3.10 Cabinet installations.....	254
14.3.11 Thermal management in cabinets	257
14.4 TELECOMMUNICATIONS CABLING PATHWAYS	258
14.4.1 General	258
14.4.2 Security.....	259
14.4.3 Separation of power and telecommunications cabling.....	259
14.4.4 Separation and installation of cabling.....	260
14.4.5 Distribution method.....	260
14.4.6 Redundant backbone cabling.....	260
14.4.7 Redundant horizontal cabling.....	260
14.4.8 Cable tray support system.....	261
14.5 TELECOMMUNICATIONS CABLING	262
14.5.1 Introduction	262
14.5.2 Data center cabling system infrastructure.....	263
14.5.3 Main distribution area (MDA).....	263
14.5.4 Intermediate distribution area (IDA)	263
14.5.5 Horizontal distribution area (HDA).....	264
14.5.6 Zone distribution area (ZDA).....	264
14.5.7 Equipment distribution area (EDA).....	264
14.5.8 Cabling topology	264
14.5.9 Horizontal cabling topology	265
14.5.10 Backbone cabling topology	265
14.5.11 Accommodation of nonstar configurations.....	266
14.5.12 Redundant cabling topologies.....	266
14.5.13 Horizontal cabling	266
14.5.14 Horizontal cabling types.....	267
14.5.15 Balanced twisted-pair cabling.....	267
14.5.16 Optical fiber cabling	268
14.5.17 Single-mode and multimode connector color	269
14.5.18 Shared sheath guidelines.....	269
14.5.19 Hybrid and bundled cable assembly applications	269
14.5.20 Trunk cabling assemblies	270
14.5.21 Horizontal cabling length limitations.....	270
14.5.22 Balanced twisted-pair cord length limitations	271
14.5.23 Horizontal cabling applications	271
14.5.24 Backbone cabling.....	271

14.5.25 Backbone cabling types	272
14.5.26 Backbone cabling length limitations.....	273
14.5.27 Centralized optical fiber cabling.....	273
14.5.28 Centralized optical fiber length limitations.....	273
14.5.29 Implementation.....	274
14.5.30 Cable management.....	275
14.5.31 Bend radius and pulling tension guidelines.....	276
14.5.32 Balanced twisted-pair cabling bend radius and pulling tension best practices.....	276
14.5.33 Optical fiber cable bend radius and pulling tension best practice.....	277
14.5.34 Abandoned cable.....	277
14.6 FIELD TESTING DATA CENTER TELECOMMUNICATIONS CABLING.....	277
14.6.1 Introduction.....	277
14.6.2 Conformance.....	278
14.6.3 100-ohm balanced twisted-pair cabling field testing.....	278
14.6.4 Optical fiber cabling field testing.....	281
14.7 TELECOMMUNICATIONS CABLING, PATHWAYS, AND SPACES ADMINISTRATION.....	284
14.7.1 General.....	284
14.7.2 Identification conventions for data center components.....	285
14.7.3 Intelligent infrastructure management.....	288
14.8 TELECOMMUNICATIONS INFRASTRUCTURE CLASSES.....	289
14.8.1 Introduction.....	289
14.8.2 Class F2 telecommunications infrastructure.....	291
14.8.3 Class F3 telecommunications infrastructure.....	291
14.8.4 Class F4 telecommunications infrastructure.....	291
15 INFORMATION TECHNOLOGY.....	293
15.1 DISASTER RECOVERY.....	293
15.1.1 Introduction.....	293
15.1.2 Offsite data storage.....	293
15.1.3 Collocation facility.....	293
15.1.4 Onsite data center redundancy.....	293
15.1.5 HVAC failure.....	294
15.1.6 Power failure.....	294
15.1.7 Mirroring.....	294
15.1.8 Location of real-time redundant storage device.....	294
15.1.9 Physical connectivity methods and devices.....	295
15.1.10 RAID.....	295
15.1.11 Distance between data centers.....	295
15.2 CHANNEL AND CONSOLE CABLING.....	295
15.2.1 Introduction.....	295
15.2.2 Mainframe channel cabling.....	295
15.3 COMMUNICATIONS.....	298
15.3.1 Wired/wireless/hands-free voice communications.....	298
15.3.2 Wireless network for portable maintenance equipment.....	298
15.3.3 Zone paging.....	299
15.4 COMPUTER ROOM LAYOUT.....	299
15.4.1 Introduction.....	299
15.4.2 Equipment line-ups for efficiency.....	300
15.4.3 Connectivity panel distribution.....	300
15.4.4 Aisle sizing and workflow analyses for proper walkways and egress pathways.....	302
15.5 OPERATIONS CENTER.....	303
15.5.1 Monitoring of building systems.....	303
15.5.2 Location.....	303

16 COMMISSIONING	305
16.1 GENERAL	305
16.1.1 Introduction	305
16.1.2 Recommendations.....	305
16.2 PHASES OF COMMISSIONING PROCESS	305
16.2.1 Program phase	305
16.2.2 Design phase.....	305
16.2.3 Construction phase.....	306
16.2.4 Acceptance phase.....	306
16.2.5 Post-acceptance phase	306
16.3 TYPES OF COMMISSIONING	306
16.3.1 Introduction	306
16.3.2 Continuous commissioning	306
16.3.3 Milestone commissioning.....	306
16.3.4 Acceptance phase commissioning	306
16.3.5 Network operability.....	306
16.4 TESTING	306
16.4.1 Introduction	306
16.4.2 Functional testing components	307
16.4.3 Functional testing procedures	307
16.5 COMMISSIONING DOCUMENTS	307
16.5.1 Introduction	307
16.5.2 Design documents.....	307
16.5.3 Process documents.....	307
16.5.4 Verification documents.....	307
16.5.5 Operation and maintenance documents	308
16.6 EXAMPLE OF FINAL COMMISSIONING REPORT (INFORMATIVE)	308
16.7 EXAMPLE OF PDU TESTING (INFORMATIVE)	308
16.7.1 Purpose	308
16.7.2 Introduction	308
16.7.3 Systems impacted	308
16.7.4 Backout plan.....	308
16.8 EXAMPLE OF PDU AND DIESEL GENERATOR TESTING (INFORMATIVE)	315
16.8.1 Purpose	315
16.8.2 Scope	315
16.8.3 Vendor’s responsibility.....	315
16.8.4 General contractor’s responsibility	315
16.8.5 Testing agent’s responsibility	316
16.8.6 Requirements.....	316
16.8.7 Emergency generator system testing	317
16.8.8 UPS testing	319
16.8.9 Data tables	322
17 DATA CENTER MAINTENANCE	331
17.1 MAINTENANCE CONSIDERATIONS	331
17.1.1 Introduction	331
17.1.2 Requirements	332
17.2 SYSTEMS REQUIRING MAINTENANCE	332
17.2.1 Cabling systems	332
17.2.2 Electrical systems	332
17.2.3 HVAC systems	335
17.2.4 IT and telecommunications systems	336
17.2.5 Access floor systems.....	338
17.2.6 Fire protection and suppression systems maintenance.....	345
17.2.7 Security systems maintenance	346
17.2.8 Monitoring and management systems maintenance	346

17.3 MAINTENANCE RECORDKEEPING	347
17.3.1 Recommendations.....	347
ANNEX A: DESIGN PROCESS (INFORMATIVE)	349
A.1 INTRODUCTION	349
A.1.1 Traditional A/E design process	349
A.1.2 Traditional technology design process.....	349
A.1.3 Data center design process requirements.....	350
A.2 PROJECT DELIVERY METHODS	350
A.2.1 Design-bid-build	350
A.2.2 Design-build	350
A.2.3 Construction management	351
A.3 FACILITY DESIGN PHASES	351
A.3.1 Planning and concept development	351
A.3.2 Schematic design (SD).....	352
A.3.3 Design development (DD).....	352
A.3.4 Prepurchase.....	352
A.3.5 Construction documents (CD)	353
A.4 TECHNOLOGY DESIGN PHASES	353
A.4.1 Needs assessment.....	353
A.4.2 Design analysis	353
A.4.3 Acquisition.....	353
A.4.4 Implementation	354
A.5 COMMISSIONING	354
A.6 DATA CENTER DOCUMENTATION	354
A.6.1 Recommendations.....	354
ANNEX B: RELIABILITY AND AVAILABILITY (INFORMATIVE)	355
B.1 INTRODUCTION	355
B.2 ADDITIONAL INFORMATION	355
B.2.1 Goals and objectives	355
B.2.2 Creating mission-critical facilities	356
B.2.3 Risk analysis	356
B.2.4 Reliability aspects of availability planning	360
B.2.5 Reliability planning worksheet	364
B.2.6 Other factors.....	364
B.2.7 Other reliability alternatives.....	366
ANNEX C: REFERENCED DOCUMENTS (INFORMATIVE)	367

This page intentionally left blank

INDEX OF FIGURES

FIGURE 1: SYSTEM CAPACITIES AT VARIOUS STAGES OF THE ELECTRICAL DISTRIBUTION SYSTEM	24
FIGURE 2: SPACE ADJACENCIES	25
FIGURE 3: EXAMPLES OF AISLE WIDTH WITH DIFFERENT CABINET SIZES	33
FIGURE 4: UNITED STATES GROUND-SHAKING AREAS (U.S. GEOLOGICAL SURVEY).....	37
FIGURE 5: UNITED STATES VOLCANIC AREAS (U.S. GEOLOGICAL SURVEY)	38
FIGURE 6: UNITED STATES LANDSLIDE AREAS (U.S. GEOLOGICAL SURVEY).....	38
FIGURE 7: UNITED STATES AQUIFER TYPES (U.S. GEOLOGICAL SURVEY).....	39
FIGURE 8: UNITED STATES GROUND WATER REGIONS (U.S. GEOLOGICAL SURVEY).....	40
FIGURE 9: UNITED STATES HURRICANE ACTIVITY AREAS (U.S. GEOLOGICAL SURVEY)	42
FIGURE 10: UNITED STATES TORNADO RISK AREAS (U.S. GEOLOGICAL SURVEY)	42
FIGURE 11: UNITED STATES GENERAL AREAS OF MAJOR FLOODING (U.S. GEOLOGICAL SURVEY)	43
FIGURE 12: UTILITY RELIABILITY EXAMPLES	45
FIGURE 13: CONCEPTUAL DATA CENTER LAYOUT	65
FIGURE 14: CLASS F0 ELECTRICAL CONCEPT DIAGRAM	79
FIGURE 15: CLASS F1 ELECTRICAL CONCEPT DIAGRAM	80
FIGURE 16: CLASS F2 CONCEPT DIAGRAM.....	81
FIGURE 17A: CLASS F3 SINGLE SOURCE SINGLE UTILITY INPUT.....	82
FIGURE 17B: CLASS F3 SINGLE SOURCE TWO UTILITY INPUTS	83
FIGURE 18: CLASS F4 ELECTRICAL TOPOLOGY (SYSTEM-PLUS-SYSTEM)	84
FIGURE 19: CLASS F4 ELECTRICAL TOPOLOGY (xN OR DISTRIBUTED REDUNDANT)	84
FIGURE 20: SINGLE-MODULE UPS WITH INTERNAL STATIC BYPASS AND MAINTENANCE BYPASS FROM THE SAME SOURCE.....	91
FIGURE 21: SINGLE-MODULE UPS WITH INPUTS TO RECTIFIER, STATIC BYPASS, AND MAINTENANCE BYPASS FROM THE SAME SOURCE	92
FIGURE 22: MULTIPLE-MODULE UPS WITH INPUTS TO RECTIFIER, STATIC BYPASS, AND MAINTENANCE BYPASS FROM THE SAME SOURCE	92
FIGURE 23: SINGLE-MODULE UPS BYPASS—ALTERNATE BYPASS SOURCE - INPUT TO RECTIFIER FROM PRIMARY SOURCE; INPUTS TO STATIC BYPASS AND MAINTENANCE BYPASS FROM A SECOND SOURCE	93
FIGURE 24: MULTIPLE-MODULE UPS BYPASS—ALTERNATE BYPASS SOURCES - INPUTS TO RECTIFIERS FROM PRIMARY SOURCE; INPUTS TO STATIC BYPASS AND MAINTENANCE BYPASS FROM A SECOND SOURCE.....	94
FIGURE 25: SINGLE-MODULE UPS BYPASS—MULTIPLE BYPASS SOURCES - INPUTS TO RECTIFIER AND STATIC BYPASS FROM PRIMARY SOURCE, AND INPUT TO MAINTENANCE BYPASS FROM A SECOND SOURCE.....	95
FIGURE 26: MULTIPLE-MODULE UPS BYPASS—MULTIPLE BYPASS SOURCES - INPUTS TO RECTIFIERS AND STATIC BYPASS FROM PRIMARY SOURCE, AND INPUT TO MAINTENANCE BYPASS FROM A SECOND SOURCE.....	95
FIGURE 27: AN EXAMPLE OF AN APPROACH TO UPS OUTPUT SWITCHBOARD LOAD MANAGEMENT	98
FIGURE 28: PDU CONFIGURATION: SINGLE-CORDED AND POLY-CORDED DEVICES	99
FIGURE 29: AUTOMATIC STATIC TRANSFER SWITCH - SINGLE TRANSFORMER, PRIMARY SIDE SWITCHING.....	101
FIGURE 30: AUTOMATIC STATIC TRANSFER SWITCH - DUAL TRANSFORMER, SECONDARY SIDE SWITCHING	101
FIGURE 31: N CIRCUIT MAP WITH 3 CIRCUITS PER CABINET (CLASS F1 AND CLASS F2)	105
FIGURE 32: N + 1 CIRCUIT MAP WITH 3 N CIRCUITS PER CABINET/4 REQUIRED (CLASS F3).....	106
FIGURE 33: xN CIRCUIT MAP WITH 3 N CIRCUITS PER CABINET/5 REQUIRED (CLASS F4).....	107
FIGURE 34: 2N CIRCUIT MAP WITH 3 N CIRCUITS PER CABINET/6 REQUIRED (CLASS F4)	108
FIGURE 35: EPO SYSTEM	111
FIGURE 36: SAMPLE POWER CIRCUITS FOR A CLASS F3 MECHANICAL SYSTEM.....	112

FIGURE 37: SAMPLE POWER CIRCUITS FOR A CLASS F4 MECHANICAL SYSTEM.....	113
FIGURE 38: CRITICAL FACILITY EXAMPLE GROUNDING DIAGRAM.....	129
FIGURE 39: DATA CENTER GROUNDING SCHEMATIC.....	135
FIGURE 40: TYPICAL CONFIGURATION OF FLAT STRIP-TYPE SBG WITHIN A MESH-BN.....	136
FIGURE 41: ADJACENT ROLLS OF FLAT-STRIP-TYPE SBG BEING EXOTHERMICALLY-WELDED TOGETHER.....	137
FIGURE 42: DATA CENTER GROUNDING INFRASTRUCTURE (ROOM LEVEL) EXAMPLE.....	137
FIGURE 43: TELECOMMUNICATIONS BONDING AND GROUNDING INFRASTRUCTURE.....	142
FIGURE 44: SIMILARITY OF RECOMMENDED GROUNDING FOR AC AND DC POWER SYSTEMS AND LOAD EQUIPMENT.....	143
FIGURE 45: DC POWER SYSTEM SHOWING SINGLE-POINT GROUNDED RETURN.....	144
FIGURE 46: INFORMATION TECHNOLOGY EQUIPMENT SHOWING GROUNDING OF DC POWER INPUT (RETURN IS INSULATED).....	144
FIGURE 47: COMMON BONDING NETWORK.....	145
FIGURE 48: ISOLATED (INSULATED) BONDING NETWORK.....	145
FIGURE 49: SAMPLE EQUIPMENT NAMEPLATE.....	147
FIGURE 50: ARC FLASH WARNING LABEL.....	148
FIGURE 51: SECURITY MEASURES.....	192
FIGURE 52: EXPIRING BADGE.....	205
FIGURE 53: SECURITY LAYERS.....	209
FIGURE 54: CROSS-CONNECTION CIRCUITS TO IDC CONNECTING HARDWARE CABLED TO MODULAR JACKS IN THE T568A 8-PIN SEQUENCE.....	238
FIGURE 55: CROSS-CONNECTION CIRCUITS TO IDC CONNECTING HARDWARE CABLED TO MODULAR JACKS IN THE T568B 8-PIN SEQUENCE.....	238
FIGURE 56: CABINET GROUND BUSBAR EXAMPLE.....	245
FIGURE 57: CABINET APERTURE OPENING.....	248
FIGURE 58: BLANK PANELS INSTALLED IN EMPTY RUS.....	248
FIGURE 59: ILLUSTRATION OF COMPONENTS FOR CABLE CAPACITY FORMULAE.....	250
FIGURE 60: CABINETS ARE IDENTIFIED AND LABELED.....	252
FIGURE 61: TERMINATION PORTS AND EQUIPMENT CABLES ARE CLEARLY LABELED.....	253
FIGURE 62: EFFECT OF INTERNAL HOT AIR RECIRCULATION.....	254
FIGURE 63: HOW REDUCING INTERNAL HOT AIR RECIRCULATION REDUCES INPUT AIR TEMPERATURE.....	254
FIGURE 64: GASKET SEALS OFF ACCESS FLOOR TILE CUTOUT IN VERTICAL CABLE MANAGER.....	255
FIGURE 65: BRUSH GROMMET SEALS ACCESS FLOOR TILE CUTOUT UNDER EQUIPMENT CABINET.....	255
FIGURE 66: CABINET DOOR AND SIDE PANEL ARE BONDED TO CABINET FRAME. FRAME GROUND TERMINAL BLOCK IS IN BOTTOM OF PICTURE.....	255
FIGURE 67: METHOD FOR SECURING RACKS AND CABINETS ON AN ACCESS FLOOR USING THREADED ROD CONNECTED TO STEEL CHANNEL BOLTED TO CONCRETE SLAB.....	256
FIGURE 68: HOT AISLE/COLD AISLE CABINET LAYOUT.....	257
FIGURE 69: DATA CENTER CABLING TOPOLOGY EXAMPLE.....	265
FIGURE 70: CENTRALIZED OPTICAL FIBER CABLING EXAMPLE.....	274
FIGURE 71: CHANNEL MODEL EXAMPLE.....	279
FIGURE 72: PERMANENT LINK EXAMPLE.....	279
FIGURE 73: ROOM GRID COORDINATE SYSTEM EXAMPLE.....	285
FIGURE 74: INTELLIGENT INFRASTRUCTURE MANAGEMENT INTERCONNECTION CONFIGURATION EXAMPLE.....	289
FIGURE 75: INTELLIGENT INFRASTRUCTURE MANAGEMENT CROSS-CONNECTION CONFIGURATION EXAMPLE.....	289
FIGURE 76: TELECOMMUNICATIONS CABLING INFRASTRUCTURE CLASSES.....	290
FIGURE 77: EXAMPLE OF LAN AND SAN INFRASTRUCTURE AT CLASS F3 AND CLASS F4.....	290
FIGURE 78: NO RADIO ZONE AROUND SUPPRESSION TANK ROOM.....	299

FIGURE 79: SIMPLE CONNECTION TOPOLOGY 301

FIGURE 80: SAMPLE ZONE DISTRIBUTION TOPOLOGY 301

FIGURE 81: SAMPLE REDUNDANT TOPOLOGY 302

FIGURE 82: ONE RACK SPACE UNIT (1U) 24 PORT ETHERNET SWITCH..... 337

FIGURE 83: ENTERPRISE CLASS NETWORK SWITCH (CONNECTIVITY AND MAINTENANCE ACCESS VIEW)..... 337

FIGURE A1: TRADITIONAL A/E DESIGN PROCESS 349

FIGURE A2: DATA CENTER A/E DESIGN PROCESS..... 350

FIGURE B1: PLANNING PROCESS FOR A MISSION-CRITICAL FACILITY 356

FIGURE B2: RISK ANALYSIS PROCESS..... 357

FIGURE B3: SAMPLE RELIABILITY CALCULATION..... 360

This page intentionally left blank

INDEX OF TABLES

TABLE 1: MULTIPLIERS FOR ELECTRICAL DISTRIBUTION SYSTEM COMPONENTS	23
TABLE 2: HYDRAULIC CHARACTERISTICS OF GROUNDWATER REGIONS OF THE UNITED STATES (COMMON RANGES)	40
TABLE 3: DATA CENTER ENERGY SAVING OPPORTUNITIES	62
TABLE 4: MINIMUM FIRE RATING OF SPACES	69
TABLE 5: COMPUTER ROOM ACCESS FLOOR PERFORMANCE SPECIFICATIONS	70
TABLE 6: DESIGN EFFICIENCY RATIOS	77
TABLE 7: STATIC BYPASS SWITCH INPUT, BY AVAILABILITY CLASS	96
TABLE 8: SUMMARY OF UPS OUTPUT SWITCHBOARD COUNTS FOR CLASSES	97
TABLE 9: EXAMPLE UPS/PDU CAPACITY CALCULATIONS	103
TABLE 10: EXAMPLE OF UPS/PDU CAPACITY CALCULATIONS	109
TABLE 11: BATTERY STANDARDS CROSS-REFERENCE TABLE (IEEE STANDARD NUMBER)	123
TABLE 12: GROUNDING AND BONDING CONNECTION SCHEDULE	138
TABLE 13: ELECTRICAL SYSTEMS AVAILABILITY CLASSES	150
TABLE 14: RECOMMENDED SPRINKLER SYSTEMS FOR DATA CENTER SPACES	185
TABLE 15: RECOMMENDED DETECTION SYSTEMS FOR DATA CENTER SPACES	186
TABLE 16: THICKNESS OF CONCRETE WALL FOR PROJECTILE PROTECTION	210
TABLE 17: VEHICLE BARRIER COMPARISON	211
TABLE 18: SPEED OF CONCRETE WALL PENETRATION	212
TABLE 19: TIME TO PENETRATE INDUSTRIAL PEDESTRIAN DOORS	213
TABLE 20: TIME TO PENETRATE WINDOWS	214
TABLE 21: MINIMUM LIGHTING LEVELS	223
TABLE 22: EXAMPLE OF CABINET DEPTH GUIDELINES	246
TABLE 23: AVAILABLE SPACE FOR CALCULATING CABINET VERTICAL CABLE CAPACITY	250
TABLE 24: MAXIMUM CABLE STACKING HEIGHT IN CABLING PATHWAYS	259
TABLE 25: BALANCED TWISTED-PAIR CABLING CHANNEL PERFORMANCE	267
TABLE 26: OPTICAL FIBER CABLE PERFORMANCE BY TYPE	268
TABLE 27: ADVANTAGES AND DISADVANTAGES OF TRUNK CABLING ASSEMBLIES	270
TABLE 28: BALANCED TWISTED-PAIR CABLE BEND RADIUS AND PULLING TENSION	276
TABLE 29: OPTICAL FIBER CABLE BEND RADIUS AND PULLING TENSION BEST PRACTICES	277
TABLE 30: BALANCED TWISTED-PAIR FIELD TESTING	280
TABLE 31: REFERENCE JUMPER REPEATABILITY ALLOWANCE	282
TABLE B1: DEFINING MISSION-CRITICAL RISK LEVEL STEP 1 – IDENTIFY OPERATIONAL REQUIREMENTS: TIME AVAILABLE FOR PLANNED MAINTENANCE SHUTDOWN	358
TABLE B2: DEFINING MISSION-CRITICAL RISK LEVEL STEP 2 – IDENTIFY OPERATIONAL LEVELS: TOLERANCE FOR UNSCHEDULED SHUTDOWN	358
TABLE B3: DEFINING MISSION-CRITICAL RISK LEVEL STEP 3 – CLASSIFY THE IMPACT OF DOWNTIME ON THE MISSION	359
TABLE B4: DETERMINING FACILITY AVAILABILITY CLASS	359
TABLE B5: SAMPLE COST AND BENEFIT OF VARYING DEGREES OF RELIABILITY	361

This page intentionally left blank

1 Introduction

1.1 General

This standard is written with the expectation that the reader is familiar with the different facets of the design process (See Annex A). The reader should understand from which role and point of view he or she intends to use this document (e.g., information technology, facilities, other corporate internal or external to the owner). Refer to Sections 1.2.1 – 1.2.3 below.

1.2 Purpose

This standard provides a reference of common terminology and design practice. It is not intended to be used by architects and engineers as their sole reference or as a step-by-step design guide but may be used by such persons to determine design requirements in conjunction with the data center owner, occupant, or consultant.

This standard is intended primarily for:

- Data center owners and operators.
- Telecommunications and information technology (IT) consultants and project managers.
- Telecommunications and IT technology installers.

Additionally, individuals in the following groups are also served by this standard.

1.2.1 Users within information technology (IT)

1.2.1.1 Information technology (IT) and telecommunications designers

IT and telecommunications designers and consultants may use BICSI 002 in conjunction with the appropriate local telecommunications infrastructure standard (e.g., ANSI/TIA-942, AS/NZS 2834-1995 Computer Accommodation, CENELEC EN 50173 Series, ISO/IEC 24764) to design the telecommunications pathways, spaces, and cabling system for the data center. The telecommunications designer/consultant should work with the data center architects and engineers to develop the IT and telecommunications equipment floor plan using guidelines specified in this standard.

1.2.1.2 Information technology (IT) and telecommunications management

IT and telecommunications management may use BICSI 002 as an aid in defining initial data center design requirements based on required levels of security, reliability, and availability. IT and telecommunications should work with information protection management, the business continuity group, and end user departments to determine the required levels of security, reliability, and availability.

1.2.1.3 Information technology (IT) operations management

Working with facilities group, IT operations managers may use BICSI 002 to guide the requirements they specify to outsource suppliers who provide computing services and server room IT operations.

1.2.1.4 Information security

Information security personnel may use BICSI 002 as a guide in defining and implementing information protection and security and assisting in the development of standard policies and operating procedures.

1.2.2 Users within facilities group

1.2.2.1 Technical representatives within facilities group capital projects

Facilities group technical representatives may use BICSI 002 as a guide during the project planning phase as they estimate costs, prepare preliminary design and construction schedules, and prepare requests for professional services (RFPS) for the design and construction of new or renovated IT facilities. Thus, after the method of project delivery is determined, BICSI 002 becomes a referenced document in the RFPS that the facilities group prepares and issues to architecture and engineering (A&E) and/or design-build (D/B) firms. These companies, in turn, bid on the design and/or construction of the IT facilities.

1.2.2.2 Facilities management representatives within facilities group

Facilities operations and management may use BICSI 002 as a guide in planning the operation and maintenance of corporate IT facilities, so that these facilities maintain defined levels of reliability and availability. For example, BICSI 002 provides guidance in defining training needs and maintenance schedules of critical equipment for operations and maintenance personnel.

1.2.3 Staff outside information technology (IT) and facilities groups

1.2.3.1 Physical security management

Security staff responsible for physical security management may use BICSI 002 as a guide in determining physical security and fire protection system requirements for IT facilities.

1.2.3.2 External resources

1.2.3.2.1 Telecommunications consulting firms

BICSI 002 is useful to telecommunications consulting firms or design/build installation firms by providing guidance in the design and/or construction of IT facilities for the corporation.

1.2.3.2.2 A&E and construction firms

BICSI 002 is useful to A&E and construction firms to guide them in the process of design and/or construction of IT facilities. It provides a reference of common terminology and reliability topologies. It is not intended to be used by A&E and construction firms as their sole reference, nor is it meant to provide a step-by-step design guide for the A&E or D/B firms, but may be used by such persons to guide design requirements in conjunction with the data center owner, occupant, or consultant.

1.3 Categories of criteria

Two categories of criteria are specified—mandatory and advisory.

- Mandatory criteria generally apply to protection, performance, administration and compatibility; they specify the absolute minimum acceptable requirements.
- Advisory or desirable criteria are presented when their attainment will enhance the general performance of the data center infrastructure in all its contemplated applications.

Mandatory requirements are designated by the word *shall*; advisory recommendations are designated by the words *should*, *may*, or *desirable*, which are used interchangeably in this standard. Where possible, requirements and recommendations were separated to aid in clarity.

Notes, cautions and warnings found in the text, tables, or figures are used for emphasis or for offering informative suggestions.

2 Scope

This standard provides best practices and implementation methods that complement TIA, CENELEC, ISO/IEC and other published data center standards and documents. It is primarily a design standard, with installation requirements and guidelines related to implementing a design. The standard includes other installation requirements and guidelines for data centers, where appropriate.

3 References

The following standards and documents are referenced within this standard and contain provisions that constitute provisions of this standard.

Alliance for Telecommunication Industry Solutions (ATIS)

- ATIS 0600336, *Engineering Requirements for a Universal Telecommunications Framework* (2003)

American Society of Heating, Refrigerating, and Air-Conditioning Engineer (ASHRAE)

- ASHRAE 62.1, *Ventilation for Acceptable Indoor Air Quality* (2007);
- ASHRAE *Best Practices for Datacom Facility Energy Efficiency* (2009);
- ASHRAE *Datacom Equipment Power Trends and Cooling Applications* (2005);
- ASHRAE *Design Considerations for Data and Communications Equipment Centers* (2009);
- ASHRAE *Gaseous and Particulate Contamination Guidelines for Data Centers* (2009);
- ASHRAE *Structural and Vibration Guidelines for Datacom Equipment Centers* (2008);
- ASHRAE *Thermal Guidelines for Data Processing Environments* (2009);

Consumer Electronics Association (CEA)

- CEA-310-E, *Cabinets, Racks, Panels, and Associated Equipment* (2005);

European Committee for Electrotechnical Standardization (CENELEC)

- CENELEC EN 50173-1, *Information technology - Generic Cabling Systems – Part 1: General Requirements* (2007);
- CENELEC EN 50173-5, *Information technology - Generic Cabling Systems - Part 5 Data Centres* (2007);
- CENELEC EN 50174-2, *Information technology - Cabling installation - Installation planning and practices inside buildings* (2009);

European Telecommunications Standards Institute (ETSI)

- ETSI EN 300-019, *Equipment Engineering (EE) - Environmental conditions and environmental tests for telecommunications equipment*

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 142-2007 (The IEEE Green Book), *Recommended Practice for Grounding for Industrial and Commercial Buildings*;
- IEEE 450-2002, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Application*;
- IEEE 484-2002, *IEEE Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications*;
- IEEE 493-2007 (The IEEE Gold Book), *Recommended Practice for Design of Reliable and Commercial Power Systems*;
- IEEE 1100-2005 (The IEEE Emerald Book), *Recommended Practice for Powering and Grounding Electronic Equipment*;
- IEEE 1106-2005, *IEEE Recommended Practice for Maintenance, Testing and Replacement of Nickel-Cadmium Batteries for Stationary Applications*;
- IEEE 1115-2000, *IEEE Recommended Practice for Sizing Nickel-Cadmium Batteries for Stationary Applications*;
- IEEE 1184-2006, *IEEE Guide for the Selection and Sizing of Batteries for Uninterruptible Power Systems*;
- IEEE 1187-2002, *IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications*;
- IEEE 1188-2005, *IEEE Recommended Practice for Maintenance, Testing and Replacement of Valve Regulated Lead-Acid Batteries (VRLA) for Stationary Applications*;
- IEEE 1189-2007, *IEEE Guide for the Selection of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications*;
- IEEE 1491-2005, *IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications*;
- IEEE 1578-2007, *IEEE Recommended Practice for Stationary Battery Electrolyte Spill Containment and Management*;

International Electrotechnical Commission (IEC)

- IEC 61280-4-1:2009(E), *Fibre-optic communication subsystem test procedures - Part 4-1: Installed cable plant - Multimode attenuation measurement*;
- IEC 61280-4-2:1999, *Fibre Optic Communication Subsystem Basic Test Procedures - Part 4-2: Fibre Optic Cable Plant - Single-Mode Fibre Optic Cable Plant Attenuation*;
- IEC 61935-1:2005, *Generic cabling systems-Communication cabling in accordance with ISO/IEC 11801-Part 1: Installed cabling*;
- IEC 62305-3: 2006, *Protection against lightning - Part 3: Physical damage to structures and life hazard*;

International Organization for Standardization (ISO)

- ISO/IEC 11801:2002, *Information technology - Generic cabling for customer premises*;
- ISO/IEC TR 14763-2:2000, *Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation of copper cabling*;
- ISO/IEC 14763-3:2006, *Information technology—Implementation and operation of customer premises cabling-Part 3: Testing of optical fibre cabling*;
- ISO/IEC 24764:2010, *Information technology - Generic cabling systems for data centres*;

National Electrical Contractors Association (NECA)

- ANSI/NECA/BICSI 607, *Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings* (2010);

National Fire Protection Association (NFPA)

- NFPA 12, *Carbon Dioxide Fire Extinguishing Systems* (2008);
- NFPA 12A, *Halon 1301 Fire Extinguishing Systems* (2009);
- NFPA 13, *Standard for the Installation of Sprinkler Systems* (2010);
- NFPA 20, *Installation of Stationary Pumps for Fire Protection* (2010);
- NFPA 70, *The National Electrical Code®* (NEC®) (2008);
- NFPA 70E, *Standard for Electrical Safety in the Workplace* (2004);
- NFPA 72, *National Fire Alarm Code* (1999);
- NFPA 75, *Standard for the Protection of Information Technology Equipment* (2009);
- NFPA 76, *Recommended Practice for the Fire Protection of Telecommunications Facilities* (2009)
- NFPA 1600, *Standard on Disaster/Emergency Management Business Continuity Programs* (2007);
- NFPA 2001, *Standard on Clean Agent Fire Extinguishing Systems* (2008);
- *NFPA Fire Protection Handbook* (2003);

Telcordia

- Telcordia GR-63-CORE, *NEBS Requirements: Physical Protection* (2006);
- Telcordia GR-139, *Generic Requirements for Central Office Coaxial Cable* (1996);
- Telcordia GR-3028-CORE (2001), *Thermal Management in Telecommunications Central Offices: Thermal GR-3028-CORE*;

Telecommunication Industry Association (TIA)

- ANSI/TIA TSB-155-A, *Guidelines for the Assessment and Mitigation of Installed Category 6 Cabling to Support 10GBASE-T* (2010);
- ANSI/TIA-526-14-A OFSTP-14 *Optical Power Loss Measurement of Installed Multimode Fiber Cable Plant* (1998);
- TIA-569-B, *Commercial Building Standard for Telecommunications Pathways and Spaces* (2004).
- ANSI/TIA/EIA-606-A, *Administration Standard for Commercial Telecommunications Infrastructure* (2002);
- ANSI-J-STD-607-A, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications* (2002);
- ANSI/TIA-862, *Building Automation Cabling Standard for Commercial Buildings* (2002);
- ANSI/TIA-942, *Telecommunications Infrastructure Standard for Data Centers* (2005);

Underwriters Laboratories (UL)

- ANSI/UL 497-2001, *Standard for Safety Protectors for Paired-Conductor Communications Circuits*;
- UL 60950-1 2003, *Information Technology Equipment - Safety - Part 1: General Requirements*;

Other Standards and Documents

- *Americans with Disabilities Act* (ADA) (1990);
- *EU Code of Conduct on Data Centres Energy Efficiency*, Version 1.0 (2008);
- *EU Best Practices for EU Code of Conduct on Data Centres*, version 1.0 (2008);
- *International Building Code* (IBC), 2009;
- *International Fuel Gas Code* (IFGC), 2009;
- *International Mechanical Code* (IMC), 2009;
- *International Plumbing Code* (IPC), 2009;

At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

Where equivalent local codes and standards exist, requirements from these local specifications shall apply. Where reference is made to a requirement that exceeds minimum code requirements, the specification requirement shall take precedence over any apparent conflict with applicable codes.

4 Definitions, acronyms, abbreviations, and units of measurement

For the purpose of this standard the following definitions, acronyms, abbreviations and units of measurement apply.

4.1 Definitions

A-C-rated fire-retardant plywood: Plywood treated with a fire-retardant that has a well-finished A grade side that typically faces outward and a less finished C grade side that typically faces the wall.

abandoned cable: Installed cables that are not terminated at both ends at a connector or other equipment and not identified 'For Future Use' with a tag.

access block: A single access switch or group of switches sharing one trunk/uplink or set of redundant uplinks to the distribution layer. Generally confined to one telecommunications room (TR). In a large TR, it is possible to have more than one access block.

access floor: A system consisting of completely removable and interchangeable floor panels that are supported on adjustable pedestals or stringers (or both) to allow access to the area beneath the floor (also known as raised floor).

access layer: The access layer is the point at which local end users are allowed into the network. In the LAN environment, this connection point is typically a switched Ethernet port that is assigned to a VLAN.

access provider: The operator of any facility that is used to convey telecommunications signals to and from a customer premises.

adapter: A device that enables any or all of the following: (1) different sizes or types of plugs to mate with one another or to fit into a telecommunications outlet, (2) the rearrangement of leads, (3) large cables with numerous conductors to fan out into smaller groups of conductors, (4) interconnection between cables, (5) limited voltage and/or polarity and/or DC rectification conversion.

administration: The method for labeling, identification, documentation and usage needed to implement moves, additions and changes of the telecommunications infrastructure

alarm: A visual and audible signal indicating the presence of heat, smoke, other products of combustion or systems malfunctions or security breach within a facility.

alien crosstalk: Unwanted signal coupling from a disturbing pair of a 4-pair channel, permanent link, or component to a disturbed pair of another 4-pair channel, permanent link, or component.

alien far-end crosstalk (AFEXT): The unwanted signal coupling from a disturbing pair of a 4-pair channel, permanent link, or component to a disturbed pair of another 4-pair channel, permanent link, or component, measured at the far end.

alien neared crosstalk (ANEXT): Unwanted signal coupling from a disturbing pair of a 4-pair channel, permanent link, or component to a disturbed pair of another 4-pair channel, permanent link, or component, measured at the near end.

asset: An employee, contractor, or any physical, technological or intellectual possession.

attenuation: The decrease in magnitude of transmission signal strength between points, expressed in dB as the ratio of output to input signal level. See also *insertion loss*.

attenuation to crosstalk ratio, far-end (ACRF): Crosstalk measured at the opposite end from which the disturbing signal is transmitted normalized by the attenuation contribution of the cable or cabling.

availability: (1) the probability that a system or component is operating at a specified time; (2) the ratio of the total time a system or component is functional divided by the length of the time interval for which availability is being determined.

backboard: Backboard generally refers to the A-C rated, fire retardant, plywood sheeting on walls typically for telecommunications facilities. Backboards may also refer to the entire wall-mounted assembly, including wire management and termination frames.

backbone: (1) A facility (e.g., pathway, cable, conductors) between any of the following spaces: telecommunications rooms (TRs), common TRs, floor-serving terminals, entrance facilities, equipment rooms, and common equipment rooms. (2) In a data center, a facility (e.g., pathway, cable, conductors) between any of the following spaces: entrance rooms or spaces, main distribution areas, horizontal distribution areas, and TRs.

backbone cable: See *backbone*.

barrier: A fabricated or natural obstacle used to control access to something, or the movement of people, animals, vehicles or any material-in-motion or the spread of fire.

blanking panel (or filler panel): (1) A panel that may be plastic or finished metal and is not integral to any discrete electronic component or system. (2) A barrier installed in an information technology equipment (ITE) cabinet, rack, or enclosure for maximizing segregation for optimized cooling effectiveness.

bonding: The permanent joining of metallic parts to form an electrically conductive path that will ensure electrical continuity and the capacity to conduct safely any current likely to be imposed.

bonding conductor: An insulated, bare, tinned or untinned copper conductor that puts various exposed conductive parts and extraneous conductive parts at a substantially equal potential especially during normal (non-transient) conditions.

bonding conductor for telecommunications (BCT): A conductor that interconnects the telecommunications bonding infrastructure to the building's service equipment (power) ground.

bonding network (BN): A set of interconnected conductive structures that provides, in varying degrees based upon the design topology and installation, an electromagnetic shield for electronic systems and personnel at frequencies to tens of MHz. NOTE: the term "electromagnetic shield", denotes any structure used to divert, block or impede the passage of electromagnetic energy. In general, a BN need not be connected to ground but all BNs considered in the Standard will have a ground connection. Typical energy sources of concern are lightning, and ac and dc power faults. Of generally lesser concern are quasi steady-state sources such as ac power harmonics, and "function sources" such as clock signals from digital equipment.

building commissioning: In the broadest sense, a process for achieving, verifying, and documenting that the performance of a building and its various systems meet design intent and the owner and occupants' operational needs. The process ideally extends through all phases of a project, from concept to occupancy and operations.

building systems: The architectural, mechanical, electrical, and control system along with their respective subsystems, equipment, and components.

bundled cable: Assembly consists of two or more cables, of the same or different types or categories, continuously bound together to form a single unit.

bus topology: (1) Networking topology, in which each communications device or network has a single connection to a shared medium that serves as the communications channel. Also called a point-to-multipoint topology. (2) A linear configuration where all network devices are connected using a single length of cable. It requires one backbone cable to which all network devices are connected.

cabinet: A container that may enclose connection devices, terminations, apparatus, wiring, and equipment.

cabinet (telecommunications): An enclosure with a hinged cover used for terminating telecommunications cables, wiring and connection devices.

cable: An assembly of one or more insulated conductors or optical fibers, within an enveloping sheath.

cable management: Physical structures attached to and/or within cabinets and racks to provide horizontal and vertical pathways for guiding and managing cabling infrastructure. Similar to pathways as defined in TIA-569-B, horizontal and vertical pathways within cabinets and racks guide cabling infrastructure in an engineered and orderly fashion when connecting to equipment and connectivity housed within the racks and/or cabinets.

cable plant: Cable, raceways, vaults, junction/pull boxes, racks, equipment, patch bays/blocks, and other infrastructure required to provide physical, electrical, optical connectivity between buildings of the owner or between buildings on the owner's property.

cable rack: Hardware designed and manufactured for horizontal pathway distribution of cable and inside wiring inside the MDF, TR, or TR rooms.

cable sheath: A covering over the optical fiber or conductor assembly that may include one or more metallic members, strength members, or jackets.

cable tray: A ladder, trough, spline, solid-bottom, or channel raceway system intended for, but not limited to, the support of telecommunications cable.

cabbling: A combination of all cables, jumpers, cords, and connecting hardware.

campus: A building or collection of buildings located within a limited geographic area – typically one contiguous piece of property.

centralized cabling: A cabling configuration from the work area to a centralized cross-connect using pull through cables, an interconnect, or splice in the telecommunications room.

change of state: A change from the normal operating stance of a system, whether required by maintenance or a failure, resulting from an automatic or a manual response to some form of system input or response.

channel: The end-to-end transmission path between two points at which application-specific equipment is connected.

Class: an abbreviation of Data Center Facility Availability Class - the characteristic uptime performance of one component of the critical IT infrastructure. A quantitative measure of the total uptime needed in a facility without regard to the level of quality required in the IT functions carried on during that uptime. As used in this standard, it applies to scheduled uptime. Class is expressed in terms of one of five Data Center Facility Availability Classes. This classification reflects the interaction between the level of criticality and the availability of operation time.

clean agent: An electrically nonconducting, volatile, or gaseous fire extinguishant that does not leave a residue upon evaporation.

clean agent fire suppression: A fire extinguishing system using a total flooding clean agent.

clear zone: An area separating an outdoor barrier from buildings or any form of natural or fabricated concealment.

client: (1) An internal or external customer. (2) A hardware or software entity, as in “client/server.”

closed transition: A change of state or transfer where the electrical circuit connection is maintained during the transfer. This is also known as “make before break.”

commissioning authority: The qualified person, company or agency that plans, coordinates, and oversees the entire commissioning process. The Commissioning Authority may also be known as the Commissioning Agent.

commissioning plan: The document prepared for each project that describes all aspects of the commissioning process, including schedules, responsibilities, documentation requirements, and functional performance test requirements.

commissioning test plan: The document that details the prefunctional performance test, functional performance test, and the necessary information for carrying out the testing process for each system, piece of equipment, or energy efficiency measure.

common bonding network (CBN): The principal means for effecting bonding and grounding inside a telecommunication building. It is the set of metallic components that are intentionally or incidentally interconnected to form the principal bonding network (BN) in a building. These components include structural steel or reinforcing rods, plumbing, alternating current (ac) power conduit, ac equipment grounding conductors (ACEGs), cable racks and bonding conductors. The CBN always has a mesh topology and is connected to the grounding electrode system.

common equipment room (telecommunications): An enclosed space used for equipment and backbone interconnections for more than one tenant in a building or campus.

common grounding electrode: (1) an electrode in or at a building structure that is used to ground an ac system as well as equipment and/or conductor enclosures. (2) a single electrode connected to separate services, feeders, or branch circuits supplying a building. (3) Two or more grounding electrodes that are bonded together.

compartmentalization: The isolation or segregation of assets from threats using architectural design or countermeasures, including physical barriers.

component redundancy: A configuration designed into a system to increase the likelihood of continuous function despite the failure of a component. Component redundancy is achieved by designing and deploying a secondary component so that it replaces an associated primary component when the primary component fails.

computer room: An architectural space with the primary function is to accommodate data processing equipment.

concurrently maintainable and operable: A configuration where system components may be removed from service for maintenance or may fail in a manner transparent to the load. There will be some form of state change and redundancy will be lost while a component or system is out of commission. This is a prime requirement for a Class F3 facility.

conduit: (1) A raceway of circular cross section. (2) A structure containing one or more ducts.

connecting hardware: A device providing mechanical cable terminations.

connectivity: Patch panels, cabling, connectors, and cable management used to create and maintain electrical and optical circuits.

consolidation point: A location for interconnection between horizontal cables extending from building pathways and horizontal cables extending into furniture pathways.

construction manager: An organization or individual assigned to manage the construction team and various contractors to build and test the building systems for the project.

core layer: the core layer is the high-speed switching backbone of the network. Its primary purpose is to allow the Distribution layer access to critical enterprise computing resources by switching packets as fast as possible.

critical distribution board: A power distribution board that feeds critical loads.

criticality: The relative importance of a function or process as measured by the consequences of its failure or inability to function.

cross-connect: A facility enabling the termination of cable elements and their interconnection or cross-connection.

cross-connection: A connection scheme between cabling runs, subsystems, and equipment using patch cords or jumpers that attach to connecting hardware on each end.

countermeasures: The procedures, technologies, devices or organisms (dogs, humans) put into place to deter, delay or detect damage from a threat.

dark fiber: Unused installed optical fiber cable. When it is carrying a light signal, it is referred to as "lit" fiber.

data center: A building or portion of a building with the primary function to house a computer room and its support areas.

data center infrastructure efficiency (DCIE): An efficiency metric for an entire data center calculated as the reciprocal of PUE: $1/PUE = IT\ equipment\ power/Total\ facility\ power \times 100\%$.

delay skew: The difference in propagation delay between the pair with the highest and the pair with the lowest propagation delay value within the same cable sheath.

demarc: Demarcation point between carrier equipment and customer premises equipment (CPE).

demarcation point: A point where the operational control or ownership changes.

design document: The record that details the design intent.

design intent: Design intent is a detailed technical description of the ideas, concepts, and criteria defined by the building owner to be important

designation strips: Paper or plastic strips, usually contained in a clear or color tinted plastic carrier, designated for insertion into a termination frame. Designation strips are usually imprinted with the adjacent terminal number and are used to aid in locating a specific pair, group of pairs, or information outlet inserted into the termination frame, or for delineating a termination field.

detection, (fire protection): The means of detecting the occurrence of heat, smoke or other particles or products of combustion;

distribution layer: Collection of switches between the core and access layer. Distribution switches may be a switch and external router combination, or a multilayer switch.

domain: A portion of the naming hierarchy tree that refers to general groupings of networks based on organization type or geography.

double ended: A power distribution switchboard with two power source inputs, with an interposing tiebreaker between the sources, where either input source of the switchboard can supply 100% of the load. The double-ended system constitutes an N + 1 or 2N system. This type of system may be used for dual utility systems, a single utility system split into redundant feeds, and may possess the circuit breaker transfer system with the generator.

earthing: See *grounding*.

electromagnetic interference (EMI): Radiated or conducted electromagnetic energy that has an undesirable effect on electronic equipment or signal transmissions.

emergency systems: Those systems legally required and classed as emergency by municipal, state, federal, or other codes, or by any governmental agency having jurisdiction. These systems are intended to automatically supply illumination, power, or both, to designated areas and equipment in the event of failure of the normal supply or in the event of accident to elements of a system intended to supply, distribute, and control power and illumination essential for safety to human life.

energy efficiency measure: Any equipment, system, or control strategy installed in a building for the purpose of reducing energy consumption and enhancing building performance.

entrance conduit: Conduit that connects the outside underground infrastructure with the building's entrance room

entrance facility (telecommunications): An entrance to a building for both public and private network service cables (including wireless), including the entrance point of the building and continuing to the entrance room or space.

entrance point (telecommunications): The point of emergence for telecommunications cabling through an exterior wall, a floor, or from a conduit.

entrance room or space (telecommunications): A space in which the joining of inter or intra building telecommunications backbone facilities takes place.

equipment cable: cord: A cable or cable assembly used to connect equipment to horizontal or backbone cabling.

equipment distribution area: The computer room space occupied by equipment racks or cabinets.

equipment grounding conductor (EGC): The conductive path installed to connect normally non-current carrying metal parts of equipment together and to the system grounded conductor or to the grounding electrode conductor, or both.

equipment room (telecommunications): An environmentally controlled centralized space for telecommunications and data processing equipment with supporting communications connectivity infrastructure.

equipotential bonding: Properly designed and installed electrical connections(s) putting various exposed conductive parts and extraneous conductive parts at a substantially equal potential, especially during normal (non-transient) conditions.

event: Typically, a message generated by a device for informational or error purposes.

failure mode: A system state resulting from an unanticipated system outage and typically an automatic system response to that failure.

Faraday cage: A metallic enclosure that is designed to prevent the entry or escape of electromagnetic fields. An ideal Faraday cage consists of an unbroken perfectly conducting shell. This ideal cannot be achieved in practice but can be approached.

fault tolerant: The attribute of a concurrently maintainable and operable system or facility where redundancy is not lost during failure or maintenance mode of operation.

fiber management: Hardware designed and manufactured for keeping optical fiber patch cords neat and orderly. Most termination frame manufacturers provide optical fiber management components designed to work in conjunction with their termination frames. Fiber management may also refer to other types of hardware for securing optical fiber cable to the building.

fiber optic: See *optical fiber*.

fire: The presence of a flame.

fire detection: The means of detecting the occurrence of heat, smoke or other particles or products of combustion.

fire protection: The active means of detecting and suppressing fires.

fire suppression: The means of extinguishing an active fire.

flexibility: The ability of a design to anticipate future changes in space, communications, power density, or heat rejection — and to respond to these changes without affecting the mission of the critical IT functions.

frame: special purpose equipment mounting structure (for example, IDC blocks, fiber termination hardware not meant to be mounted in standard 19" or 23" racks).

functional performance test: The full range of checks and tests carried out to determine whether all components, subsystems, systems, and interfaces between systems function in accordance with the design documents.

ground: A conducting connection, whether intentional or accidental, between an electrical circuit or equipment and the earth, or to some conducting body that serves in place of earth.

ground fault circuit interrupter (GFCI): A device intended for the protection of personnel that functions to de-energize a circuit or portion thereof within an established period of time when a current to ground exceeds the values established for a Class A device.

grounding: The act of creating a ground.

grounding conductor: A conductor used to connect the grounding electrode to the building's main grounding busbar.

grounding electrode: A conducting object through which a direct connection to earth is established.

grounding electrode conductor (GEC): The conductor used to connect the grounding electrode to the equipment grounding conductor, or to the grounded conductor of the circuit at the service equipment or at the source of a separately derived system.

grounding electrode system: One or more grounding electrodes that are connected together.

grounding equalizer (GE): The conductor that interconnects elements of the telecommunications grounding infrastructure.

hanging load: The weight that can be suspended from the underside of the floor or structure above.

hardening: Protection from physical forces, security breaches, and natural disasters.

heat (fire protection): The existence of temperatures significantly above normal ambient temperatures.

high-order mode transient losses: Losses in optical signal level power caused by the attenuation of weakly guided high-order modes of multimode optical fiber.

high resistance/impedance grounding system: A type of impedance grounded neutral system in which a grounding impedance, usually a resistor, limits the ground-fault current.

horizontal cabling: (1) The cabling between and including the telecommunications outlet/connector and the horizontal cross-connect. (2) The cabling between and including the building automation system outlet or the first mechanical termination of the horizontal connection point and the horizontal cross-connect. (3) in a data center, horizontal cabling is the cabling from the horizontal cross-connect (in the main distribution area or horizontal distribution area) to the outlet in the equipment distribution area or zone distribution area.

horizontal cross-connect (HC): A cross-connect of horizontal cabling to other cabling (e.g., horizontal, backbone, equipment).

horizontal distribution area (HDA): A space in a computer room where a horizontal cross-connect is located, and may include LAN switches, SAN switches, and keyboard/video/mouse (KVM) switches for the end equipment located in the equipment distribution areas.

hot spot: A temperature reading taken at the air intake point of equipment mounted in a rack or cabinet in excess of the design standard or equipment requirement.

human events: Man-made disasters, including economic, general strike, terrorism (ecological, cyber, nuclear, biological, chemical), sabotage, hostage situation, civil unrest, enemy attack, arson, mass hysteria, accidental, special events.

hybrid cable: Assembly consists of two or more cables, of the same or different types or categories, covered by one overall sheath.

identifier: An item of information that links a specific element of the telecommunications infrastructure with its corresponding record.

impact of downtime: Specified as local, regional, or enterprise wide.

incipient products of combustion: Particles emitted from materials developing inherently high heat but from which no smoke is yet visible.

inductive/reactance-grounded power system: method of grounding in which the system is grounded through impedance, the principle element of which is inductive reactance

information technology equipment (ITE) power: The power consumed by ITE to manage, monitor, control, process, store, or route data within the data center, excluding all infrastructure equipment.

infrastructure (telecommunications): A collection of those telecommunications components, excluding equipment, that together provides the basic support for the distribution of all information within a building or campus.

input source transfer: The function of and the location in the electrical system where the transfer occurs between two sources.

insertion loss: The signal loss resulting from the insertion of a component, or link, or channel, between a transmitter and receiver (often referred to as attenuation).

inside plant (ISP): Communications system inside a building (wire, optical fiber, coaxial cable, equipment racks, and information outlets). Telecommunications companies refer to this as inside wire (IW) or intrafacility cabling (IFC).

interconnection: (1) A connection scheme that employs connecting hardware for the direct connection of a cable to another cable without a patch cord or jumper. (2) A type of connection in which single port equipment connections (e.g., 4-pair and optical fiber connectors) attach to horizontal or backbone cabling by means of patch cord or jumper.

intermediate cross-connect: A cross-connect between first level and second level backbone cabling. Also referred to as the horizontal cross-connect (HC).

intersystem bonding conductor: A conductor used in conjunction with an intersystem bonding termination device.

isolated bonding network (IBN): An insulated bonding network in which all associated equipment cabinets, frames racks, trays, pathways and supplementary bonding grids that are designated to be within that IBN are bonded together (such as in a functional system block) that has a single point of connection (SPC) to either the common bonding network or another isolated bonding network. The IBN indirectly augments the CBN via a single point connection. All IBNs considered here will have a connection to ground through the SPC window.

isolation: A design strategy that mitigates the risk of concurrent damage to some components in a facility using physical, logical, or system separation.

jumper: (1) An assembly of twisted pairs without connectors, used to join telecommunications circuits/links at the cross-connect. (2) A length of optical fiber cable with a connector plug on each end. (3) A length of twisted-pair or coaxial cable with connectors attached to each end, also called a patch cord.

label: A piece of paper or other material that is fastened to something and gives predefined information about it. Describes its identity, path, location, or other important information about the product or material.

ladder rack: A cable tray with side stringers and cross members, resembling a ladder, which may support cable either horizontally or vertically.

layering: The use of many layers of barriers, other countermeasures, or a mixture of both, used to provide the maximum level of deterrence and delay.

link: A transmission path between two points, not including terminal equipment, work area cables, and equipment cables.

linkage: A connection between a record and an identifier or between records.

load bank: A device to simulate actual equipment consisting of groups of resistive and/or reactive elements, fans and controls. The load bank is an electrical load that is connected to PDU systems, UPS systems or generators in load test situations.

local distribution point (LDP): (CENELEC EN 50173-5 and ISO/IEC 24764) Connection point in the zone distribution cabling subsystem between a zone distributor and an equipment outlet. Equivalent to the consolidation point (CP) in a zone distribution area (ZDA) in ANSI/TIA-942.

luminaire: An electric light and its components; an electrical lighting fixture.

M13 multiplexer: Consolidates T-1 and E-1 signals into a T-3 or E-3 circuit. A cost-effective device for combining independent T-1s, E-1s, or a combination of the two over the same T-3 or E-3 circuit.

main cross-connect (MC): A cross-connect for first level backbone cables, entrance cables, and equipment cables.

main distribution area (MDA): The space in a computer room where the main cross-connect is located.

main distributor (MD): (CENELEC EN 50173-5 and ISO/IEC 24764) distributor used to make connections between the main distribution cabling subsystem, network access cabling subsystem and cabling subsystems specified in ISO/IEC 11801 or EN 50173-1 and active equipment. Equivalent to the main cross-connect in ANSI/TIA-942.

main electrical grounding busbar (MEGB): The main electrical ground busbar for the building at which electrical service grounding electrode conductor(s) and other grounding and bonding conductors are interconnected to establish the main equipotential location for the building.

maintenance mode: A system state resulting from an anticipated system outage or routine maintenance activity and typically a manual system response to that activity.

management information base (MIB): Within simple network management protocol (SNMP), defines objects and attributes to be managed.

mechanical room: An enclosed space serving the needs of mechanical building systems.

media (telecommunications): Wire, cable, or conductors used for telecommunications.

medium voltage: any electrical voltage above the normal utilized value and below transmission-level system voltages. The utilization voltage varies from country to country. In the US, medium voltage is considered to be between 601 V and 35,000V, where as in the EU or other parts of the world, the utilization voltage level can be significantly higher than in the United States.

meshed bonding network (mesh-BN): A non-insulated bonding network to which all associated equipment cabinets, frames racks, trays, pathways are connected by using a bonding grid. This grid is connected to multiple points to the common bonding network

mission critical: Any operation, activity, process, equipment, or facility that is essential to continuous operation for reasons of business continuity, personnel safety, security, or emergency management

modular jack: A female telecommunications connector that may be keyed or unkeyed and may have 6 or 8 contact positions, but not all the positions need to be equipped with jack contacts.

multimode optical fiber: An optical fiber that carries many paths (modes) of light.

natural barrier: Any object of nature that impedes or prevents access, including mountains, bodies of water, deserts, and swamps.

natural events: Natural disasters, including drought, fire, avalanche, snow/ice/hail, tsunami, windstorm/tropical storm, hurricane/typhoon/cyclone, biological, extreme heat/cold, flood/wind-driven water, earthquake/land shift, volcanic eruption, tornado, landslide/mudslide, dust/sand storm, and lightning storm.

near-end crosstalk (NEXT): (1) The unwanted signal coupling between pairs. It is measured at the end of a cable nearest the point of transmission. Contrast with far-end crosstalk. (2) The signal transfer between circuits at the same (near) end of the cable.

normal mode: The steady-state system configuration while under load.

open transition: A change of state or transfer where the electrical circuit connection is not maintained during the transfer. This is also known as “break before make”.

operational level: Defined for a given facility by assigning one of four levels, according to the amount of time that will be available in the facility for testing and maintenance.

optical fiber: Any filament made of dielectric materials that guides light.

optical fiber cable: An assembly consisting of one or more optical fibers.

outside plant (OSP): Communications system outside of the buildings (typically underground conduit and vaults, exterior/underground, aerial, and buried rated wire and cable).

overall availability range: Defined by combining a given facility's availability requirement "while running" with the operational classification defined for the facility.

panelboard (electrical): A single panel or groups of panel units designed for assembly in the form of a single panel, including buses and automatic overcurrent devices such as fuses or molded-case circuit breakers, accessible only from the front.

patch cord: A length of cable with a plug on one or both ends.

patch panel: A connecting hardware system that facilitates cable termination and cabling administration using patch cords.

pathway: A facility for the placement of telecommunications cable.

performance test: A series of tests for specified equipment or systems, which determine that the systems are installed correctly, start up, and are prepared for the functional performance tests. Often these tests are in a checklist format. The prefunctional test checklists may be completed as part of the normal contractor startup test.

performance verification: The process of determining the ability of the system to function according to the design intent.

permanent link: A test configuration for a link excluding test cords and patch cords.

plenum: A compartment or chamber that forms part of the air distribution system.

power distribution unit (PDU): Sometimes called a computer power center or a power distribution center—a floor- or rack-mounted enclosure for distributing branch circuit electrical power via cables, either overhead or under an access floor, to multiple racks or enclosures of information technology equipment (ITE). A PDU includes one or more distribution panel boards and can include a transformer, monitoring, and controls.

power strip: A device mounted onto or within an information technology equipment (ITE) rack or enclosure, supplied by a single branch circuit, and containing power receptacles into which multiple IT devices can be plugged. A power strip can include metering, controls, circuit protection, filtering, and surge suppression. Also known in IEEE 1100 as a power outlet unit (POU). Sometimes called rack-mount PDU, rack power distribution unit, ITE-PDU, cabinet distribution unit, or plug strip.

power sum alien far-end crosstalk (PSAFEXT): The power sum of the unwanted signal coupling from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components to a disturbed pair of another 4-pair channel, permanent link, or component, measured at the far end.

power sum alien near-end crosstalk (PSANEXT): The power sum of the unwanted signal coupling from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components to a disturbed pair of another 4-pair channel, permanent link, or component, measured at the near end.

power sum attenuation to alien crosstalk ratio at the far end (PSACRF): The difference in dB between the power sum alien far-end crosstalk (PSAFEXT) from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components, and the insertion loss of a disturbed pair in another 4-pair channel, permanent link, or component.

power sum attenuation to crosstalk ratio, far-end (PSACRF): A computation of the unwanted signal coupling from multiple transmitters at the near end into a pair measured at the far end and normalized to the received signal level.

power sum near-end crosstalk (PSNEXT): A computation of the unwanted signal coupling from multiple transmitters at the near end into a pair measured at the near end.

power usage effectiveness (PUE): An efficiency metric for an entire data center calculated as: Total facility power usage/information technology equipment (ITE) power usage.

primary side: The high-voltage side of the electrical power service transformer (above 600V), the electrical power service line side of the UPS, the electrical power service line side of the PDU transformer or the 480V side of the static switch.

private branch exchange (PBX): A private telecommunications switching system.

propagation delay (PD): The time required for a signal to travel from one end of the transmission path to the other end that limits the voltage between the conductors and shield of a cable.

protection, fire: The active means of detecting and suppressing fires occurring within the data processing facility;

psychological barrier: A device, obstacle or lack of obstacle that by its presence alone discourages unauthorized access or penetration.

pull box: A housing located in a pathway run used to facilitate the placing of wire or cables.

quality control: One of the four major strategies for increasing reliability by ensuring that high quality is designed and implemented in the facility, thus reducing the risk of downtime due to new installation failures or premature wear.

raceway: An enclosed channel of metal or nonmetallic materials designed expressly for holding wires or cables. Raceways include, but are not limited to rigid metal conduit, rigid nonmetallic conduit, rigid nonmetallic conduit, intermediate metal conduit, liquid tight flexible conduit, flexible metallic tubing, flexible metal conduit, electrical nonmetallic tubing, electrical metallic tubing, underfloor raceways, cellular, cellular concrete floor raceways, cellular metal floor raceways, surface raceways, wireways, and busways.

rack: An open structure for mounting electrical and/or electronic equipment.

rack unit (U or RU): The modular unit on which panel heights are based. One rack unit is 45 mm (1.75 in).

radio frequency interference (RFI): Electromagnetic interference within the frequency band for radio transmission.

raised floor: See *access floor*.

record drawing: Plan, on paper or electronically, that graphically documents and illustrates the installed infrastructure in a building or portion thereof.

record: Collection of detailed information related to a specific element of the infrastructure.

records: A logical collection of data fields consisting of characters (bytes or bits).

redundancy: Providing secondary components that either become instantly operational or are continuously operational so that the failure of a primary component will not result in mission failure. See also *component redundancy*.

reliability: The probability that a component or system will perform as intended over a given time period.

remote power panel (RPP): power distribution cabinet downstream from a PDU or UPS, typically containing circuits and breakers, without a transformer, located near the load.

report: Presentation of a collection of information from various records.

resistively grounded power system: A method of grounding in which the system is grounded through impedance, the principle element of which is resistance.

return loss: A ratio, expressed in dB, of the power of the outgoing signal to the power of the reflected signal. When the termination (load) impedance does not match (equal) the value of the characteristic impedance of the transmission line, some of the signal energy is reflected back toward the source and is not delivered to the load; this signal loss contributes to the insertion loss of the transmission path and is called return loss.

return on investment (ROI): The ratio of money gained or lost on an investment relative to the amount of money invested.

ring topology: A physical or logical network topology in which nodes are connected in a point-to-point serial fashion in an unbroken circular configuration. Each node receives and retransmits the signal to the next node.

riser: 1. Vertical sections of cable (e.g., changing from underground or direct-buried plant to aerial plant). 2. The space used for cable access between floors.

riser cable: Communications cable that is used to implement backbones located on the same or different floors.

risk: The likelihood that a threat agent will exploit a vulnerability creating physical or technological damage

risk management: The process of identifying risks and developing the strategy and tactics needed to eliminate, mitigate, or manage them.

SAN: Storage Area Network (SAN) is a high-speed network of shared storage devices. A SAN permits storage devices attached to the SAN to be used by servers attached to the SAN.

SCADA system: SCADA is the acronym for "Supervisory Control and Data Acquisition." This is a control system composed of programmable logic controllers (PLCs), data input to the PLCs, custom software, and electrically operated circuit breakers in the distribution gear. All these combine to form a unique system that allows automatic operation and monitoring of the electrical system through control panel workstations.

scan: Scan is a nonintrusive analysis technique that identifies the open ports found on each live network device and collects the associated port banners found as each port is scanned. Each port banner is compared against a table of rules to identify the network device, its operating system, and all potential vulnerabilities.

screen: An element of a cable formed by a shield.

screened twisted-pair (ScTP) cable: A balanced metallic conductor or pair cable with an overall screen.

secondary side: The low-voltage side of the electrical power service transformer, the load side of the UPS, the load side of the PDU transformer or the output side of the static switch.

seismic snubber: Mechanical devices, when anchored to the building structure and placed around vibration-isolated equipment, are intended to limit motion by containing the supported equipment. Snubbers are designed for use in locations subject to earthquakes, high winds, or other external forces that could displace resiliently supported equipment.

separately derived system: A premises wiring system in which power is derived from a source of electric energy or equipment other than a service. Such systems have no direct electrical connection, including a solidly connected grounded circuit conductor, to supply conductors originating in another system.

service gallery: Space adjacent to computer room where electrical and mechanical equipment that supports the computer room may be located.

service provider: The operator of any service that furnishes telecommunications content (transmissions) delivered over access provider facilities.

sheath: See *cable sheath*.

shield: A metallic sheath (usually copper or aluminum), applied over the insulation of a conductor or conductors for the purpose of providing means for reducing electrostatic coupling between the conductors.

shielded twisted-pair (STP) cable: Cable made up of balanced metallic conductor pairs, each pair with an individual shield. The entire structure is then covered with an overall shield or braid and an insulating sheath (cable jacket).

simplicity: The application of irreducible functionality to achieve the intended goal with the corresponding understanding that complexity introduces additional risk.

single-mode optical fiber: An optical fiber that carries only one path (mode) of light.

smoke: Visible products of combustion prior to and concurrent with a fire.

solidly grounded: Connected to ground without inserting any resistor or impedance device.

space (telecommunications): An area used for housing the installation and termination of telecommunications equipment and cabling.

splice: A joining of conductors, meant to be permanent.

star topology: A topology in which telecommunications cables are distributed from a central point.

static switch: Automatic transfer switch capable of electronically sensing power deviations and transferring load conductor connections from one power source to another without interruption of the connected load.

structural barrier: Defined as something that physically deters or prevents unauthorized access, movement, destruction or removal of data center assets.

supplementary bonding grid (SBG): A set of conductors or conductive elements formed into a grid or provided as a conductive plate and becomes part of the bonding network to which it is intentionally attached.

suppression, fire: The means of extinguishing an active fire.

surge protection device (SPD): A protective device for limiting transient voltages by diverting or limiting surge current, has a nonlinear voltage-current characteristic that reduces voltages exceeding the normal safe system levels by a rapid increase in conducted current. Surge protection device is the preferred term. Also called a voltage limiter, overvoltage protector, (surge) arrester, or transient voltage surge suppressor (TVSS).

switch (also switching device): (1) A device designed to close or open, or both, one or more electrical circuits. [IEEE] (2) A mechanical device capable of opening and closing rated electrical current. [IEC] (3) a device for making, breaking, or changing the connections in an electric circuit. (NOTE: a switch may be operated by manual, mechanical, hydraulic, thermal, barometric, or gravitational means, or by electromechanical means not falling with the definition of “relay”.) (4) An electronic device connected between two data lines that can change state between open and closed based upon a digital variable.

switchboard: A single-panel frame or assembly of panels, typically front access, containing electrical disconnects, fuses and/or circuit breakers used to isolate electrical equipment. Switchboards are typically rated 400A to 5,000 A, and are characterized by fixed, group-mounted, molded case or insulated case circuit breakers, but may include draw-out circuit breakers, and usually require work on de-energized equipment only.

switchgear: An electrical enclosure, typically both front and rear access, containing overcurrent protective devices such as fuses and/or circuit breakers used to isolate electrical equipment. Switchgear is typically rated 800A to 5,000A and is characterized by segregated, insulated-case or low-voltage power circuit breakers, usually draw-out, and frequently containing monitoring and controls as well as features to permit addition or removal of switching devices on an energized bus.

switching: (1) The action of opening or closing one or more electrical circuits. (2) the action of changing state between open and closed in data circuits.

system redundancy: Strategy for increasing reliability by providing redundancy at the system level.

targeted availability: A positive expression of allowable maximum annual downtime

technological events: Technological disasters, including hazardous material release, explosion/fire, transportation accident, building/structural collapse, power/utility failure, extreme air pollution, radiological accident, dam/levee failure, fuel/resource shortage, strike, business interruption, financial collapse, and communication failure.

telecommunications: Any transmission, emission, and reception of signs, signals, writings, images, and sounds, that is, information of any nature by cable, radio, optical, or other electromagnetic systems.

telecommunications bonding backbone (TBB): A conductor that interconnects the telecommunications main grounding busbar (TMGB) to the telecommunications grounding busbar (TGB).

telecommunications entrance point: See *entrance point (telecommunications)*.

telecommunications entrance room or space: See *entrance room or space (telecommunications)*.

telecommunications equipment room: See *equipment room (telecommunications)*.

telecommunications infrastructure: See *infrastructure (telecommunications)*.

telecommunications main grounding busbar (TMGB): A busbar placed in a convenient and accessible location and bonded by means of the bonding conductor for telecommunications, to the building service equipment (power) ground.

telecommunications media: See *media (telecommunications)*.

telecommunications room: An enclosed architectural space for housing telecommunications equipment, cable terminations, and cross-connect cabling.

telecommunications space: See *space (telecommunications)*.

termination: The physical connection of a conductor to connecting hardware.

test procedures: The detailed, sequential steps to set the procedures and conditions necessary to test the system functionality.

threats: The agents by which damage, injury, loss, or death can occur. Threats are commonly classified as originating from temperature extremes, liquids, gases, projectiles, organisms, movement, or energy anomalies.

topology: The physical or logical arrangement of a system.

total facility power: The power dedicated solely to the data center, including all infrastructure equipment that supports the information technology equipment (ITE) such as power delivery components, cooling and environmental control system components, computer network and storage nodes, and miscellaneous other components necessary for the operation of the data center.

transfer switch, automatic (ATS): Self-acting equipment for transferring load conductor connections from one power source to another.

transfer switch, nonautomatic: Equipment operated manually and initiated either locally or remotely, for transferring load conductor connections from one power source to another (also commonly referred to as manual transfer switch).

tree topology: A LAN topology that has only one route between any two nodes on the network. The pattern of connections resembles a tree, or the letter T.

trunk cables: Cables bundled together to form a single unit

trunk cabling assemblies: Consist of two or more preconnectorized, cabling links, of the same or different types or categories that may either be covered by one overall sheath or individual units may be continuously bound together to form a single unit.

trunking: Combining (multiplexing) frames from multiple VLANs across a single physical link (trunk) by using an encapsulation protocol such as IEEE 802.1Q. The protocol modifies the frame to identify the originating VLAN before the frame is placed on the trunk. The reverse process occurs at the receiving end of the trunk

uninterruptible power supply (UPS): A system that provides a continuous supply of power to a load, utilizing stored energy when the normal source of energy is not available or is of unacceptable quality, and until the stored energy is all used up or the normal source of power returns to acceptable quality, whichever happens first.

unshielded twisted-pair (UTP): A balanced transmission medium consisting of a pair of electrical conductors twisted to provide a level of immunity to outside electrical interference. Typical construction has four such pairs of conductors contained with a common outer sheath.

uplink: Referring to data processing, a connection between layers (switches) in a hierarchical network. Uplinks are usually fiber optic links configured on Gigabit Ethernet (GE) ports. (Fast Ethernet uplinks can also be configured using optical fiber or balanced twisted-pair cabling). An uplink can be referred to as a "trunk".

UPS, rotary: A UPS consisting of a prime mover (such as an electric motor), a rotating power source (such as an alternator), a stored energy source (such as a battery), associated controls and protective devices, and a means of replenishing the stored energy (such as a rectifier/charger).

UPS, static: A UPS consisting of nonmoving (solid state) components, usually consisting of a rectifier component, an inverter component, a stored energy component, associated controls and protective devices.

uptime: The period of time, usually expressed as a percentage of a year, in which the information technology equipment (ITE) is operational and able to fulfill its mission.

validation: The establishment of documented evidence that will provide a high degree of assurance the system will consistently perform according to the design intent.

verification: The implementation and review of the tests performed to determine if the systems and the interface between systems operates according to the design intent.

virtual local area network (VLAN): Virtual networking allows the overlay of logical topologies onto a separate physical topology. VLANs provide traffic separation and logical network partitioning. A VLAN forms a broadcast domain. To communicate between VLANs a routing function is required.

vulnerability: Defined as a physical, procedural, or technical weakness that creates and opportunity for injury, death, or loss of an asset.

wire: An individual solid or stranded metallic conductor.

wire management: Hardware designed and manufactured for keeping cross-connect wire and patch cables neat and orderly. Wire management may also refer to other types of hardware for securing wire and cable to the building.

wireless: The use of radiated electromagnetic energy (e.g., radio frequency and microwave signals, light) traveling through free space to convey information.

X-O bond: The point in the electrical system where a separately derived ground is generated. This point generates a power carrying neutral conductor or 4th wire for the electrical power system. The X-O bond point is typically used as the ground reference for the downstream power system.

zero U space: Space for mounting accessories in cabinets that does not consume any rack mount spaces, typically between the side panel and the sides of equipment mounted in the rack unit mounting space.

zone distribution area (ZDA): A space in a computer room where a zone outlet or a consolidation point is located

zone distributor (ZD): (CENELEC EN 50173-5 and ISO/IEC 24764) Distributor used to make connections between the main distribution cabling subsystem, zone distribution cabling subsystem, network access cabling subsystem and cabling subsystems specified in ISO/IEC 11801 or EN 50173-1 and active equipment. Equivalent to the horizontal cross-connect (HC) in ANSI/TIA-942.

zone outlet: A connecting device in the zone distribution area terminating the horizontal cable enabling equipment cable connections to the equipment distribution area.

4.2 Acronyms and abbreviations

Abbreviations and acronyms, other than in common usage, are defined below.

A/E	architectural/engineering	EMD	equilibrium mode distribution
AHJ	authority having jurisdiction	EMI	electromagnetic interference
AHU	air handling unit	EMS	energy management system
AISS	automated information storage system	EO	equipment outlet
ASTS	automatic static transfer switch	EPO	emergency power off
ATM	asynchronous transfer mode	ESCON	Enterprise System Connection
ATS	automatic transfer switch	ESD	electrostatic discharge
AWG	American wire gauge	F/UTP	foil screened unshielded twisted-pair
BAS	building automation system	FDDI	fiber distributed data interface
BCT	bonding conductor for telecommunications	FE	Fast Ethernet
BMS	building management system	FICON	fiber connection
BNC	Bayonet Neill-Concelman	GbE	Gigabit Ethernet
CATV	community antenna television	GE	grounding equalizer
CBN	common bonding network	GUI	graphical user interface
CCTV	closed-circuit television	HC	horizontal cross-connect
CD	construction document	HCP	horizontal connection point
CFD	computational fluid dynamics	HDA	horizontal distribution area
CP	consolidation point; critical power	HEPA	high-efficiency particulate air
CPE	customer premises equipment	HVAC	heating, ventilating, and air conditioning
CPU	central processing unit	IBC [®]	International Building Code [®]
CPVC	chlorinated polyvinyl chloride	IBN	isolated bonding network
CRAC	computer room air conditioner; computer room air conditioning	IC	intermediate cross-connect
CRAH	computer room air handler; computer room air handling	IDC	insulation displacement contact
DCIE	data center infrastructure efficiency	IFGC [®]	International Fuel Gas Code [®]
DD	design development	IIM	intelligent infrastructure management
DP	data processing; distribution panel	IMC [®]	International Mechanical Code [®]
DS-1	digital signal level 1	IPC [®]	International Plumbing Code [®]
DS-3	digital signal level 3	IT	information technology
DSX	digital signal cross-connect	ITE	information technology equipment
DWDM	dense wave division multiplexer	KVM	keyboard/video/mouse
E-1	European trunk level 1	LAN	local area network
E-3	European trunk level 3	LDP	local distribution point
EAC	electronic access control	LED	light-emitting diode
EAP	electronic asset program	LSZH	low smoke zero halogen
EDA	equipment distribution area	MC	main cross-connect
EGS	equipment grounding system	MD	main distributor
		MDA	main distribution area
		MERV	minimum efficiency reporting value

Mesh-BN	mesh-bonding network	SPD	surge protection device
MPLS	multiprotocol label switching	STM	synchronous transport module
MTBF	mean time between failures	STP	shielded twisted-pair
MTTR	mean time to repair	STS	static transfer switch
NC	noise criterion	T-1	trunk level 1
NEBS	Network Equipment Building System	T-3	trunk level 3
NEC [®]	National Electrical Code [®]	TBB	telecommunications bonding backbone
NEXT	near-end crosstalk	TGB	telecommunications grounding busbar
NRTL	Nationally Recognized Testing Laboratory	TMGB	telecommunications main grounding busbar
OC	optical carrier	TR	telecommunications room
OLTS	optical loss test set	TVSS	transient voltage surge suppression
OTDR	optical time domain reflectometer	UL [®]	Underwriters Laboratories Inc. [®]
PBX	private branch exchange	UPS	uninterruptible power supply
PC	personal computer	UTP	unshielded twisted-pair
PDU	power distribution unit; protocol data unit	VRLA	valve-regulated lead-acid
PEMCS	power and environmental monitoring and control system	WAN	wide area network
PLC	programmable logic controller	ZD	zone distributor
PM	preventive maintenance	ZDA	zone distribution area
PoE	power over Ethernet		
POU	power outlet unit		
PQM	power quality monitoring		
PUE	power usage effectiveness		
PVC	polyvinyl chloride		
QoS	quality of service		
RAID	redundant array of independent (or inexpensive) disks		
RC	room cooling		
RCI	rack cooling index		
RF	radio frequency		
RFI	radio frequency interference		
RFP	request for proposal		
RH	relative humidity		
RJ48X	registered jack with individual 8-position modular jacks with loopback		
RPP	remote power panel		
SAN	storage area network		
SC	supplemental cooling		
SCADA	supervisory control and data acquisition		
SCSI	small computer system interface		
ScTP	screened twisted-pair		
SD	schematic design		
SDH	synchronous digital hierarchy		
SNMP	simple network management protocol		
SONET	synchronous optical network		

4.3 Units of measurement

The majority of dimensions in this standard are metric. Soft conversions from metric to U.S. customary units are provided in parentheses; e.g., 100 millimeters (4 inches).

Units of measurement used in this standard are defined below.

A	ampere	RU	rack unit
°C	degree Celsius	μm	micrometer
ft ³ /min	cubic foot per minute	V	volt
dB	decibel	VA	volt-ampere
°F	degree Fahrenheit	W/ft ²	watt per square foot
fc	foot-candle	W	watt
ft	foot	W/m ²	watt per square meter
ft/min	foot per minute		
ft/s	foot per second		
Gb/s	gigabit per second		
GHz	gigahertz		
gpd	gallons (U.S.) per day		
gpm	gallons (U.S.) per minute		
Hz	hertz		
in	inch		
in Hg	inches of mercury (pressure)		
in WC	inches of water column		
in WG	inches water gauge		
kb/s	kilobit per second		
kg	kilogram		
kHz	kilohertz		
km	kilometer		
kN	kilonewton		
kPa	kilopascal		
kVA	kilovolt-ampere		
kW	kilowatt		
lb	pound		
lbf	pound-force		
lx	lux		
m	meter		
Mb/s	megabit per second		
MHz	megahertz		
MHz•km	megahertz kilometer		
mm	millimeter		
mph	mile per hour		
m/s	meter per second		
MW	megawatt		
N	newton		
nm	nanometer		
Pa	pascal (pressure)		
psi	pound per square inch (pressure)		

This page intentionally left blank

5 Space planning

5.1 Overall facility capacity

The capacity of a data center is based on the size of the computer room space (floor space available for IT and telecommunications equipment), and the capacity of the power and cooling systems per unit of computer room floor space. High-density data centers have a higher capacity of power and or cooling per unit of computer room floor space.

A balance between space and capacity needs to be determined at the outset when designing a new data center and when modifying an existing data center space. The balance will depend on the type of IT and telecommunications systems the data center is to support and the number/combination of those systems which are to be placed within each cabinet or rack.

When planning for the overall facility:

- design to accommodate a defined load (N) over a defined area.
- consider current and future platforms for servers and storage when identifying the design load and area requirements.
- determine percentages for mainframe high-end processing, mid-range processing, small-form or blade servers, communications networks, and storage.
- identify potential growth rates not only within business units, but also identify growth rates across platforms, as these effect capacity and space plans.

If it is perceived that to meet the performance balance will require delivery of both high levels of power and large amounts of cooling to the cabinet or rack, it may be more cost-effective to design and build a more moderate density data center by designing the data center into a space that can accommodate a larger computer room. Resulting space utilization and power / cooling density limitations should be clearly communicated and documented.

5.2 Power systems

5.2.1 Introduction

The primary considerations when developing the space plan for the power systems are as follows:

- minimizing the distance of electrical feeders between various distribution equipment; excessive distances require increased feeder sizes and additional costs.
- providing sufficient space for the conduit runs with minimal bends; as the routing of the electrical feeders can be very complex in a data center, coordination with all other disciplines is required.
- in power configurations that have redundant systems, dedicated space should be provided for each system to provide physical separation between the systems.

5.2.1.2 Requirements

Sufficient clearances shall be provided for safety, access and maintenance for all electrical equipment, as specified by the manufacturer, applicable codes and standards, and/or the applicable AHJ.

Sufficient access shall be provided to the electrical equipment spaces to remove components or systems for maintenance or replacement, as specified by the manufacturer, applicable codes and standards, and/or the applicable AHJ.

5.2.1.3 Recommendations

Subsystems of the electrical distribution systems (e.g., main switch gear, generator switch gear, UPS and batteries) should be installed in dedicated electrical rooms or located outside of the data center computer room space, separated by a fire-rated wall. See Table 4 regarding fire-rated construction.

The electrical infrastructure for the data center should be isolated and separate from the base building electrical systems if the building is not exclusively dedicated to the data center function.

5.2.1.4 Additional information

The space required for the power systems will be proportional to the required capacity and level of redundancy/reliability of the electrical systems. It is not proportional to the square footage of the computer room alone. For example, a power system for a 1,000 m² (10,000 ft²) computer room with a total critical capacity of 1 MW will require roughly the same physical space as a 500 m² (5,000 ft²) computer room with a total critical capacity of 1 MW.

The following is a partial list of electrical equipment, components and systems that should be included in the space plan:

Equipment typically installed in dedicated electrical rooms outside the main computer area:

- 1) service entrance switchgear (medium or low voltage, metal enclosed, or metal clad);
- 2) unit substation (medium voltage);
- 3) tie breaker section for dual entrance configurations;
- 4) generators (indoor/outdoor);
- 5) generator paralleling switchgear;
- 6) automatic transfer switches (ATS);
- 7) load banks (permanently installed or portable load banks on trailers requiring connection to electrical systems);
- 8) distribution boards (critical loads, noncritical loads, life safety loads);
- 9) transformers;
- 10) uninterruptible power system (UPS—static system or rotary system);
- 11) UPS battery room (static or rotary system with flooded cell batteries);

Equipment typically installed in the computer room spaces:

- 1) power distribution units (PDUs), with or without transformers and static transfer switches depending on the UPS design and load requirements;
- 2) remote power panels (RPPs)—rack or cabinet mounted panels used to provide a concentration of breakers, typically close to the load;
- 3) power strips within each server cabinet that provide power dedicated to the specific cabinet.
- 4) PDU equipment may be located outside the computer room, in adjacent space. The benefit to locating the PDU equipment outside the computer room is that the electrical operations and maintenance activities are outside the critical computer room space.

5.2.2 Electric utility service feeds

5.2.2.1 Single entrance single pathway

5.2.2.1.1 Recommendations

The electric utility service feeds and associated switchgear should be located in a dedicated space that is adjacent or in close proximity to the main data center electrical distribution space.

5.2.2.2 Single entrance/dual pathway

5.2.2.2.1 Recommendations

The electric utility service feeds and associated switchgear should be located in a dedicated space that is equally distanced between or in close proximity to the dual data center electrical distribution spaces.

5.2.2.3 Dual entrance/dual pathway

5.2.2.3.1 Recommendations

The electric utility service feed and associated switchgear should be located in dedicated spaces separate from each other. Utility entrance space A should be located adjacent to electrical distribution space A, and utility entrance space B should be located adjacent to electrical distribution space B.

5.2.3 Generator power

5.2.3.1 Indoor/outdoor installations

5.2.3.1.1 Introduction

Locating the generators either indoors or outdoors is based on site and client specific requirements.

While there may not be a large difference in cost between locating the generators indoors or outdoors, factors to consider during the evaluation of generator location include:

Indoor generators

- placement of indoor generators in an area of the building with the lowest cost per square meter to construct;
- additional costs for items associated with an indoor implementation, such as automated louvers and noise reduction/mitigation;
- requirements for weight, vibration, lateral structure, and fire rating of surrounding surfaces of the space intended for a generator;
- fuel tank capacity and location;
- local and building regulations, codes, or standards.

Outdoor generators

- increased exposure to physical and weather related damage;
- requirements for weight, vibration, lateral structure, and fire rating of surrounding surfaces of the space intended for a generator;
- fuel tank capacity and location;
- local and building regulations, codes, or standards.

5.2.3.1.2 Requirements

Generators installed outdoors shall be installed within shelters.

Generator exhaust systems shall be located so they do not flow into building ventilation air intakes, preferably on the prevailing downwind side from building ventilation air intakes

5.2.3.1.3 Recommendations

It is recommended that generators are installed indoors. With sufficient clearances, indoor generators are easier to monitor and maintain, especially during extreme weather conditions when their operation may be required.

5.2.3.2 Onsite fuel storage

5.2.3.2.1 Introduction

Space planning will need to account for onsite fuel storage. The quantity of fuel that is required and can be stored will be affected by the following:

- proximity of the data center to locations or services which provide fuel replenishment;
- priority status of the organization and response time for fuel replenishment, during regional disasters such as earthquakes, floods and hurricanes;
- criticality of applications, regulatory requirements;
- business drivers requiring self sustaining operations;
- availability of backup or disaster recovery site for applications supported by the data center and expected time required to recover applications at the backup site;
- local codes and acceptance by the AHJ.
- environmental requirements

Storage of large amounts of fuel onsite may trigger extensive jurisdictional and/or environmental permit reviews, and the permitting process may be more stringent for underground storage tanks (UST) than for aboveground storage tanks (AST).

5.2.3.2.2 Recommendations

The minimum amount of generator fuel storage required should be between 8 and 96 hours running at full load depending on the data center availability requirements.

Depending on specific owner needs, the amount of fuel storage required may be far greater than 4 days.

5.2.4 Power distribution

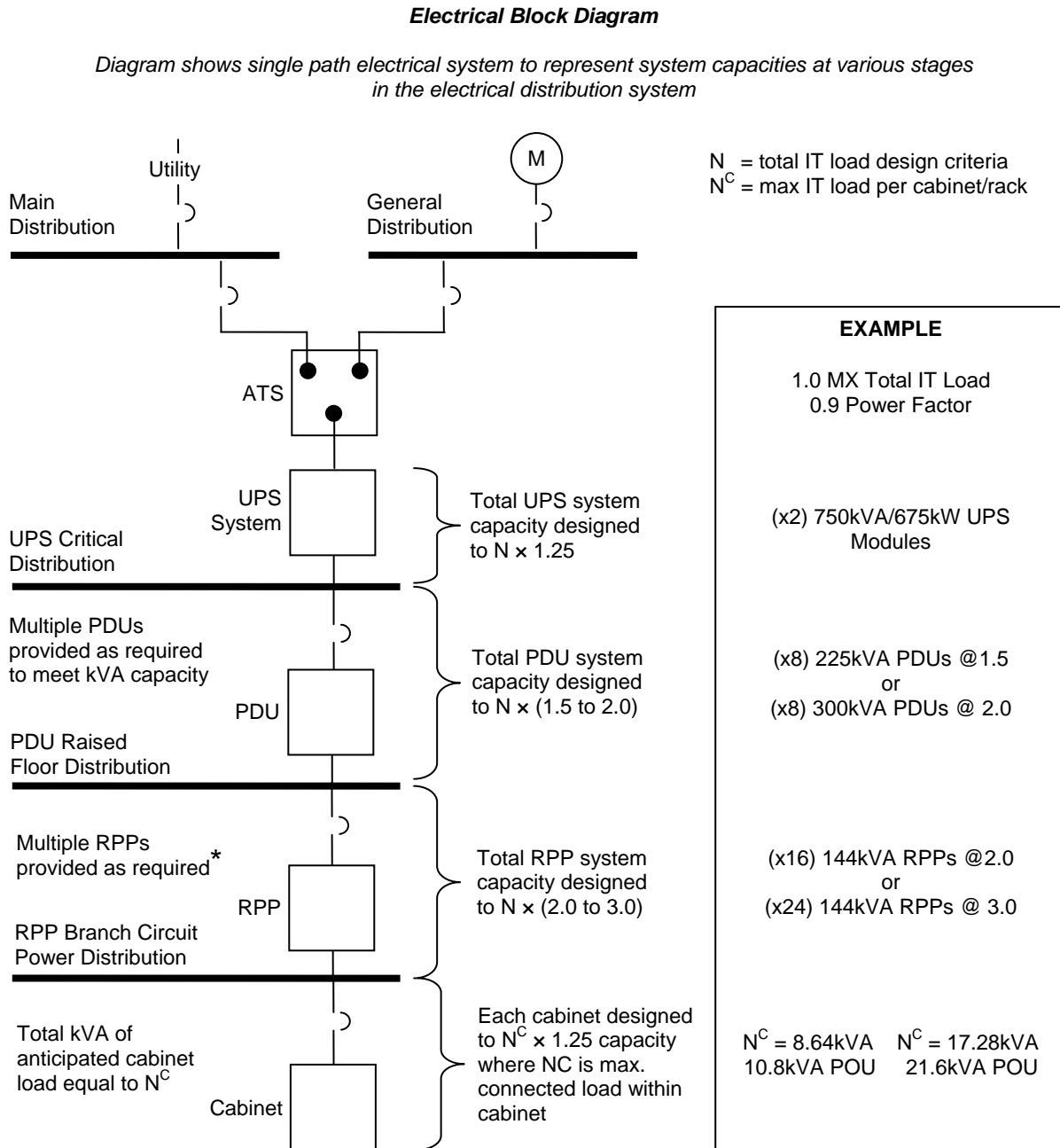
5.2.4.1 Recommendations

Power distribution design should have sufficient flexibility and scalability to allow the load to increase or decrease in any rack, cabinet, or IT equipment zone within acceptable design limits. If the total anticipated data processing load has a capacity criteria of N, the multipliers for each subsystem within the electrical distribution system (as shown in Table 1) will provide sufficient capacity to meet normal equipment layout diversity and scalability, thereby preventing the creation of areas where the power available is insufficient to support the connected load..

Table 1: Multipliers For Electrical Distribution System Components

<i>Distribution system component</i>	<i>Multiplier (N = IT load design criteria)</i>
UPS and UPS critical distribution	N x 1.25
Remote power panels (RPP)	N x 2.0 to 3.0
Power strips (POU)	NC x 1.25
UPS and UPS critical distribution	N x 1.25

Figure 1 shows a single path electrical system to represent system capacities at various stages of the electrical distribution system.



- * Quantity of RPPs is not only dependent on the total IT load "N" but also the:
- 1) layout of the IT equipment, coordinate with number of cabinet rows or equipment zones.
 - 2) capacity of RPPs shall be sized to accommodate total N^C of all IT hardware within rows or zone covered by RPP.
 - 3) number of pole positions required to support quantity of circuits required for IT hardware within rows or zone covered by RPP, pole positions (min.) = 2 x circuits required.

Figure 1: System Capacities At Various Stages Of The Electrical Distribution System

5.3 Cooling capacity

5.3.1 Introduction

The space required to support the cooling systems will vary depending on the type of cooling system selected. Items to consider include:

- central air handlers versus CRAC units,
- chilled water versus air-cooled systems,
- liquid-cooled cabinets in the computer processing area,
- cooling tower (chilled water system),
- thermal storage (chilled water system),
- piping and pumps,
- other required equipment or resources.

5.3.2 Recommendations

Mechanical infrastructure for the data center should be isolated and separate from the base building mechanical systems if the building is not exclusively dedicated to the data center function.

The cooling system design capacity should be sufficient to support the electrical distribution system and subsystem cooling requirements within each rack, cabinet or IT equipment zone.

5.4 Data center supporting spaces

5.4.1 Adjacencies of functional spaces

5.4.1.1 Introduction

The appropriate adjacencies of spaces can be determined by performing an exercise of required staff and material flow. Figure 2 shows an example of staff and material flow through a data center; it is not meant to show the physical adjacencies, but can be used to assist in identifying required adjacencies.

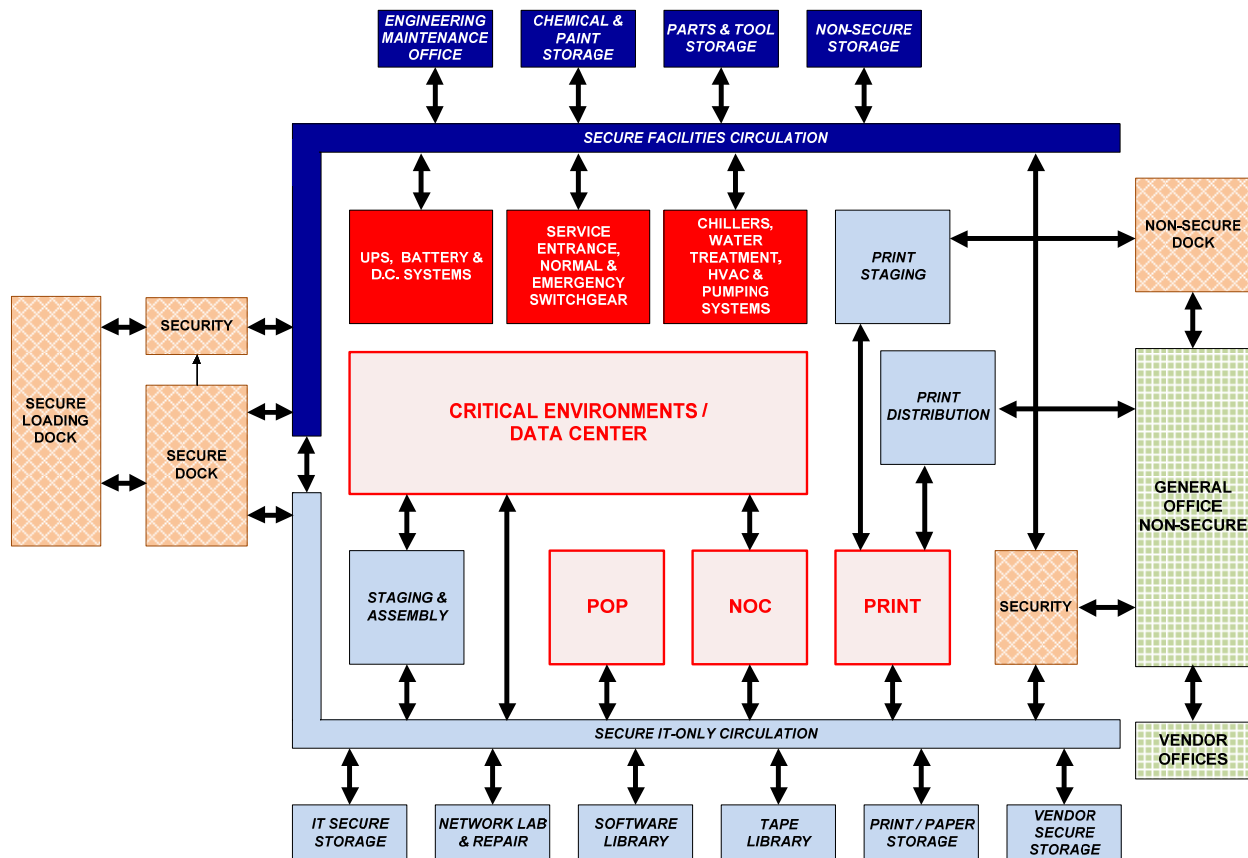


Figure 2: Space Adjacencies

5.4.2 Security

5.4.2.1 Recommendations

Security should be located at or adjacent to the main personnel entrance to facility.

Visitor sign-in area should be physically separate from security operations facility.

The security room should include the security operations facility, including video monitoring and access control system database and front end user interface. When planning this space consider:

- video monitoring space requirements,
- access control system space requirements,
- access control storage requirements,
- unobstructed access to key storage,
- unobstructed access to access-card (temporary and blank) storage;
- fire/smoke alarm monitoring systems.

5.4.3 Telecommunications entrance room

5.4.3.1 Introduction

The function of the entrance room is twofold:

- 1) Provide a secure point where entering media from access providers can be converted from outdoor cable to indoor cable.
- 2) House the access provider-owned equipment such as their demarcation, termination, and provisioning equipment.

5.4.3.2 Location

5.4.3.2.1 Recommendations

The location of the entrance room with respect to the computer room needs to be designed to accommodate the distance limitations of circuits to be provisioned from the entrance room. Where possible, the entrance room should be adjacent to or be in a secured space within the computer room.

Pay particular attention to distance limitations for T-1, T-3, E-1, and E-3 circuits, the type of media these circuits utilize, and the number of DSX panels and patch panels in the channel. See the applicable cabling standard (e.g., ANSI/TIA-942-1 for coaxial circuits) for guidance on the maximum distances allowed for T-3 and E-3 circuits in data centers.

The entrance room with the telecommunications main grounding busbar (TMGB) should be close to the main electrical ground bar to minimize the length of the bonding conductor for telecommunications (BCT), the conductor that interconnects the main electrical ground bar to the TMGB. The BCT shall be sized per applicable standards (e.g., ANSI/NECA/BICSI 607).

5.4.3.3 Access provider considerations

5.4.3.3.1 Recommendations

Where access provision is contracted for the delivery of a service, the access provider's equipment and any associated cabling must be provided with space and the required services. Separate and/or secured cable routes may be required between the entrance room and the access provider's equipment.

Where a separate entrance room is provided, access to the entrance room will be required by both the data center network operations staff and the access provider's technicians. Customer-owned equipment in the entrance room and the computer room should be secure from access provider technicians.

The entrance room may be divided into separate areas to provide separation between access provider-owned and customer-owned equipment. If the room is subdivided, there are typically only two spaces – one for the data center owner and one shared by all access providers. However, if there are multiple access providers, they may each request their own space. These requested spaces may be provided within the same room by using secure fencing, or can be created through the use of walls

Where required by access provision contract, each access provider will terminate its entrance cables and connect its equipment in racks or cabinets separate from the other access providers.

The customer may ask all carriers to place demarcation equipment (patch panels, DSX panels, and IDC blocks) in shared meet-me or demarcation racks. Consolidating all patching to carrier circuits into meet-me racks and locating patch panels for cabling to the computer room in the same racks or adjacent ones simplifies cabling in the entrance room. Placing the demarcation panels and blocks adjacent to the patch panels that support cabling to the computer room allows circuits to be cross connected to the computer room cabling system using short patch cords.

The entrance room should be sized to accommodate each anticipated access provider. The designer should meet with each carrier to determine its space requirements before sizing the entrance rooms. Additionally rack and cabinet space will be required for customer-owned equipment and termination of cabling to the computer room and rest of the building.

Carrier equipment included in the entrance room consists of carrier-owned patch panels, digital cross-connect (DSX) panels, routers, SONET, DWDM, and circuit provisioning equipment. The power requirement for the entrance room typically ranges from 500 to 1500 watts per access provider. However, the designer should meet with each access provider to determine its electrical, space, interface, and other facility requirements.

5.4.4 Operations center

5.4.4.1 Recommendations

The telecommunications room (TR) that supports the operations center and other nearby data center support spaces should be outside the computer room.

The work area communications devices within the operations center may need connectivity back to two different supporting cross-connect fields. Network monitoring may need connectivity directly to the core network hardware located in the MDA space. Corporate LAN and telephony will need connectivity to the general telecommunications cross-connect serving noncomputer room communications.

Some applications may require installation of large video displays easily visible to all operations center personnel.

Depending on the data center, there may be need for CATV systems (local cable provider and satellite service).

5.4.5 Helpdesk

5.4.5.1 Recommendations

The helpdesk does not need to be located near the computer room and may be integrated into the general office space adjoining the data center. Additionally, it may be acceptable to build helpdesk and other general office space in a different building, when there is no need for its location within the hardened portion of the data center facility.

Operator workstations for the helpdesk should be provided with critical electrical circuits fed from the backup generator and UPS systems to ensure that support functions are not disrupted by power fluctuations or blackouts.

5.4.6 Print

5.4.6.1 Recommendations

Printers should be located within a dedicated print room separate from the main computer room. The print room should have its own dedicated air handling system.

Power and cooling systems supporting the print functions should be considered critical, and supported by the backup generator and UPS systems.

Both a separate paper storage room near the print room and a suitable route from loading dock to print room and paper storage room, to facilitate pallets of bulk paper products, should be provided. Ensure that printer manufacturers' environmental criteria are included in the design parameters of the facility. Typical environmental parameters that are unique for a print room are humidity and temperature.

5.4.7 Loading dock

5.4.7.1 Recommendations

Location of the loading dock should provide a step free route through to the computer spaces with sufficient floor loading capacity to withstand material and equipment weights.

A non-secure loading dock should be provided for general building deliveries.

For all high-value equipment, a secure loading dock should be provided. Some considerations when planning a secure loading dock include:

- provision of an enclosed area for the delivery truck to protect deliveries from extreme weather;
- use of a dock leveler so that equipment can be safely moved from any type of delivery truck;
- monitoring of the area by the building CCTV security system, with preference for security guards from the building's guard station to be able to visually monitor all activity;
- Controlling access to the loading dock by the facility access control system, with the system able to generate a history of all access attempts.

5.4.8 Storage

5.4.8.1 Secured high value

5.4.8.1.1 Recommendations

A secured storage area for high-value equipment should be located adjacent to a secured loading dock.

The space required for secured high-value storage is recommended to be a ratio of 1:10 in comparison to the computer room space. The minimum space recommended is 23 m² (250 ft²). The ratio may be reduced for large data centers depending on the specific operational practices.

The secured storage area should be monitored by the building CCTV security system and/or access controlled by the facility access control system. The system should generate a history of all access attempts.

5.4.8.2 Staging

5.4.8.2.1 Recommendations

All storage and unpacking activities should occur outside the computer room space, either in storage rooms or in staging areas. Preferably, a staging area should be located adjacent to the computer room. For high-value equipment, a staging area should be provided for unpacking, and should be separate from any test-bench or lab space.

A staging area should have an air conditioning system separate from the computer room, as cardboard boxes and packing materials can generate large amounts of particulates

Due to limited space within a lab, the staging area may be used to test and burn-in equipment for larger mainframe or high-end servers space. However, this should not be a regular occurrence and alternatives should be considered.

The staging area should be monitored by the building CCTV security system and/or access controlled by the facility access control system. The system should generate a history of all access attempts.

5.4.8.3 Vendor storage

5.4.8.3.1 Recommendations

A secured storage area should be provided for vendors' equipment. The space needed depends on the number and type of vendors that will be storing equipment onsite.

The vendor storage area should be monitored by the building CCTV security system and/or located near or adjacent to a secured loading dock.

The security requirements for vendor storage should be the same as the staging area.

5.4.8.4 Print storage

5.4.8.4.1 Recommendations

Print storage may be located adjacent either to a loading dock or preferably, the print room.

5.4.9 Engineering offices

5.4.9.1 Recommendations

The engineering offices should be located near the electrical switchgear, UPS, generator, chiller and HVAC rooms, with sufficient space provided for power and cooling engineers and support staff

For offices, at least 10 m² (100 ft²) of office floor space should be provided with sufficient noise baffling from adjacent equipment rooms to meet ASHRAE NC rating of not more than 35.

5.4.10 Administrative

5.4.10.1 Recommendations

The administrative or general office space may not require the same level of detailed construction as the data center and supporting back-of-house areas.

Factors affecting administrative space requirements include:

- disaster recovery and business continuity plans;
 - operational policy during extreme weather conditions
- Example: the facility and have only minimal required staff to ensure the data center remains operational, allowing administrative and general office space to be constructed to standard office design criteria
- future administrative space requirements, either as an expansion to the overall data center or as a stand-alone project
 - special function rooms, such as a large conference or “war room” with wall-to-wall, floor-to-ceiling white boards

5.4.11 Waste/recycle

5.4.11.1 Recommendations

As these facilities generate a large amount of boxes, packing material, and other waste, adequate space should be allocated for its handling. Frequency of removal, fire prevention/protection, local AHJ requirements, and dumpster requirements, such as size, access, and location, should also be considered.

Recycling and/or compliance with local environmental initiatives (e.g., United States Green Building Council [USGBC], Leadership in Energy and Environmental Design [LEED], Building Research Establishment Environmental Assessment Method [BREEAM]) is recommended.

5.5 Non-IT equipment on access floor

5.5.1 Cooling

5.5.1.1 Floor vents/perforated tiles

5.5.1.1.1 Recommendations

While the exact locations of the required floor vents or perforated tiles are not typically known at the time the construction documents are issued for the flooring system, the general layout and approximate locations should be identified. The HVAC designer should coordinate the anticipated quantities with the technology consultant or end user and ensure that the construction documents require the appropriate number and type of cutouts for floor vents and quantity of perforated floor tiles. The exact locations can be validated prior to installation of the flooring system.

It is recommended that a computational fluid dynamics (CFD) model of the floor design be produced to ensure proper placement of floor tiles and that the cooling design will meet the design requirements.

Tile cutouts should have a means of restricting airflow for cutouts that are not fully populated with cabling. Open cutouts can cause more than 50% of the air supplied by the air handlers or CRAC units to bypass the perforated tiles.

The location of the tile cutouts and perforated tiles need to be coordinated with the specific design of the equipment racks and cabinets. Open frame racks should have the floor cutouts positioned directly below the back half of the vertical cable management between each rack. Cabinets should have the floor cutouts positioned below the vertical channel that will be used for power and communications cabling within the cabinet.

When placing floor cutouts below open rack vertical cable managers, ensure that the grommet system used does not protrude above the access floor and interfere with proper installation and leveling of the vertical cable managers and racks.

Consider positioning cabinets with the front or back edges aligned with the edge of the floor tiles. The adjacent clear floor tile can then be removed without interference from the rack or cabinet.

Do not install perforated floor tiles until they are required. The efficiency and performance of the air distribution system will be affected by additional perforated floor tiles.

5.5.1.2 Ducting

5.5.1.2.1 Recommendations

Ducting may be required, particularly for computer rooms without access floors.

5.5.1.3 Air-handling units

5.5.1.3.1 Recommendations

The exact location of the air-handling units should be coordinated with the mechanical engineer, technology consultant and/or end user to ensure that an optimal equipment layout can be determined without hindering airflow requirements or utilization of floor space.

If air handlers are required to be located within the computer room area due to the size and density of the data center, coordination is required to ensure that the technology equipment layout and/or low-voltage cable routing is not constrained.

5.5.2 Power distribution

5.5.2.1 Remote power panels (RPP)

5.5.2.1.1 Recommendations

RPP locations should be coordinated with the technology equipment layout. The preferred RPP configuration is to place the RPPs at one or both ends of equipment cabinet rows.

5.5.2.2 PDU placement

5.5.2.2.1 Recommendations

The preferred location for PDUs is in a service gallery (a space outside but adjacent to the computer room). This location is subject to the approval by the AHJ and if the feeder distances to the remote power panels allow such a placement. Security for this space should be the same as for other critical electrical and mechanical spaces.

NOTE: This is the preferred approach because it removes a maintenance item from the computer room, removes a source of heat (if provided with transformers), and allows the PDUs to be located in less expensive space.

5.5.3 Fire protection systems

5.5.3.1 General

Space for fire protection system detection and protection equipment in the data center space should be coordinated with the fire protection system engineer.

Sufficient aisle space should be provided and coordinated with ceiling mounted fire detection and protection devices. Ceiling heights that are in excess of 3.7 m (12 ft) may require additional aisle space to maneuver support lifts in the computer room.

For computer rooms with an access floor, the placement of fire detection and protection devices which are installed below the access floor (including sprinkler or gaseous suppression piping and tanks) should be coordinated with all power and communications underfloor pathways and placement of technology equipment situated on the access floor.

For automatic protection information, See Section 11, as well as NFPA 75, NFPA 76, and AHJ requirements for additional information.

Manual fire extinguishing methods include handheld extinguishers and fire blankets. See Section 11 and NFPA 75 for additional information on manual methods.

5.6 Information technology equipment placement in a computer room with an access floor

5.6.1 Telecommunications spaces

NOTE: See Section 14.2 and ANSI/TIA-942 for more information on telecommunications spaces.

5.6.1.1 Introduction

The computer room will support one or two main distribution areas (MDA) and can support several horizontal distribution areas (HDAs). Some computer rooms require only a single MDA, however a second MDA is often deployed to provide redundancy.

The main distribution area will support the main cross-connect for the computer room, network equipment for the computer room (e.g., core routers, core LAN switches, core SAN switches, firewalls), and can support a horizontal cross-connect for portions of the computer room near the MDA.

The horizontal distribution areas support horizontal cabling to equipment areas (e.g., server cabinets) and LAN, SAN, console, or KVM (keyboard/video/mouse) or other edge switches.

The entrance rooms, MDAs, and HDAs need to be carefully situated to ensure that maximum cable lengths for applications to be used in the data center are not exceeded (e.g., WAN circuits, LAN, SAN).

Whereas a small data center may only have an MDA and no HDAs, TRs, or entrance room, a large data center may require multiple entrance rooms to be able to provision circuits in all locations of the data center.

Larger data centers will require more HDAs not only to ensure that maximum horizontal cable lengths are not exceeded, but also to avoid cable congestion. HDAs should not be so large as to completely fill all raceways feeding the HDAs during initial occupancy. Due to the high density of cabling in data centers, HDAs are more often required in data centers to avoid cable congestion than to avoid maximum cable length restrictions.

5.6.1.2 Recommendations

If the computer room has two MDAs, they should be physically separated. It may not necessary to place the MDAs on opposite ends of the computer room, if such a configuration causes cable lengths for distance-limited applications, such as T-1, T-3, E-1, E-3, and SANs, to be exceeded.

5.6.2 Racks, frames, and equipment

NOTE: Section 14.3 contains additional information regarding racks and cabinets.

5.6.2.1 Rack unit capacity

5.6.2.1.1 Recommendations

The amount of IT equipment (ITE) that should be placed within a cabinet will depend on many factors that vary for each hardware platform, data center, and organization. For example, each organization has its own practices for populating cabinets, and some may prefer not to install servers in all positions, leaving room for patch panels or switches, or for ease of maintenance.

ITE implementation planning should consider occupying cabinets based upon:

- Platforms (e.g., appliance servers, mid-range, blade servers).
- Departments, independent of platforms.
- Occupancy to the desired density independent of platform or departments.

Adequate space should be allocated for patch panels, switches, power strips, and cabling for the cabinet when it is at its desired maximum capacity. Patch panels and power strips should not be placed directly behind servers, as this may impede access and airflow to the rear of these systems.

The availability of power and cooling, rather than space, may limit the amount of ITE per cabinet or rack. As equipment power densities continue to increase, it is recommended to design the data center so that space constraints are realized before power and cooling constraints.

To ensure that the initial and ultimate power and cooling system capacities will meet the anticipated demands, validate power consumptions either by performing measurements or by obtaining actual power consumption data from manufacturers.

Any unused rack space should be filled with blanking devices to reduce any nonfunctional airflow migration through the equipment rack.

Initial and ultimate system weight loads should be used when verifying the structural design parameters of the various platforms that will be installed within the computer room.

5.6.2.2 Network racks

5.6.2.2.1 Recommendations

When arranging the computer room space and organizing the hot/cold aisle locations with respect to the cabling and cabinets, consider future changes. For example, it may be desirable to locate the cabinets or racks in which cabling is terminated in the hot aisle, so that a hot and/or cold aisle containment system may be installed in the future.

If redundant network equipment is located in equipment racks that are physically separated, these network racks should be separated to ensure facility infrastructure (power, cooling) diversity. This also provides physical separation of the cabling pathways and cabling from the redundant network equipment to the servers that are connected.

The areas in the computer room where the entrance rooms, MDAs, and HDAs are located may be secured with caging. This may be an end user requirement, dependent on internal operating procedures and security requirements.

5.6.2.3 End equipment cabinets and racks

5.6.2.3.1 Requirements

For new installations, a preliminary layout of the equipment cabinets and racks shall be completed prior to establishing the reference point for the access floor grid in computer rooms, entrance rooms, and TRs. The preliminary layout should anticipate logical groupings of equipment, flush front alignment of equipment rows, heat and energy density proximity to ducting and cooling, and worst-case cabinet depth.

The required clearances for the equipment cabinets, access floor grid, and internal columns will determine where the front alignments of rows of cabinets and racks are best located. The access floor grid shall line-up with the preferred layout of the rows of cabinets and allow for easy removal of tiles. Rear access (or hot aisle width when deployed in hot aisle/cold aisle arrangement) must allow for minimum service clearance appropriate to the voltage of the equipment per applicable local codes and regulations. Because all equipment may not be known at the time of initial layout, a final layout with adjustments may be required after the access floor grid has been established.

For existing installations, the access floor grid has already been determined. An equipment layout and alignments shall be made with the same considerations as in the previous paragraph, based upon the existing floor grid.

5.6.2.3.2 Recommendations

High density of servers within cabinets, higher density port counts per server, and the number of power cords per server create significant cable and cooling management issues within the server cabinets, particularly those with a 600 mm (24 in) width. Since most blade server chassis and emergent storage and rack-mounted server chassis are

more than 800 mm (32 in) deep, cabinets should be 1200 mm (48 in) deep. This also provides adequate space to install redundant power strips and vertical cable management in the back of the cabinets. Prior to committing to a standard server cabinet size, the end users should review, and have the vendors provide mock-ups of, the various server cabinet configurations that they will implement. A mock-up of the worst-case configuration with maximum number of anticipated servers and cabling should also be provided. Upon completion of the mock-up, power and heat loads should be recalculated to ensure adequate power and cooling are delivered to the cabinet.

Additional room for cable management can be gained by increasing the depth or width of the cabinet. However, increasing the width of the cabinets will reduce the number of cabinets that can be installed in the computer room.

When equipment cabinets or racks are installed adjacent to each other, thus forming a continuous aisle, the number of cabinets or racks within one row should not exceed twenty. Where one end of an aisle is closed off or has no personnel exit, the number of cabinets and racks within one row should not exceed ten racks/cabinets. There may be AHJ restrictions on the length of an aisle, which will take precedence over these guidelines.

The layout of the computer equipment, electrical equipment, and air conditioning equipment should be done concurrently. One recommended method is to place the RPPs on the ends of the server cabinet rows.

Cabinets and racks should be placed to permit access floor tiles in front and in back to be lifted. It is a good practice to align one edge of the cabinets flush with one edge of the floor tiles, preferably the front edge to maximize cold aisle airflow by leaving at least two tile positions for perforated tiles.

In hot/cold aisle floor layouts, there should not be any gaps in the cabinet row. All gaps should be eliminated to minimize hot air migration into the cold aisle.

5.6.2.4 Large frame servers

5.6.2.4.1 Requirements

The layout of the large frame servers shall be coordinated with respect to weight loads, cooling airflow, power and connectivity requirements, as they will not fit within the standard server cabinet space.

5.6.2.5 SAN equipment

5.6.2.5.1 Requirements

The layout of the SAN equipment shall be coordinated with respect to weight loads, cooling airflow, power and network connectivity requirements, as they may not fit within the standard server cabinet space.

5.6.2.5.2 Additional information

Some SAN implementations require centralization of SAN storage and switches. Other SAN implementations use core-edge SAN architecture with core switches in the MDA and edge switches in the HDA.

5.6.2.6 SAN frames

5.6.2.6.1 Recommendations

SAN frames are network racks that provide the infrastructure to terminate the media that provide connectivity to the servers. SAN frames should be located within the SAN equipment area and typically consist of large quantities of high-density optical fiber termination panels.

The SAN frames need to provide proper optical fiber cable management to facilitate the interconnects from the patch panels to the SAN equipment.

Where the SAN frames consist of fabric core switches and edge layer switches, the edge layer switches and core switches should be installed in separate racks because the number of edge switches may increase. In addition, the amount of moves, adds, and changes at the edge layer is typically much higher than at the core layer.

5.6.3 Aisles

5.6.3.1 Orientation

5.6.3.1.1 Recommendations

For rectangular computer rooms, equipment rows may be run parallel or perpendicular to the long walls. The optimum configuration should be determined by examining both options.

5.6.3.2 Clearances

5.6.3.2.1 Requirements

The minimum width of an aisle shall be 0.9 m (3 ft), depending on local code requirements and voltage level present in cabinet.

5.6.3.2.2 Recommendations

There should be at least a 1.2 m (4 ft) clearance at the front of racks and cabinets to permit unobstructed access, equipment movement, and maintenance.

Aisle widths may need to be 3 or 4 tiles depending on HVAC engineer's analysis, requirements for planned equipment, and the design of the cooling system.

As equipment is typically installed within cabinets from the front, the front aisle width should, at a minimum, be equal the greatest value of the following:

- the anticipated depth of equipment to be installed within the cabinets;
- the current or planned cabinet depth to permit replacement of cabinets;
- the width required by local code(s) requirements and/or the AHJ;
- 0.9 m (3 ft).

NOTE: Additional allowance should be provided if moving equipment (e.g., hand truck) will be used

Clearance in front of racks and patching frames should provide for safe access and clearance to work. When the swing of a door encounters an obstruction such as a building support column, double (wardrobe) doors may be considered in place of a single door to facilitate full access to the cabinet content.

If the end user has an environment that changes equipment between server cabinets and floor standing equipment frequently, it may be desirable to designate two rows of floor tiles for equipment and two rows of floor tiles for aisles (both hot and cold). This will reduce the floor space utilization of the computer room, but will provide the flexibility that this particular environment requires.

5.6.3.3 Hot/cold aisles

5.6.3.3.1 Recommendations

The front of the racks and cabinets should be oriented toward the cold aisle. The cold aisle should have at least two rows of floor tiles that can be configured with perforated tiles, providing the required flexibility in airflow management. Additional front (cold) aisle clearance may be required subject to HVAC and operational considerations.

A minimum of least two complete rows of floor tiles that can be removed in the hot aisles at the rear of the cabinets and racks should be provided. This allows the designer to make use of two rather than one row of tiles for cable trays.

With 1100 mm (42 in) deep server cabinets and the front of the cabinets aligned with the edge of a 600 x 600 mm (24 in x 24 in) floor tile in the cold aisle, there would be 100 mm (4 in) of under lap provided in the hot aisle, which would necessitate two further rows of floor tiles that can be removed. (See Figure 3)

If cabinets or equipment have a depth that is greater than 1.1 m (42 in), there will need to be coordination with the hot and cold aisle configuration to ensure that the required clearances are provided.

5.6.3.4 Location

5.6.3.4.1 Recommendations

The equipment cabinets and racks should have a minimum of 1.2 m (4 ft) and preferably 1.8 m (6 ft) of clearance from the server cabinets to air conditioning equipment and power distribution equipment along the perimeter wall. This provides a large aisle for the movement of large equipment such as electrical distribution equipment and air conditioning equipment within the computer room.

In the more traditional model, air conditioning equipment and power distribution equipment are placed along the perimeter walls for distribution under raised, perforated tiles. When subfloor air distribution is used, there should be a minimum of 1.2 m (4 ft) and, preferably, 1.8 m (6 ft) of clearance between the server cabinets and the air conditioning equipment. The cold aisle should be a minimum of 2.4 m (8 ft) from the cooling units. This will help reduce the possibility of the effect in which air is drawn from above the access floor through the perforated floor tile

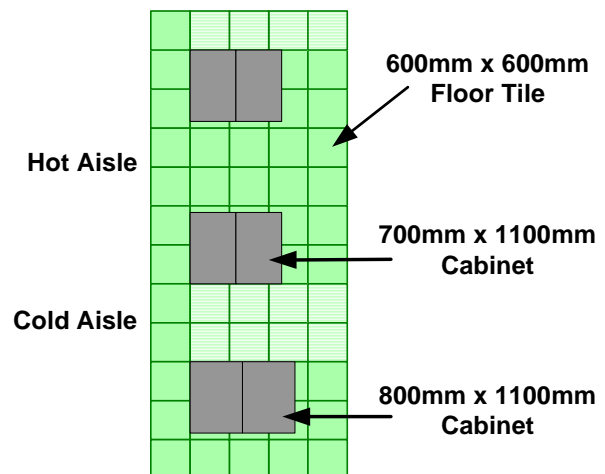


Figure 3: Examples Of Aisle Width With Different Cabinet Sizes

due to low pressure caused by the high-velocity air below the floor near the discharge of the air conditioning equipment. These distances are dependent on mechanical considerations such as the depth of the access floor, the absence or presence of turning vanes on the discharge of the CRAC unit, the speed of the air discharge, or the deployment of fans that are recessed under the access floor. Equipment cabinet and server row lengths may be limited by the maximum distance that the air conditioning equipment can provide adequate air pressure for delivering cold air. This distance is a function of the CRAC unit blower, the access floor depth, and the distribution of the perforated tiles.

When overhead or in-row cooling is provided, the CRAC units should be close coupled to the racks to be cooled, meaning that the cooling equipment should be as close as possible to the heat source. Close coupling minimizes hot and cold air mixing and improves efficiency because it minimizes the volume of air that must be cooled.

5.6.4 Power and telecommunications cable distribution

5.6.4.1 Introduction

Various configurations can be used to distribute power and telecommunications cables. See Section 14.4.8 for considerations of overhead versus under-floor cable routing.

5.6.4.2 Requirements

A telecommunications cable pathway (such as cable trays or other containment) shall contain a maximum depth of cable of 150 mm (6 in) when fully populated.

The bottom of the access floor tiles shall be:

- a minimum of 50 mm (2 in) from the top of the cable tray (if cables exit the cable tray from the top of the tray)
- a minimum of 200 mm (8 in) from the bottom of the cable tray if the cable tray is expected to be filled to the capacity of 150 mm (6 in) depth.

Cable pathways shall meet the clearance requirements of fire detection, suppression, and prevention systems, and these systems must be coordinated with other systems (e.g., electrical, mechanical, telecommunications) and meet the requirements of the manufacturer and the AHJ.

5.6.4.3 Recommendations

Raceways should be sized for the maximum number of cable expected, with a 50% additional capacity to allow for future growth. Raceway size should be calculated in areas of maximum density, such as near MDAs and HDAs.

Where fiber optic cabling is installed under the floor, it should be protected from damage by placing it within a cable tray or other containment. There is no separation requirement between power and fiber optic cabling, except that which is required by the AHJ.

If both power and telecommunications cabling are distributed from below the access floor then:

- the power cabling should be routed either adjacent to or within the cold aisle;
- the telecommunications cabling should be routed adjacent to or within the hot aisle.

This ensures that the telecommunications cabling does not interfere with airflow in the cold aisles.

If both power and fiber optic telecommunications cabling are distributed from overhead and copper telecommunications cabling is distributed from below the access floor then:

- the fiber optic telecommunications cabling should be routed above the power cabling on separate containment, and should be coordinated with mechanical and electrical systems above the cabinets;
- the copper telecommunications cabling should be routed adjacent to or within the hot aisles.

Power and communication pathways should be positioned at different heights off the floor so that they can cross each other without interference. Alternatively, at every point where the power and copper cabling cross the path of each other, the crossing should be at a right (90 degree) angle.

5.6.4.4 Additional information

Patch cabling within a row of cabinets and racks is often routed overhead to maximize space underfloor for horizontal and backbone cabling. This routing also separates patch cabling, which changes often, from horizontal and backbone cabling, which should be more permanent.

The data cabling standards used in the design provide guidance as to the recommended separation between power and copper telecommunications cabling to maintain signal integrity (e.g., ANSI/TIA-942, CENELEC EN 50174-2, ISO/IEC 14763-2). Separation and segregation for safety shall be in accordance with the requirements of the AHJ.

5.6.5 Airflow circulation and equipment placement coordination

5.6.5.1 Recommendations

Consider the following items when coordinating placement of equipment, airflow, and cable routes:

On-floor equipment:

- Equipment type and dimensions
- Orientation with respect to airflow direction

Underfloor services:

- Electrical services:
 - Dimensions and clearances
 - Orientation with respect to airflow direction
- Data cabling:
 - Dimensions and clearances
 - Orientation with respect to airflow direction
- Ducting:
 - Dimensions and clearances
 - Orientation with respect to airflow direction
- Fire suppression system:
 - Dimensions and clearances
 - Orientation with respect to airflow direction
- Fire detection system:
 - Dimensions and clearances
 - Orientation with respect to airflow direction
- Air conditioning pipes:
 - Dimensions and clearances
 - Orientation with respect to airflow direction

5.6.6 Information technology (IT) equipment adjacencies

5.6.6.1 Proximity to EMI and RFI energies

5.6.6.1.1 Recommendations

Where possible, exposure to sources of EMI and RFI should be avoided. Transformers, other than those in PDUs, should be placed a minimum of 600 mm (24 in), and preferably at least 1.2 m (4 ft) from ITE and data cabling.

5.6.6.2 Information technology equipment (ITE) access space requirements

5.6.6.2.1 Recommendations

The equipment access space for ITE and non-ITE should be coordinated so that access space can be shared whenever possible, maximizing computer room utilization.

5.6.7 Access floor grid layout and reference point

5.6.7.1 Recommendations

The access floor reference point should be coordinated with the technology equipment layout, PDUs, CRAHs, chilled water piping and associated valving.

The reference point should not be selected simply at one of the corners of the computer room without coordinating the placement of the technology equipment. While having the reference point at one of the corners is the most cost effective from an installation cost perspective as it results in the fewest partial floor tiles, it may not provide the most optimized technology layout. The best long-term solution may be to position the reference point some distance away from a corner to accommodate the maximum number of server cabinet rows while still maintaining the required clearances.

5.7 Network architecture

Network architecture considerations include:

- centralized/decentralized location and its impact on space planning;
- copper communications cabling distance limitations and their impact on space planning;
- optical fiber distance limitations and their impact on space planning.

6 Site selection

6.1 Introduction

This section outlines the considerations that should be reviewed and provides recommendations when selecting a location for a data center, whether the location is for a “green field” site that involves the construction of a new data center, reviewing the location of an existing building that will function as a data center, or the ranking of data centers when considering closure or consolidation. As this section specifically relates to the location of the data center, criteria to be considered when evaluating existing buildings as to their suitability as a data center can be found in other sections of this standard (e.g., Sections 7 and 8).

The examples used in this section relate to North America. It is recommended that the designer follow the local guidelines and codes as specified by the AHJ for the specific data center location.

The occupancy classification of a data center is dependent on the use of the facility as defined by applicable standards (e.g., ASCE 07). This requirement can be increased by the owner based on the need or desire for the facility to operate after an event (class IV). Generally, data centers fall into classification II but could be rated occupancy classification IV if required by use or owner. Wind, snow, ice, flood and earthquake requirements are affected by the selected occupancy classification.

A project that is designated as critical by AHJ will effect site selection and design of the building and the mechanical electrical systems.

6.2 Natural environment

6.2.1 Seismic activity

Seismic activity and the potential for activity should always be strongly considered before selecting a data center site.

Seismically active areas should be avoided whenever possible. If this is not possible, provide the appropriate seismic equipment supports and structures to meet or exceed the requirements of local AHJ. In a seismically active area, the equipment within the data center, including the network and server racks and cabinets, should have additional structural anchorage in addition to higher structural requirements for the facility. Consider working with, if it is not required by the AHJ, a professional structural engineer to meet the appropriate seismic criteria of the data center facility.

Refer to seismic charts and other seismic activity information for the specific proposed data center site. Figures 4, 5, and 6 are some examples of seismic related documents that should be available for the data center site.

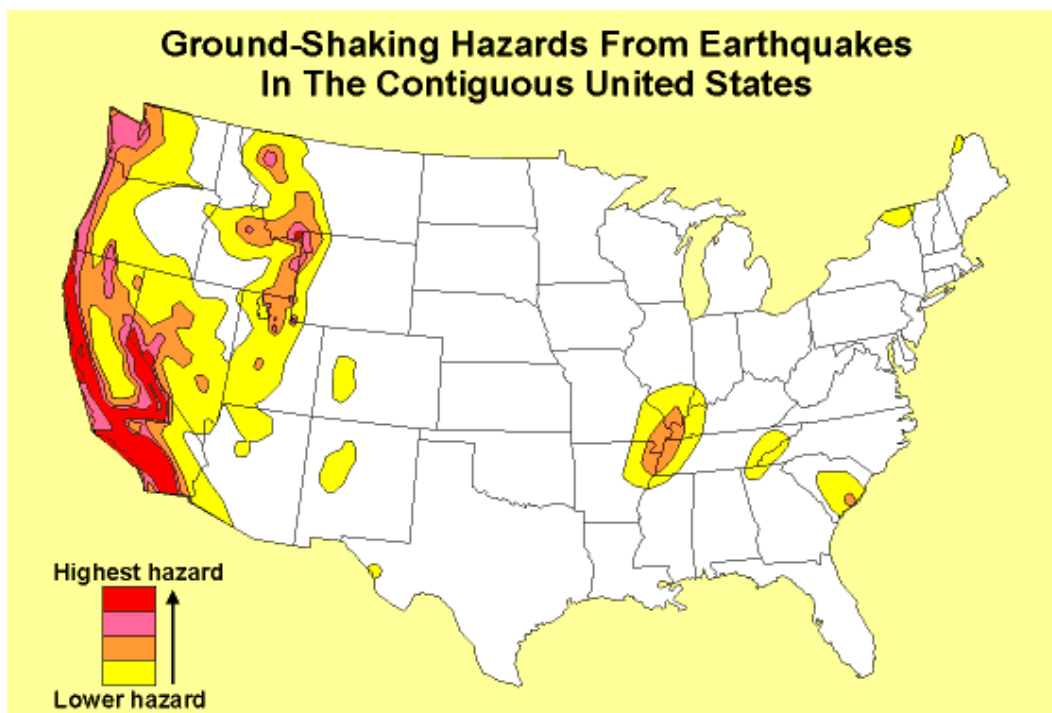


Figure 4: United States Ground-Shaking Areas (U.S. Geological Survey)

The United States Geological Survey Earthquake Hazards Program website is a resource for additional seismic historical data and current seismic activity (<http://earthquake.usgs.gov/>).

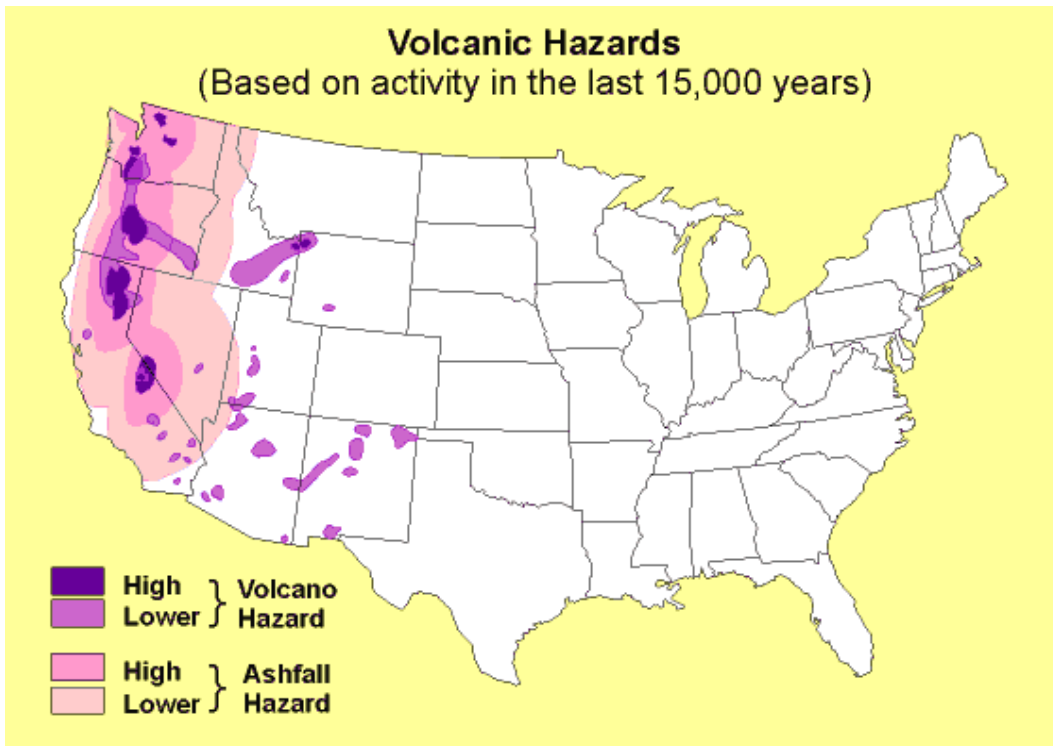


Figure 5: United States Volcanic Areas (U.S. Geological Survey)

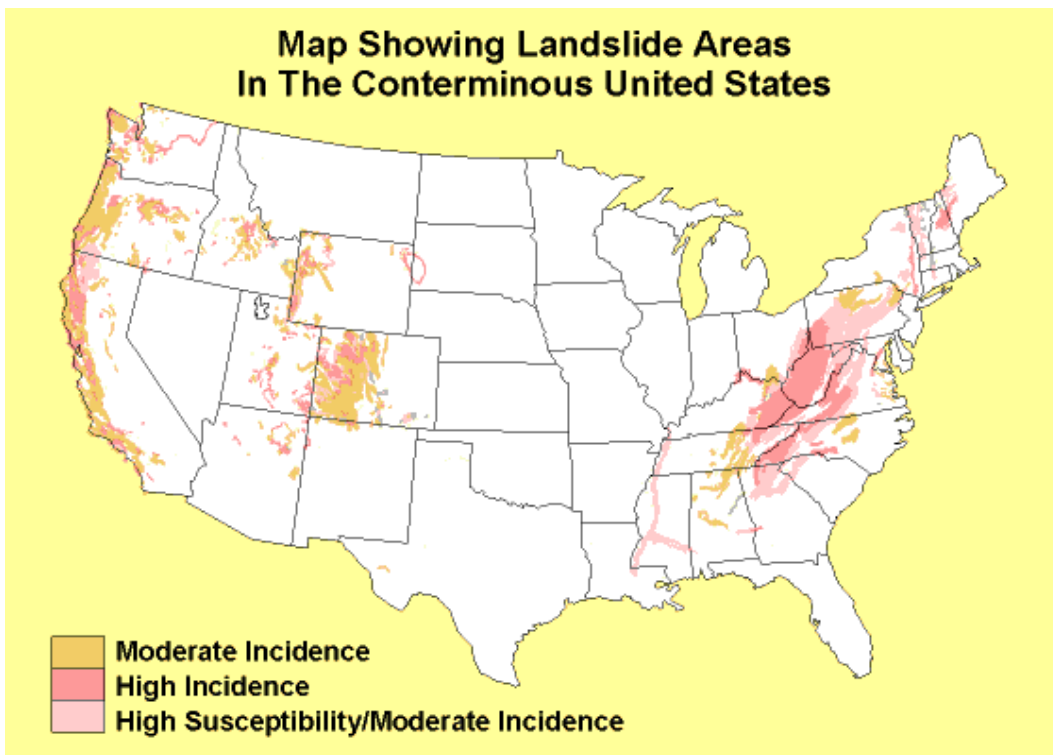


Figure 6: United States Landslide Areas (U.S. Geological Survey)

6.2.2 Subsurface stability

The following criteria should be used:

- Avoid the potential for quick, unstable or expansive soils.
- Ensure that there are no known subsurface contamination from either on-site hazardous waste storage or other adjacent site.
- Ensure that there is no potential of underlying solution-formed cavities common in limestone formations or the source of potential sinkhole problems.

Consider working with a professional geotechnical engineer to meet the appropriate criteria of the data center and to provide a formal written geotechnical report.

6.2.3 Groundwater

When selecting a site for a data center, careful consideration should be given to ground water saturation. It is preferable to have a water table that is as low as possible, with having a water table that is below the utility ducts and lowest level of the building the highest preference.

If the data center is a “slab on grade” on top of a hill, there should only be minor concerns for ground water issues.

If the data center is a “slab on grade” building in a relative flat topographical area, there may be small concerns for ground water issues. However, if the building has one or more subgrade floors in the same flat topographical area, the risk of water filtration into the structure increases.

If the data center is located at the bottom of a hill, there should be great concern for ground water issues.

Refer to ground water charts and other ground water activity information for the specific proposed data center site. Also, investigate whether the site is in a flood plain (100-year prediction).

Figures 7 and 8 and Table 2 are some examples of ground water related documents that should be available for the data center site.

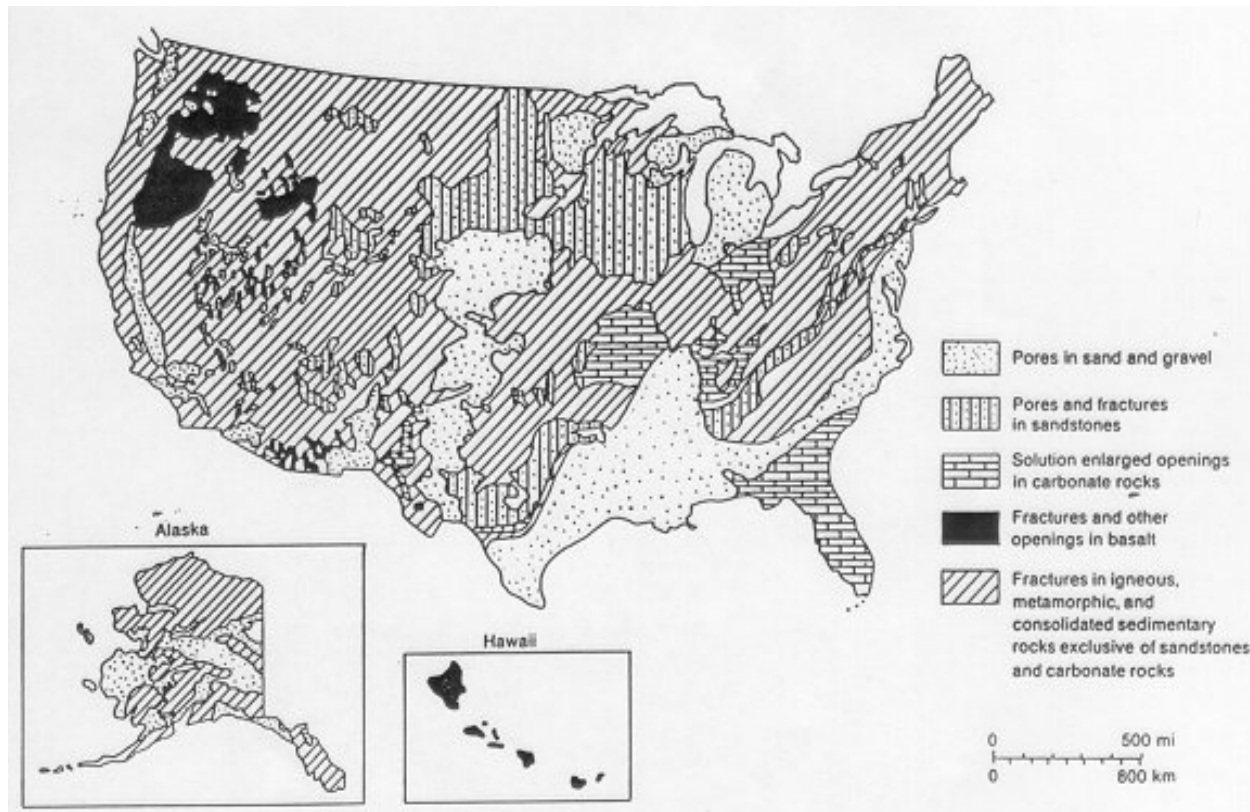


Figure 7: United States Aquifer Types (U.S. Geological Survey)

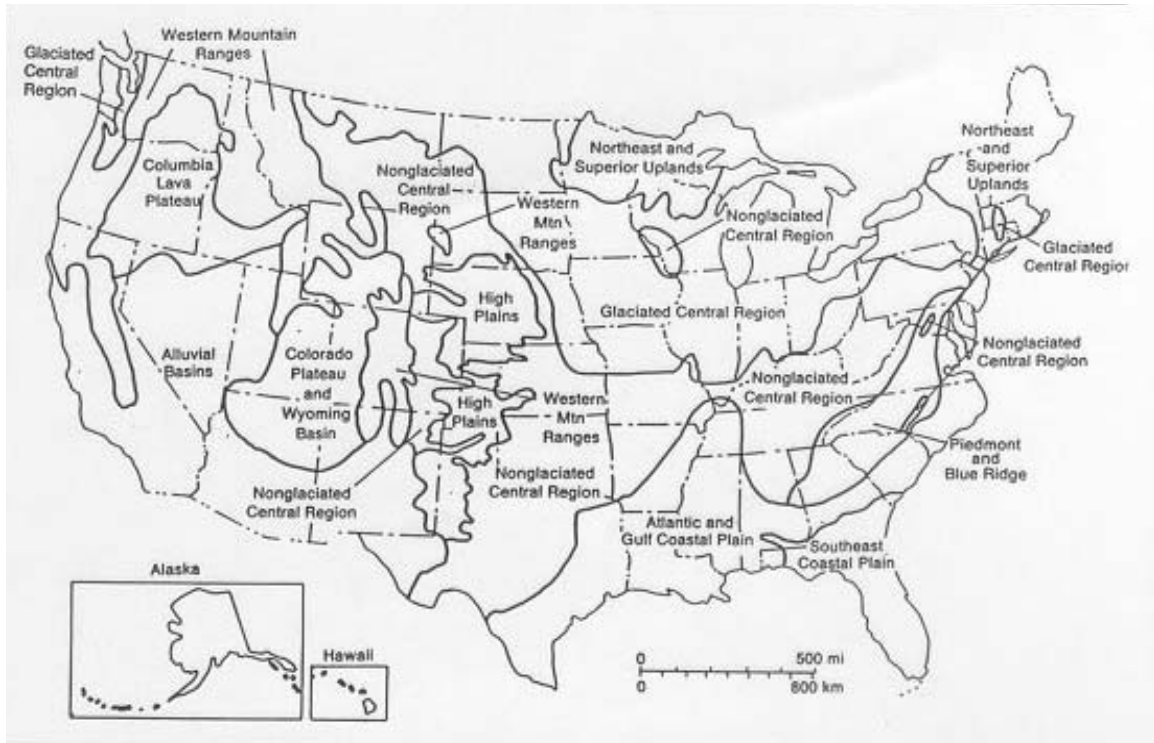


Figure 8: United States Ground Water Regions (U.S. Geological Survey)

Table 2: Hydraulic Characteristics Of Groundwater Regions Of The United States (common ranges)

Region number and name	Overview of geological forms	Transmissivity		Hydraulic conductivity		Recharge rate		Well yield	
		gpd/ft	m ² /day	gpd/ft ²	m/day	in/yr	mm/yr	gpm	m ³ /day
1 Western Mountain Ranges	Mountains with thin soils over fractured rocks, alternate with narrow, alluvial and, in part, glaciated valleys	40–7,000	0.5–100	0.007–400	0.0003–15	0.1–2	3–50	10–100	50–500
2 Alluvial Basins	Thick alluvial (locally glacial) deposits in basins and valleys bordered by mountains	10,000–1 million	20–20,000	700–10,000	30–600	0.001–1	0.03–30	100–5,000	500–30,000
3 Columbia Lava Plateau	Thick lava sequences interbedded with unconsolidated deposits and overlain by thin soils.	100,000–40 million	2,000–500,000	8,000–70,000	200–3,000	0.2–10	5–300	100–20,000	500–100,000
4 Colorado Plateau and Wyoming Basin	Thin soils over fractured sedimentary rocks	40–7,000	0.5–100	0.07–40	0.003–2	0.01–2	0.3–50	10–1,000	50–5,000
5 High Plains	Thick alluvial deposits over fractured sedimentary rocks	70,000–700,000	1,000–10,000	700–7,000	30–300	0.2–3	5–80	100–3,000	500–20,000

Region number and name	Overview of geological forms	Transmissivity		Hydraulic conductivity		Recharge rate		Well yield	
		gpd/ft	m ² /day	gpd/ft ²	m/day	in/yr	mm/yr	gpm	m ³ /day
6 Non-glaciated Central Region	Thin regolith over fractured sedimentary rocks	20,000–700,000	300–10,000	70–7,000	3–300	0.2–20	5–500	100–5,000	500–30,000
7 Glaciated Central Region	Thick glacial deposits over fractured sedimentary rocks	7,000–100,000	100–2,000	40–7,000	2–300	0.2–10	5–300	50–500	300–3,000
8 Piedmont and Blue Ridge	Thick regolith over fractured crystalline and metamorphosed sedimentary rocks	700–10,000	9–200	0.02–20	0.001–1	1–10	30–300	50–500	300–3,000
9 Northeast and Superior Uplands	Thick glacial deposits over fractured crystalline rocks	4,000–40,000	50–500	40–700	2–30	1–10	30–300	20–200	100–1,000
10 Atlantic and Gulf Coastal Plain	Complexly interbedded sands, silts, and clays	40,000–700,000	500–10,000	70–3,000	3–100	2–20	50–500	100–5,000	500–30,000
11 Southeast Coastal Plain	Thick layers of sand and clay over semi-consolidated carbonate rocks	70,000–7 million	1,000–100,000	700–70,000	30–3,000	1–20	30–500	1,000–20,000	5,000–100,000
12 Alluvial Valleys	Thick sand and gravel deposits beneath floodplains and terraces of streams	10,000–4 million	200–50,000	700–40,000	30–2,000	2–20	50–500	100–5,000	500–30,000
13 Hawaiian Islands	Lava flows segmented by dikes, interbedded with ash deposits, and partly overlain by alluvium	700,000–7 million	10,000–100,000	4,000–70,000	200–3,000	1–40	30–1,000	100–5,000	500–30,000
14 Alaska	Glacial and alluvial deposits in part perennially frozen and overlying crystalline, metamorphic, and sedimentary rocks	7,000–700,000	100–10,000	700–10,000	30–600	0.1–10	3–300	10–1,000	50–5,000

NOTE: Data produced by the U.S. Geological Survey

6.2.4 Wind

The most desirable location would have no exposure to tornado, hurricane, high wind, or sand storm risks.

An area with less than or equal to 2% annual probability of winds in excess of 129 km/hr (80 mph) would be ideal. When business drivers dictate that a data center be located in an area that has a greater than 2% probability, specific detail in the “hardening” of the facility should be incorporated into the design.

All structures on the site, including overhead cables, architectural screening, sound barriers, and the like, should meet the appropriate wind-loading requirements.

Refer to wind charts and other wind activity information for the specific proposed data center site. Figures 9 and 10 show examples.

Typical wind design parameters include FM I-90, I-120 and I-210. These parameters are based on Factory Mutual Global Insurance and Risk design practices to withstand 145 km/h (90 mph), 193 km/h (120 mph), and 338 km/hr (210 mph) winds respectively.

Wind mitigation strategies include window protection, anchoring, and roof protection.

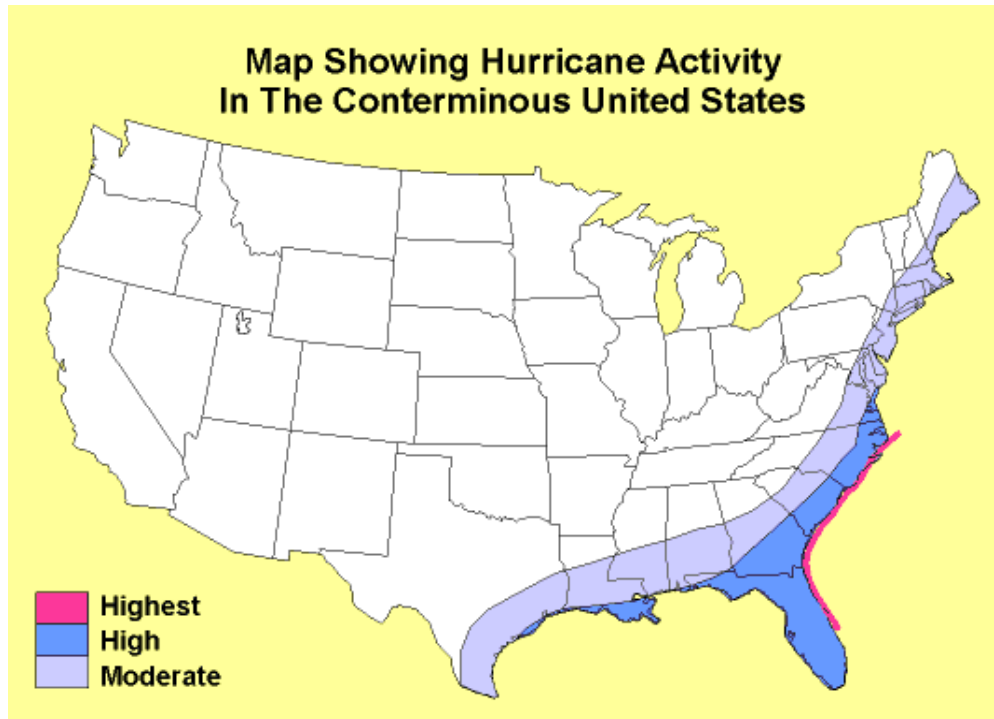


Figure 9: United States Hurricane Activity Areas (U.S. Geological Survey)

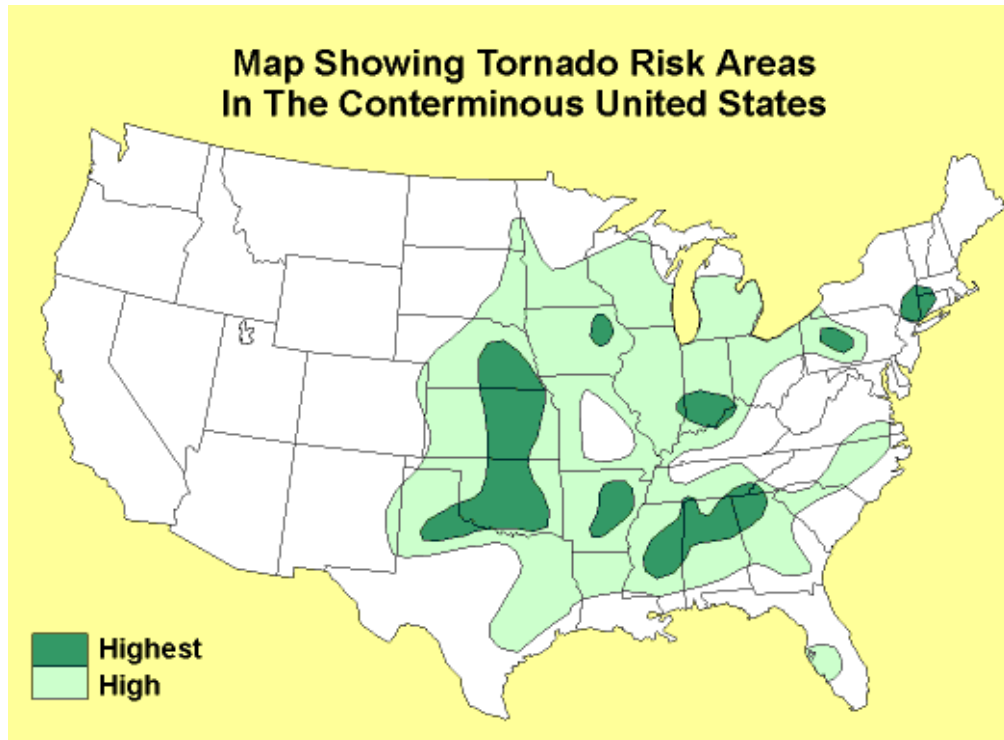


Figure 10: United States Tornado Risk Areas (U.S. Geological Survey)

6.2.5 Flood plain/wet lands

The site should be free of flood risk from river flood plain proximity, tidal basin proximity, dam failure, or levee failure. The site should also be above the maximum projected (100-year protection) flood levels.

An example of available flood information is Figure 11, which shows a general flood risk within the United States.

Sites with wetlands and protected habitat should be avoided. While issues related to these sites can be addressed or mitigated, they can cause time delays, increase costs and public awareness of the facility.

6.2.6 Topographical

Avoid sites within flashflood, brush fire, rockslide, mudslide or other debris flow areas.

Avoid sites with >15% ground slopes if possible; otherwise this may limit developable area. Sites with steep slopes may be difficult to access in adverse weather conditions.

The site topographical features should not restrict line of sight to geosynchronous satellites and location of ground dish arrays, if required.

Line-of-sight issues should be considered to locate wireless access equipment such as microwave, infrared, and directional antennas.

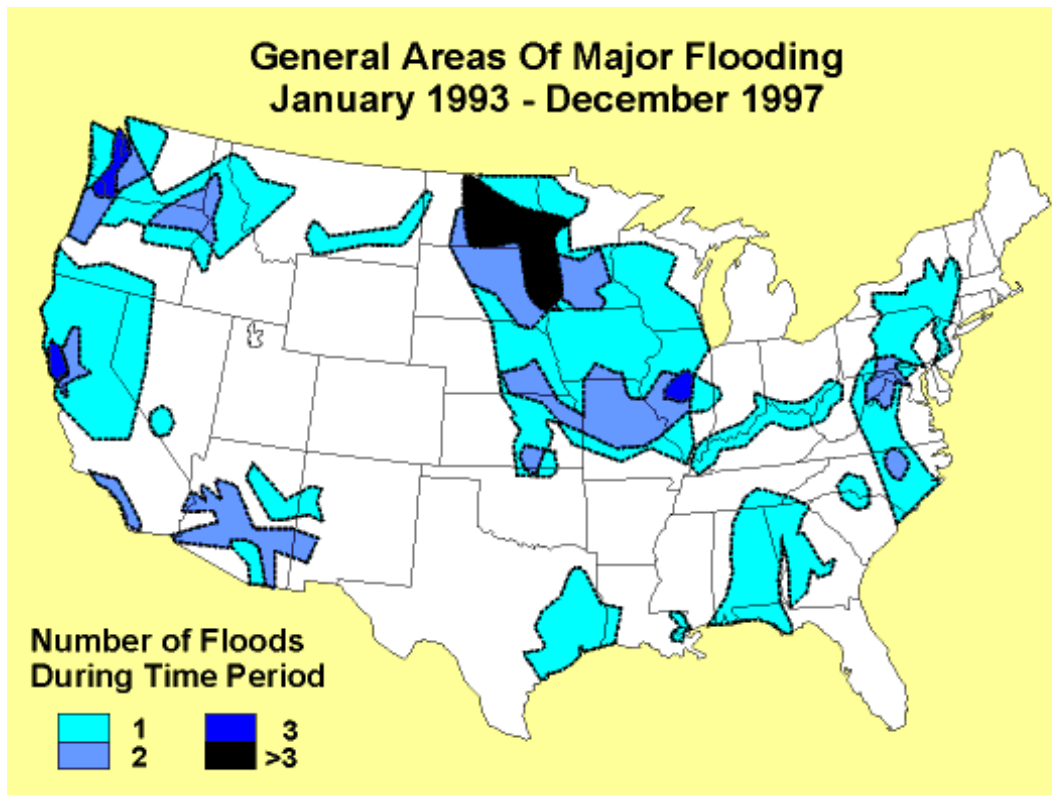


Figure 11: United States General Areas Of Major Flooding (U.S. Geological Survey)

6.2.7 Air quality

An area with clean air quality is preferred, so that emission of gases and particles does not cause a new air quality problem or worsen an existing problem.

In areas with existing air quality problems, regulations may be very stringent regarding emissions produced from fossil fuel consumption.

Ensure that generator run time permitting documents are issued in a timely manner to the jurisdiction overseeing air quality control and other local environmental authorities. In most cases, annual operation hours will be restricted and compliance must be verified.

If the owner wants to consider cogeneration of electricity there may be stricter air quality requirements and special permits required.

Air quality issues should be considered for the data center fresh air intake as well as any that may be emitted from the site. Fresh air intake requirements are usually regulated by the local AHJ. Provide appropriate air intake filtration systems as required.

When data centers must be located in densely populated areas or metropolitan areas, consider the effects of noise and emissions from the data center exhausts on neighbors and surroundings. Although usually regulated, it is common to have restaurants, dry cleaners, and other similar businesses requiring venting of chemicals and contaminants into the immediate environment. Special air intake filtration systems may be required for the data center in addition to any regulations.

6.2.8 Altitude

A maximum elevation of 3050 m (10,000 ft) is recommended, as the effectiveness of air cooling systems degrades significantly at higher elevations where air density is lower.

6.2.9 Noise

Wind will carry sound long distances. Even the slightest breeze can carry the sound of a facility well beyond the property line. Consider using sound attenuation whenever possible.

It is recommended to verify acceptable noise levels at property line and determine the noise levels produced by equipment.

Critical silencers on generator exhausts and sound attenuated enclosures on outdoor equipment such as generators, cooling towers should be always considered.

Outdoor equipment located on the ground and on rooftops may require screening for architectural aesthetics or building codes. Consider incorporating sound barriers within the architectural screening.

6.3 Utility environment

6.3.1 Power

6.3.1.1 Overhead utility service to facility

Overhead utility service to the facility is not desirable, especially if there is only one service entrance feed. Instead, provide underground utility service to the facility whenever possible. This will reduce the potential for system failure caused by overhead utility line damage. Vehicle accidents, wind, snow and other weather conditions are known factors for utility line damage.

If overhead utility lines to the site cannot be avoided, provide multiple power source paths. It is recommended that all electrical service entrances to the facility have a minimum separation of 20 m (66 ft) from the other electrical service entrances along the entire route.

The following is a list of preferences (in successive order) of overhead utility line sources:

- 1) at least one circuit from two separate and distinct utility substations; each substation to be fed from separate and diverse power grids; each circuit to be delivered to the site from their respective substations using separate and diverse paths;
- 2) at least one circuit from two separate and distinct utility substations; both utility substations fed from the same power grid; each circuit to be delivered to the site from their respective substations using separate and diverse paths;
- 3) at least two circuits from one utility substation; the utility substation to be fed from one power grid; each circuit to be delivered to the site from the same substation using separate and diverse paths;
- 4) At least one circuit from one utility substation; the utility substation to be fed from one power grid; the one circuit to be delivered to the site from the substation using a single path.

6.3.1.2 Underground utility service to facility

It is recommended that all electrical service entrances and feeds to the facility be underground. If there are redundant electrical service entrances, it is recommended that there be a minimum separation of 20 m (66 ft) along the entire route. Electrical service entrance feeds should have a minimum separation of 1.2 m (4 ft) from other utilities along the entire route.

Consider if the site can accommodate customer-owned maintenance holes and if the elevation of maintenance holes (utility or customer owned) can cause problems with water infiltration into the data center.

Provide underground utility service to the facility whenever possible. The following is a list of preferences (in successive order) of underground electrical utility line sources:

- 1) at least one circuit from two separate and distinct utility substations; each substation to be fed from separate and diverse power grids; each circuit to be delivered to the site from their respective substations using separate and diverse paths;
- 2) at least one circuit from two separate and distinct utility substations; both utility substations fed from the same power grid; each circuit to be delivered to the site from their respective substations using separate and diverse paths;
- 3) at least two circuits from one utility substation; the utility substation to be fed from one power grid; each circuit to be delivered to the site from the same substation using separate and diverse paths;
- 4) at least one circuit from one utility substation; the utility substation to be fed from one power grid; the one circuit to be delivered to the site from the substation using a single path.

6.3.1.3 Proximity to utility substation(s)

Data centers should be located in an area with easy sustainable circuit access to utility substations, with preference towards an area with utility circuits provided by two or more utility substations.

6.3.1.4 Capacity available to site

Provide adequate electrical utility capacity to the site to meet both current and projected needs of the entire site, and depending on the data center Class requirements, provide one or multiple electrical utility circuits, each with enough capacity, to handle the entire site requirements.

Circuit capacity to the site should be planned and implemented very carefully. If the data center is designed for minimal initial capacity with large future capacity requirements, careful consideration should be given to the amount of initial power requested to be delivered to the site by the utility company.

Work with a professional electrical engineer and the electrical utility or utilities serving the site. A cost benefit analysis and progressive circuit capacity design/implementation may benefit the site.

6.3.1.5 Proven utility reliability (percentage availability)

The benefit of installing a second utility feed should be analyzed based on the mean time between failure (MTBF) rate, mean time to repair (MTTR) and the power quality of the service to the data center.

The reliability of the backup power systems (generator) is typically significantly higher than the reliability of the power utility. If analysis is conducted over a 10-year period, the increase in reliability by adding a second utility is negligible, whereas adding backup power systems can show significant increase in the overall reliability of the power systems.

The power utility services in the United States average 1.86 outages annually at any point in the distribution with an average repair time of 4 hours. Consider three options with a mission time of 5 years and average reliability values for a generator of 80%, power distribution of 95%, and a UPS system of 80%.

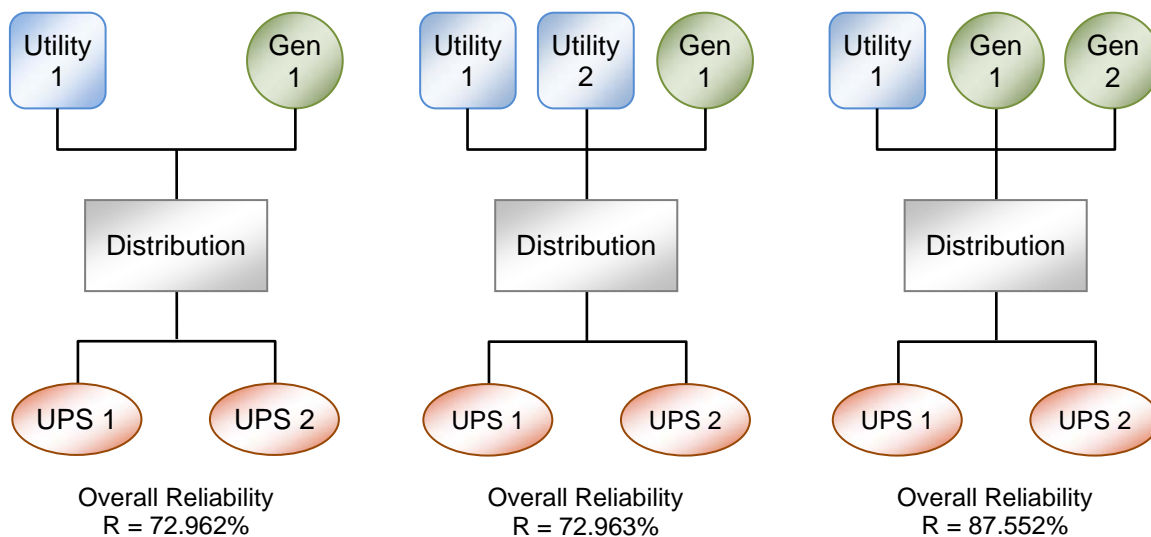


Figure 12: Utility Reliability Examples

The value added by implementing a second generator can have a much greater impact on the overall availability of the power system than adding a second utility feed. The above also assumes that there are no common mode failures between the two utility sources, which are often difficult to obtain. The reliability of the utility feeder is affected by the substation design. Preference is for multiple substation transformers and utility buses that can serve the facility feeder.

For the electrical feed, determine if there are other customers, such as manufacturing plants, that can create electrical noise. An electrical feed that also serves a hospital is generally desirable because such feed is less prone to shutdown by a utility.

6.3.1.6 Single feed from single utility substation

This is the least desirable method for power delivery to a site. Refer to *Overhead utility service to facility* and *Underground utility service to facility* above.

6.3.1.7 Redundant/diverse feeds from single utility substation

This is a moderately desirable method for power delivery to a site. Refer to *Overhead Utility Service to Facility* and *Underground Utility Service to Facility* above.

6.3.1.8 Redundant/diverse feeds from redundant utility substations

This is the most desirable method for power delivery to a site. Refer to *Overhead utility service to facility* and *Underground utility service to facility* above.

6.3.1.9 Unit substations

Depending on the size, Class and location of the data center, a unit substation may be required on the site.

Unit substations are usually medium voltage (e.g., 13,800 volts in most parts of the United States) switchgear that is used to parallel electrical utility circuits and/or transfer between redundant electrical utility circuits feeding the data center site. Unit substations are generally located outdoors on the ground, but in some cases may be found inside of the data center building (e.g., data centers located in metropolitan settings).

Unit substations generally connect to electrical transformers sized to meet the building voltage and amperage requirements.

When selecting a site, consider space for an electrical unit substation and its associated transformers and electrical utility circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

6.3.1.10 Utility transformers

Depending on the size, Class and location of the data center, utility transformers will most likely be required on the site.

Utility transformers usually transform medium voltage (13,800 volts in most parts of the United States) to low voltage (480 or 277 volts in most parts of the United States) electrical utility circuits feeding the data center site. Utility transformers are generally located outdoors but in some cases may be found inside the data center building (e.g., data centers located in metropolitan settings).

When selecting a site, consider space for one or more electrical utility transformers and their associated electrical utility circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

6.3.1.11 Backup generators

Backup generators (as opposed to emergency generators) are used to backup data center equipment in case of utility power failure. Depending on the size, Class and location of the data center, one or more backup generators will most likely be required on the site.

Backup generators can be as small as a compact car and as large as a full sized tractor-trailer box. These may be either indoors or outdoors, and it is common to find building rooftop mounted generators.

When selecting a site, consider space for one or more backup generators and their associated electrical utility circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

6.3.1.12 Emergency generators

Emergency generators (as opposed to backup generators) are used to power data center life safety systems (e.g., emergency lighting, fire pumps) if utility power fails. Depending on the size, at least one emergency generator will most likely be required on the site. For buildings to be occupied for extended power outages, areas other than the non data center must provide basic life safety and building occupancy requirements, including but not limited to lighting, fire alarm, operable restrooms, elevators, security, and ventilation.

Emergency generators can be as small as a compact car and as large as a full size truck. These may be either indoors or outdoors, and it is also common to find building rooftop mounted emergency generators.

When selecting a site, consider space for one or more emergency generators and their associated electrical life safety circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

6.3.1.13 Existing facilities

If the data center is moving into an existing building, determine if the building is up to current code and industry standards. It may actually be less desirable to move into a building with an existing electrical and mechanical plant, as it may be unsuitable for use in the data center. The existing systems may need to be removed and replaced at considerable expense.

6.3.2 Communications

If the data center is moving into an existing building, determine if the building is up to current code and industry standards. It may actually be less desirable to move into a building with an existing cabling infrastructure, as it may be unsuitable for use and need to be removed and replaced at considerable expense.

6.3.2.1 Overhead service to facility

Overhead utility service to the facility is not desirable, especially if there is only one service entrance. Instead, provide underground utility service to the facility whenever possible. This will reduce the potential for system failure caused by overhead utility line damage. Vehicle accidents, wind, snow and other weather conditions are known factors for utility line damage.

If overhead service is the only available option, ensure that the entrance cables are well protected from physical damage at the drop pole. If cables drop from service poles to underground, the drop pole should provide 100 mm (4 in) rigid conduits from below grade up to the elevation where the cables are suspended to protect the entrance cables from physical damage.

If overhead utility lines to the site cannot be avoided, provide multiple source paths. If telecommunications service cabling is redundant, it is recommended that telecommunications service cabling pathways have a minimum separation of 20 m (66 ft) along the entire route.

The following is a list of preferences (in successive order) of overhead utility line sources:

- 1) at least one service feed each from two separate and distinct access provider central offices—each access provider central office connected to multiple redundant long-distance carrier offices; each service feed to be delivered to the site from their respective access provider central office using separate and diverse paths;
- 2) at least one service feed from two separate and distinct access provider central offices; both access provider central offices connected to the same long-distance carrier offices; each service feed to be delivered to the site from their respective access provider central office using separate and diverse paths;
- 3) at least two service feeds from one access provider central office—the access provider central office to be fed from one or more long-distance carriers; each service feed to be delivered to the site from the same access provider central office using separate and diverse paths;
- 4) at least one service feed from the one access provider central office—the access provider central office to be fed from one or more long-distance carriers; the one service feed to be delivered to the site from the access provider central office using a single path.

6.3.2.2 Underground service to facility

It is recommended that all telecommunications service cabling to the facility be underground with a minimum separation of 1.2 m (4 ft) from other utilities along the entire route. If telecommunications service cabling is redundant, it is recommended that telecommunications service cabling pathways have a minimum separation of 20 m (66 ft) along the entire route.

Determine if the site can accommodate customer-owned maintenance holes and if elevation of maintenance holes (utility or customer owned) can cause problems with water infiltration into data center.

Provide underground utility service to the facility whenever possible. The following is a list of preferences (in successive order) of telecommunication service line sources:

- 1) at least one service feed each from two separate and distinct access provider central offices—each access provider central office connected to multiple redundant long-distance carrier offices; each service feed to be delivered to the site from their respective access provider central office using separate and diverse paths;
- 2) at least one service feed from two separate and distinct access provider central offices; both access provider central offices connected to the same long-distance carrier offices; each service feed to be delivered to the site from their respective access provider central office using separate and diverse paths;
- 3) at least two service feeds from one access provider central office—the access provider central office to be fed from one or more long-distance carriers; each service feed to be delivered to the site from the same access provider central office using separate and diverse paths;
- 4) at least one service feed from the one access provider central office—the access provider central office to be fed from one or more long-distance carriers; the one service feed to be delivered to the site from the access provider central office using a single path.

6.3.2.3 Proximity to service providers and/or other data centers

Data centers should be located in an area with easy sustainable connectivity to the access provider central offices. Locating a data center in an area with connectivity provided by two or more access provider central offices is most desirable.

Redundant data centers for disaster recovery (DR) purposes should be located at least 48 km (30 mi) away from each other. The two locations should be on separate distribution systems to minimize the occurrence of one outage effecting both locations.

6.3.2.4 Capacity available to site

Adequate copper conductor and fiber optic capacity to the site should be provided to meet the current and projected needs of the entire site, and depending on the data center Class requirements, provide one or multiple connectivity paths, each with enough capacity, to handle the entire site requirements.

Connectivity capacity to the site should be planned and implemented very carefully. If the data center is designed for minimal initial capacity with large future capacity requirements, careful consideration should be given to the amount of capacity requested to be delivered to the site by the access providers.

Work with a professional IT consultant and the access providers serving the site. A cost benefit analysis and progressive connectivity capacity design/implementation may benefit the site.

6.3.2.5 Proven access provider reliability (percentage availability)

The reliability of the primary access provider should be determined to ensure that the required availability requirements can be achieved.

Reliability of the communication services can be improved by either adding redundant circuits from the primary access provider, or adding services from alternate access providers. The reliability of the overall communications services can be further increased if the redundant circuits are serviced from separate access provider offices following diverse routes.

6.3.2.6 Service redundancy alternatives

The service redundancy alternatives are as follows:

- Redundant/diverse feeds from redundant access provider central offices supported by multiple long-distance carrier offices. This is the most desirable method for connectivity to a site. Refer to Overhead utility service to facility and Underground utility service to facility above.
- Redundant/diverse feeds from redundant access provider central offices supported by same long-distance carrier office. This is a more desirable method for connectivity to a site. Refer to Overhead utility service to facility and Underground utility service to facility above.
- Redundant/diverse feeds from single access provider central office. This is a moderately desirable method for connectivity to a site. Refer to Overhead utility service to facility and Underground utility service to facility above.
- Single feed from single access provider central office. This is the least desirable method for telecommunications delivery to a site. Refer to Overhead utility service to facility and Underground utility service to facility above.

6.3.3 Water

6.3.3.1 Municipal water supply

6.3.3.1.1 Capacity available to site

The data center may need to have access to reliable significant quantities (750-1100 liter/min [200-300 us gallon/min]) of quality water depending on cooling system design. However, not all areas are able to provide this quantity of quality water continuously independent of long-term weather conditions.

Provide adequate municipal water delivery to the site to meet the requirements of the data center. For Class F3 or F4 data centers, the ability of the water supply pumping station(s) to deliver water when there is a major power outage must be documented and/or mitigated.

Data centers may require large volumes of water for other uses. Some uses of water that may be required are as follows:

- Domestic water (e.g., drinking water, restrooms, kitchens)
- Irrigation (e.g., lawn watering)
- Fire suppression (e.g., sprinkler systems)
- HVAC (e.g., cooling towers)

6.3.3.1.2 Water quality

Although water delivered to sites by most municipalities are generally considered to be potable (drinkable), the water should be tested for contaminants and particulates. Water filtration systems may be required for some or all of the various water uses listed above. It is common to find a water filtration system specific to the domestic water system in a building.

6.3.3.1.3 Graywater systems

Graywater (waste water that doesn't contain serious or hazardous contaminants) systems can be municipally provided supplies or project generated and can be used to minimize a project's impact on the surrounding community and potentially reduce operating costs.

6.3.3.2 Private well supply (well water)

6.3.3.2.1 Capacity available to site

Make sure that there is adequate well water delivery on the site to meet the requirements of the data center.

6.3.3.2.2 Quality

The available on-site water (well water) should be tested for contaminants and particulates. Water filtration systems may be required for some or all of the various water uses listed above. It is common to find a water filtration system specific to the domestic water system in a building.

6.3.3.3 Dual water supply (municipal water supply and well water supply)

Occasionally, a data center site will require both a municipal water feed to the site as well as using an on-site well. It is common to find a domestic water system and fire suppression system connected to the municipal water source while having the HVAC and irrigation systems connected to the on-site well.

6.3.3.4 Backup supply

Review need and availability of a backup water supply for the facility for domestic uses as well as water cooled cooling systems. Backup systems could be multiple water sources or onsite water storage. Backup water supply is required for Class F3 or F4 data centers when evaporative cooling towers are the heat rejection methodology.

6.3.4 Sanitary sewer

6.3.4.1 Municipal sanitary waste sewer system

6.3.4.1.1 Capacity available to site

Provide adequate sanitary waste capacity from the site to the municipal sanitary waste sewer system. Sanitary systems or storm drainage systems (depending on local requirements) need to be sized for the amount of expected water usage by cooling systems, including cooling tower blow down or filtration systems, which could be greater than 750 liters/min (200 gpm).

6.3.4.1.2 Remediation requirements

Coordinate with the local AHJ and provide all remediation as may be required by code and standards. Holding tanks, traps and the like may be required and need to be planned into the site design.

6.3.4.2 Private sanitary waste system

6.3.4.2.1 Capacity available to site

Provide adequate sanitary waste capacity from the building to the on-site sanitary waste system (septic system).

6.3.4.2.2 Remediation requirements

Coordinate with the local AHJ and provide all remediation as may be required by code and standards. Holding tanks, traps, and similar facilities may be required and need to be planned into the site design.

6.3.5 Natural gas

6.3.5.1 Utility provided natural gas

6.3.5.1.1 Capacity availability to site

Provide properly sized natural gas feed from the local utilities to support adequately the heating systems, cooling systems and electricity generation (emergency and backup generators) that the site requires.

Make sure that the utility company assures full capacity natural gas delivery to the site for the duration of any prolonged power outage or disaster situation.

6.3.5.1.2 Redundant/diverse gas feeds from redundant gas sources

Redundant gas feeds from redundant gas sources is most desirable method for natural gas delivery to a site.

6.3.5.1.3 Redundant/diverse gas feeds from single gas source

Redundant gas feeds from a single gas sources is desirable method for natural gas delivery to a site, but less desirable than having redundant gas sources.

6.3.5.1.4 Single gas feed from single gas source

A single gas feed from a single source is the least desirable method for natural gas delivery to a site.

6.3.6 Other fuel (utility natural gas unavailable)

Onsite stored fuel sources may be required by code or when utility provided natural gas is not available.

The data center site should be carefully planned to support on-site fuel storage when it is required. On-site fuel storage should be located on the data center site in a secure and aesthetically pleasing manner.

6.3.6.1 Onsite propane gas

Onsite propane gas may be selected as a fuel source to support the site requirements. Propane tanks are usually located outdoors on the ground and are sometimes buried below grade.

Fuel should be stored as far away from the data center as practical. Blast containment (proximity to building or actual structure) should always be planned into the site.

6.3.6.2 Onsite diesel

On-site diesel fuel may be a good alternate fuel source to support the site requirements. Diesel tanks are usually located outdoors on the ground and are sometimes buried below grade. Special containment is usually required in case of fuel leaks.

Fuel should be stored as far away from the data center as practical. Blast containment (proximity to building or actual structure) should always be planned into the site.

6.3.6.3 Other fuel sources

Other fuel or energy sources may be used to support the site. Some sources, including wind generators and photovoltaic panels, may be used and will need additional space planning for them as well as their associated equipment.

Careful consideration should be given to the visual intrusion on neighbors and any effects on the surrounding environment. Zoning, codes, and other governmental/municipal restrictions may not allow for alternate fuel/energy sources.

6.4 Transportation

6.4.1 Public road access

6.4.1.1 Proximity

6.4.1.1.1 Road traffic accidents

The site should allow the placement of the building so that it is not close enough to the road that an adjacent road traffic accident could result in vehicular contact with the building fabric and the potential for resulting structural damage or the potential for fire.

6.4.1.1.2 Vehicle spillage

The site should allow the placement of the building so that it is not close enough to the road that an adjacent road traffic accident could result in the spillage of a toxic or flammable load coming into contact with the building fabric and resulting in structural damage or the potential for fire.

6.4.1.2 Traffic type

6.4.1.2.1 Recommendations

Site should be within reasonable distance—3.2 km (2 mi) to 16 km (10 mi)—to a freeway or other major arterial road. However, it is generally not desirable for the data center to be within 1.6 km (1 mi) of a freeway, railroad, or other major thoroughfare to minimize exposure to contaminants in the event of an accident.

The site should have two or more access roads from the nearest major arterial road, with each road having a minimum of 4.3 m (14 ft) height clearance throughout.

If the data center is on a campus, the campus should have redundant access roads with a security checkpoint at each access point.

Locations that are adjacent to or accessed via routes that are adjacent to roads carrying large volumes of combustible, toxic, or otherwise dangerous loads, or that could be subject to protest or blockade due to their antisocial nature, should be avoided.

6.4.2 Air traffic

The following site selection considerations regarding air traffic apply when planning the location of a data center:

- type and frequency of air traffic
- location of civilian (commercial or private) and military airfields
- flight path data for primary, secondary, and emergency approaches of any nearby airfield
- potential for crash landings
- terrorist attack
- EMI from radar installations.

Commercial airports should be greater than 8 km (5 mi) away, with flight paths to any airport located at least 1.6 km (1 mi) away from any potential site boundaries.

6.4.3 Railways

The following site selection considerations regarding railways apply when planning the location of a data center:

- frequency and type of rail traffic service (e.g., mainline, commuter, local spur)
- derailment and accident history
- types of rail traffic loads , such as
 - passenger
 - mixed freight
 - fuel and other combustibles
 - chemicals and other hazardous materials
 - radioactive material
- location of railroad, classification, and marshalling yards
- terrorist attack.

Data centers should be located at least 1.6 km (1 mi) away from transportation corridors (for example, railroads, highways, or waterways) on which hazardous material could be transported and which could explode or be released, thereby posing a hazard to the data center and its occupants or preventing access to and from the data center..

6.4.4 Marine

The data center should not be located within 1.6 km (1 mi) of a major port handling cargo vessels.

6.5 Regulations (local, regional, federal)

6.5.1 Air quality

Determine if local air quality regulations exist such as generator emission restrictions. These regulations may restrict the acceptable hours of operating backup generators.

In the United States, the Federal Government has passed a federal law through the 1990 Clean Air Act. The individual States must ensure that the requirements of the Act are the minimum standards that must be met; individual States may enforce stricter requirements.

Particular concern that data centers may have for local authorities are the emissions of oxides of nitrogen (NO_x), carbon monoxide (CO) and particulate matter (PM-10).

6.5.2 Noise

6.5.2.1 Noise levels within data center

Determine if there are any local, regional or federal regulations that identify acceptable levels of noise from equipment operating within the data center.

6.5.2.2 Noise levels outside data center

Determine if there are any local, regional or federal regulations that identify acceptable levels of noise that cannot be exceeded at or beyond the property line.

6.5.3 Communication towers

Determine if there are any local regulations that will restrict the height or proximity to other facilities for communication towers.

Determine if there are any federal or local requirements to hide visually antennas from public view.

6.5.4 Water tanks/cooling towers

Determine if there are any local regulations that will restrict the height, diameter or proximity to other facilities for water tanks and cooling towers.

Determine if there are any local requirements to hide visually water tanks or cooling towers from public view.

6.5.5 Fuel tanks

Determine if there are any local regulations that will restrict the size, or proximity to other facilities for fuel tanks.

Determine if there are local regulations that will allow above ground fuel tanks only.

Evaluate security of the fuel tanks.

6.5.6 Generator exhaust

Emission levels need to meet state and local emission requirements.

6.5.7 Generator hours of operation

Generator hours may be limited by local codes.

6.5.8 Required parking

Determine how the AHJ determines the required number of parking stalls for a new facility. Negotiations with the AHJ may be necessary to try to reduce the number of required stalls if the AHJ treats the data center as typical commercial office space.

6.5.9 Truck traffic

Determine if there are any road restrictions (permanent or seasonal) on the size of vehicular traffic, or time of day restrictions for truck traffic.

6.5.10 Setbacks

Determine the required setbacks from the property line for the building, parking, or perimeter security.

6.5.11 Height restrictions

Determine if there are any local height restrictions for the data center.

6.5.12 Environmental assessment

An environmental assessment could include an environmental impact study if wet lands are impacted or if the site has any contaminants present. An environmental impact study may be required by the AHJ. Ensure sufficient time prior to proceeding with the detailed design phase to allow completing the study and attend AHJ meetings as required to obtain approval.

For example, refer to U.S. Environmental Protection Agency (<http://www.epa.gov/>).

6.5.13 Sight lines

Assure from AHJ that the target location does not have sight line restrictions that must be mitigated, or that they can be done so economically.

6.6 Location environment

6.6.1 Adjacent properties

6.6.1.1 Proximity

The data center should be built far from any other buildings and facilities that may pose a fire threat or that could cause damage to the data center should the other buildings or structures collapse.

6.6.1.2 Impact on access/egress due to traffic levels

A facility located adjacent to a large campus or manufacturing plant may suffer from traffic issues at certain times of the day (e.g., at the start and end of the working day, if adjacent to a 24-hour facility, this could be three times a day or more depending on shift patterns).

6.6.1.3 Impact on operations

The following is a partial list of adjacent properties that have an increased potential to affect data center operations.

- Embassy/consulate;
- Military;
- Police;
- Fire station;
- Hospital;
- Chemical plant;
- Political target;
- Research lab;
- Publishing house/foreign press.

6.6.1.4 Vacant lots

Adjacent vacant lots may cause future issues due to:

- Possible future development;
- Unknown tenant(s);
- Disruption during construction.

6.6.1.5 Proximity to hazardous operations and other high-risk facilities

Many hazards exist that are not normally considered facility risks. Agencies such as the Critical Infrastructure Assurance Office (CIAO) cite examples of critical infrastructure risks. One or more of these potential hazards will not render an existing facility inherently unreliable only less reliable and/or more prone to adverse consequences.

Nuclear power plants should be at least 80 km (50 mi) away.

The following should be at least 13 km (8 mi) away: minor airports (propeller and light aircraft only), missile bases or control sites, and military bases or other military/munitions support operations.

The following should be at least 8 km (5 mi) away: conventional fossil fuel power plants, chemical and fertilizer plants, grain elevators, tank farms (e.g., natural gas, gasoline, fuel oil), foundries, and other smokestack industry operations.

The following should be at least 5 km (3 mi) away: embassies, extremist political group properties, research laboratories, weather or other radar installations, and radio/TV transmitters/stations.

The following should be at least 3.2 km (2 mi) away: landfills, dumps, junk yards, quarries, interstate highways, railroads, inland harbors/canals, municipal water and sewage treatment plants, stockyards and livestock feedlots, lakes, dams, and reservoirs.

The following should be at least 1.6 km (1 mi) away: gas stations, compressed gases distributors, auto body or other paint shops, self-storage facilities, high-voltage power distribution lines, public utility substations, and water storage towers.

Having emergency services reasonably accessible can be a valuable life-saving resource for site occupants. Ideally, a staffed (or at least volunteer) fire station and/or police station should be within 8 km (5 mi) of the candidate site, and a hospital emergency room within 16 km (10 mi).

Data centers should be located:

- More than 91 m (300 ft) from 100-year flood hazard areas.
- More than 1.6 km (1 mi) from coastal or inland waterways.
- A minimum of 3 m (10 ft) height above highest known flood level and highest waterway levels.
- More than 1.6 km (1 mi) from commercial railways used to carry cargo, highways and other major traffic arteries.
- More than 8 km (5 mi) from an airport and preferably not more than 48 km (30 miles).
- Not more than 16 km (10 mi) from a major metropolitan area (to ensure prompt response to vendor service calls).
- In single tenant buildings unless all occupants are also data centers or telecommunications facilities.

6.6.1.6 Proximity to existing or redundant data center

For disaster backup sites, consider the issue of distance from the main data center. Distance will be determined by the use of the primary site and whether the backup site must have synchronous or asynchronous replication with the primary data center.

6.6.2 Security

Avoid high crime areas. Refer to Section 12 for additional threats and concerns to be considered.

Consideration should be made for level and type of perimeter security required for the site. This would include building type, site location, fenestration, and neighborhood. These factors will vary based on the users need.

6.6.3 Underground train or public transportation stations

6.6.3.1 Proximity

Close proximity to an underground station can be beneficial for getting staff to and from the facility. However, other issues may outweigh the benefits.

6.6.3.2 Terrorist attack

Risk of terrorist attack can be a significant reason for avoiding a location close to an underground train station

6.6.3.3 Usage/type of traffic

The type of traffic using the underground facility should be established to ascertain the risk level (e.g., passenger traffic only or commercial loads such as fuel or chemical).

6.6.3.4 Vibration

Underground train traffic can create vibration within a building located directly above the train tunnel. Vibration within a data center can be associated with many intermittent faults because of connections within many infrastructure elements becoming loose over time. For more information, refer to *Structural and Vibration Guidelines for Datacom Equipment Centers* by ASHRAE.

6.6.3.5 Electromagnetic interference

Underground trains can create electromagnetic interference within a building located directly above the train tunnel, particularly near steel columns located on lower floors.

6.7 Cost evaluation

The site selection process should include a detailed analysis of all the costs associated with any particular location. The following lists identify costs that should be considered when comparing available sites.

One-time costs that may be significant such that any one may drive the site selection process are:

- Real estate costs.
- Local tax incentives.
- Environmental assessment consulting costs. This could include an environmental impact study if wet lands are impacted or if the site has any contaminants present. This could require a significant effort to develop the assessment and attend required meetings with the AHJ. This may drive the site selection process due to the impact on the schedule in addition to any additional costs incurred.
- Cost to bring adequate utilities infrastructure to site in order to support the critical load, both initial and future anticipated growth (power, water, sewer, gas, telecommunications).
- Cost to provide redundant utilities (power, water, gas, telecommunications) to the site, if required. Determine the additional costs associated with redundant site utilities and any impact that the implementation may have on the schedule.
- Demolition costs for any existing structures, site preparation costs.
- Cost and availability of permanent telecommunications service and temporary telecommunications services to support the migration of data from existing data center(s).

Determine the costs to bring telecommunications service to the building. Costs for diverse underground service from an alternate access provider office may be quite high. Additionally, consider temporary telecommunications circuits that may be needed to support the migration of data from the existing data center(s) to the new data center. Identify costs associated with the temporary circuits for movement of data, including:

- Cost of relocation of systems into the new data center:

Develop a high-level move strategy so that appropriate funds can be allocated for the move of systems and networks into the new data center. Identify any needs for consultants, temporary labor, media, network, server, and storage hardware to support the move and their associated costs.
- Impact of data center constructability:

Determine if there are any conditions at a particular site that will affect the constructability of the new data center. A particular site may require a longer approval, permitting, or construction schedule. An extended schedule may affect feasibility due to decommissioning requirements of the existing data center.
- Recurring costs that will have long-term effects on feasibility of site:
 - Usage costs for utility services (power, water, sewer, gas)
 - Cost of telecommunications services
 - Prevailing wage for skilled labor in local area
 - Lease costs
 - Taxes
- Intangible costs:
 - Proximity to other corporate facilities (travel time)
 - Proximity of skilled staff
 - Availability of alternate or multiple telecommunications access providers:
 - Data services
 - Voice services

This page intentionally left blank

7 Architectural

7.1 Facilities planning

7.1.1 General overview

7.1.1.1 Introduction

The purpose of this section is to provide information to assist a designer in the planning and specification of a computer room and related spaces. This section will focus on the architectural and general construction elements of a data center. Some reference will be made to other elements, as the purpose of the architectural elements of a data center is to provide a physical envelope that assists in meeting the needs of the end user (information technology/telecommunications processor).

The initial planning of the data center must work in conjunction with the client facilities planners, the IT personnel, the telecommunications personnel, the client office users, the various disciplines that will assist in the completion of the data center.

Several methods of planning the data center are currently utilized in today's environment. Two of those are:

- IT, telecommunications, and other users collect data and turn it over to the facilities manager who then puts together a team that locates a site, designs it, and constructs it;
- the facilities and IT personnel select an initial programmer and/or designer to assist in the gathering of information and prepare a document that assists in the search of the site and assists in the budgeting of the project.

From this point, the project is completed one of two ways:

- the initial design team continues to prepare a complete set of construction documents that are bid to a preselected group of contractors (design-bid-build), or;
- the initial programming information is handed to a preselected design build contractor who provides all documents and construction for the project (design/build).

See Annex A for more information regarding design and construction approaches.

The appropriate approach for a given project varies depending on a project. For an entity that has limited specific design requirements, has a preselected location, and trusts the contracting entity, the second planning method listed above is the most likely utilized. For companies that want to ensure that the data center planned meets some specific needs, and for those entities who want to ensure that the initial planning decisions meet their detailed user and market requirements, the first planning option listed above is recommended. To determine whether design-bid-build or design/build is best suited for a specific project, the client should consider the complexity of the project. Companies that have several data centers of the same type and complexity may find the design/build process can save time and money. If the space is complex, and there are a variety of end users and multiple processing elements, the design-bid process can ensure all the issues are addressed initially, and reduce time delays and costs increases later.

It should be noted that the accessibility standards and guidelines (e.g., Americans with Disabilities Act of 1990 [ADA] Standards for Accessible Design) or similar standard may need be followed for the design and construction of computer rooms and support spaces. The designer should be aware that the AHJ may require adherence to these standards and may publish its own enhancements to the standards.

7.1.2 Site selection

7.1.2.1 Requirements

While most site selection criteria is covered in Section 6, from an architectural/general construction consideration, it is important to ensure that:

- all interfering elements be eliminated (vibration, air contamination, security, flood plains, electromagnetic interference, and hazardous materials);
- sufficient space is provided around the building to allow for complete security;
- space is provided for a variety of support equipment, such as
 - generator(s);
 - fuel tank(s) to support the generator;
 - HVAC heat rejection systems.

These elements shall also be secure from public access.

- all electrical service requirements are met (see Section 9).

7.1.2.2 Addition information

Other issues to be considered for site selection, but not addressed here include availability of power, telecommunications connections and stability, fire services, secure neighborhood, and others. (See Section 6).

7.1.3 Location within a building**7.1.3.1 Requirements**

When looking into a floor below grade level, water infiltration issues shall be considered, including height below surrounding drainage systems, secure, continuous vapor barriers, water and vapor extraction systems, main building systems that might create damage to the data center, as well as hazardous materials stored or utilized in the basement. The required distributed floor loading capacity is specified in Section 8.

7.1.3.2 Recommendations

For equipment access, the floor nearest prevailing grade level (ground floor) is often the most advantageous. Floor loading considerations also tend to lead to the first floor as a location. Upper floors can be a solution to security and water issues, but in areas with major lateral force issues (hurricane, wind, seismic), the upper floor can contribute to structural instability. Many times, the upper floors are not designed for the floor loading required for a data center.

7.2 General design concepts**7.2.1 Levels of reliability****7.2.1.1 Introduction**

The level of required reliability plays a major part in the design of the data center. A generally accepted method of describing levels of reliability is the Class system (discussed in Annex B).

Reliability is defined in relationship to the identified risks. For example, NFPA 75 identifies risks such as life safety, fire threat, loss of revenue, loss of equipment, and loss of telecommunications. It is safe to assume that the loss of the data center will affect one or more of the elements above.

In the United States, for further information on construction and protection of computer rooms, refer to NFPA 75.

7.2.1.2 Requirements

Building shall be of construction appropriate for the level of durability and reliability consistent with the best structural practices for processing facilities. (See Section 8)

7.2.1.3 Recommendations

The building should be designed to meet design criteria for seismic and wind lateral conditions.

7.2.2 Facility purpose**7.2.2.1 Introduction**

The general purpose of the data center affects the construction, operation, and physical security of the data center. Medical, financial, and government information regulations may impose special security requirements. Codes might dictate requirements for certain types of facilities such as hospitals, utilities, telecommunications, and other critical services.

The occupancy category of a data center is dependent on the use of the facility as defined by applicable standard (e.g., ASCE 07) or AHJ. This requirement can be increased by the owner based on the need or desire for the facility to operate after an event (occupancy category IV). Generally, data centers fall into occupancy category II, but could be rated occupancy category IV if required by use or owner. Wind, snow, ice, flood and earthquake design requirements for the building and the mechanical electrical systems are affected by the selected occupancy category.

The importance factor to be used in calculating design requirements may be increased by the owner to provide a more robust design even if the occupancy is less than occupancy category IV.

A project that requires critical power systems per AHJ (e.g., critical operations power systems [COPS] under article 708 of NFPA 70 (NEC) and NFPA 1600) will affect site selection and the design of the building and its mechanical electrical systems.

7.2.2.2 Requirements

The design team shall work with the users to determine the purpose of the facility with the focus on the effects of failure of the facility. By utilizing the Class definitions as described in Annex B, determine the appropriate level of reliability to meet the purpose of the facility.

7.2.3 Multiuser versus single user groups

7.2.3.1 Introduction

Multiuser facilities have more security requirements than single user facilities. Administrative functions require access be limited to a minimum number of authorized personnel. Groups such as engineering and research may require a greater access to accommodate more frequent equipment setup and changes.

7.2.3.2 Requirements

Data centers that house data processing equipment from multiple companies will require physical security for equipment of each user. Physical user security can be accomplished by partitions (such as walls or cages), or at the cabinet level with electronic controls or physical locks.

Multiuser facilities may require surveillance systems and additional access control and records, including tenant power metering.

7.2.4 Equipment change cycle

7.2.4.1 Requirements

Flexibility needs to be planned into a data center that adds or changes equipment frequently. Designers and users are to determine the expected life cycle for equipment, and determine the effect on facilities operations, including the need for space inside and outside the computer room to stage and bring into service new hardware.

7.2.4.2 Recommendations

The average data center may significantly change its ITE inventory every 3 to 5 years. The physical power and cooling infrastructure should be flexible and scalable in order to optimize it for the conditions of power capacity and density at any given time and place within the computer room.

7.2.5 Occupied versus unoccupied computer rooms

7.2.5.1 Recommendations

In general, data centers, which must remain reliable, are to be designed with a “lights out” computer room – that is, a data center with no personnel permanently housed in the computer room space. The design of a lights out environment will require planning of personnel areas and control room to reduce the access to the computer room. In addition, design of the support equipment (e.g., mechanical, electrical) should be such that the amount of required service within in the computer room is minimized.

7.2.6 Data center location within building

7.2.6.1 Requirements

If the data center is on a floor above the first (grade level) floor, ensure access is provided for the equipment required in the data center.

The data center shall be located as close as possible to incoming power to reduce the power cabling lengths.

7.2.6.2 Recommendations

The computer room should be located in close proximity to the communications distribution point (carrier entrance rooms) of the building.

The computer room is best located away from the exterior walls, on the ground floor, or on a floor that has structural support capabilities to support equipment.

7.2.7 Type of building

7.2.7.1 Requirements

Critical data centers shall be installed within a steel or concrete framed building, such as a Type I, II, or III building as defined in the International Building Code. Under certain conditions, Type IV construction can be utilized if constructed in accordance with NFPA 75.

The exterior of buildings shall be nonflammable and of durable material.

The building section shall allow for a clear access floor to ceiling height of a minimum of 3 m (10 ft).

7.2.7.1 Recommendations

The slab to structure above should be a minimum of 4.5 m (15 ft).

7.2.8 Multitenant buildings

7.2.8.1 Requirements

Where a data center is in a multitenant building, the data center shall be located away from hazards and mutual access points with other tenants. Services to the data center shall be separate from service to other tenants.

All water lines, sprinkler lines, ductwork, and gas lines serving areas outside of the computer room shall not pass through the computer room area. No systems hazardous to the computer room shall be located in or around the computer room.

7.2.9 24/7 operation of data center

7.2.9.1 Introduction

Critical data centers are often operational 24 hours per day, 7 days per week.

7.2.9.2 Requirements

The data center, including office and control room functions, shall be arranged in a manner to provide security to personnel within the data center, and security to arrival and departure locations. At high security facilities, walls, windows and doors of rooms typically permanently staffed (i.e., control room, guard station), should be hardened / bullet resistant.

Twenty-four hour operations shall have break facilities within the building, in the vicinity of the data center.

7.2.10 Temperature and relative humidity control

7.2.10.1 Requirements

The computer room shall be located so that temperature and relative humidity can be maintained with minimum energy usage.

The design of the computer room shall include proper insulation and moisture control to maintain steady temperature and relative humidity ranges within the data center.

7.2.11 Materials

7.2.11.1 Requirements

The computer room shall be designed and built with new materials, which are durable, of superior quality, and easy to maintain and operate. Where recycled materials will not affect the operation of the space, they may be considered for use.

7.3 Design for efficiency

7.3.1 Holistic energy efficient data center design

Historically, data centers have been designed in a piecemeal manner. Critical components, such as UPS systems, computer room air conditioners (CRACs), power distribution equipment, equipment racks and the ITE itself are often specified and purchased separately without a view of how they could all fit together as one cohesive system. Likewise, the buildings in which many data centers are housed were not designed to provide the robust environment required to support and protect mission-critical operations. Many data centers are still designed this way.

Availability of the operation has always been the main concern, with cost of the operation well down the list of priorities. But with government sanctions such as “carbon caps” and “green mandates,” the idea of achieving higher operating efficiencies is gaining attention for reasons of energy reduction, lower cost of operation, competitive advantage, and regulatory compliance. To achieve dramatic advances in performance, data center architecture must be designed as a whole, not in pieces. The Green GridSM organization has published many papers and tools directed toward viewing the data center as one fully integrated system (See Annex C).

7.3.1.1 Scalability

All systems and subsystems should be able to scale to or near their optimum operating efficiency throughout the life of the facility. Designs should be flexible enough to adapt to changing power and cooling requirements and technological improvements that cannot be anticipated at the time of the data center design. This approach has a greater chance of achieving the lowest practical energy consumption over the life of the facility when the planner/designer:

- pays close attention to establishing a rational model for growth of space and power requirements over time; and
- models power and cooling system performance over the life of the data center in accordance with the growth model.

7.3.1.2 Instrumentation and control

All systems and subsystems should be instrumented so that they can gather real time operating power and performance data. All components should be able to communicate status through standardized management interfaces. Data should include indicators of optimum energy efficiency such as power consumption, temperature, percent load, and other metrics as appropriate to the device.

In particular, if measurement of PUE is desired (discussed below), instrumentation should be installed that permits measurement and trending of the energy consumption of the specific equipment that directly supports the data center.

7.3.1.3 Annunciation

All systems and subsystems should be discoverable through the single management system, to report and trend such metrics as location, minimum and maximum energy used, and performance level capabilities.

7.3.1.4 Management

All systems and subsystems should be able to network through standardized management, interoperability interfaces, and language. Operations should be automated at all levels via policies set through management infrastructure.

7.3.2 Data center efficiency metrics

The expression is, “You cannot control what you cannot measure.” In order to know if a design is good or if it is working as well as intended, there must be a means to measure its effectiveness. Most manufacturers of ITE or IT infrastructure equipment provide some information about equipment power consumption. For code compliance purposes, nameplate data typically includes very conservative numbers on power consumption so that the cables, circuit breakers and fuses will be sized for worst case. But designing for worst case exacts a penalty in efficiency and operating costs.

Accurate measurement of power consumption in real time allows a baseline to be established. Future performance can be compared to the baseline to document changes in data center efficiency, and against industry performance in general.

Recently the industry has started to standardize on two measurements for data center efficiency: PUE and DCiE.

7.3.2.1 Power usage effectiveness (PUE)

PUE is simply a measure of the power consumed by the data center as a whole divided by the power consumed by servers, storage devices, and other ITE. It is expressed in Equation 1.

$$PUE = \frac{\text{Total facility power}}{\text{ITE power}} \quad (1)$$

PUE will be greater than 1.0. Many data centers operate with PUE near 2.0. Inefficient or poorly managed data centers have PUE as high as 3.0. A good target to strive for is a PUE within a range of 1.3–2.0.

The concept is easy, but actual implementation and interpretation is more challenging. PUE can be measured instantaneously, or at any time interval – hourly, daily, weekly, monthly—all the way to the life of the facility in years. A rough analogy is vehicle fuel efficiency measured in distance traveled per volume of fuel consumed (miles per gallon or kilometers per liter). This metric can vary widely over time, and is influenced by many variables. Similarly, PUE is highly dependent how facilities infrastructure performs at any point in time. This performance can vary widely over the life of the facility, depending on the magnitude of load relative to capacity, and the degree to which efficiency is dependent on the load versus capacity of components and systems.

PUE is a ratio of power consumption in a specific data center, so comparison of two facilities solely on the basis of PUE can be misleading. The Green Grid is currently working to develop improved metrics to represent data center efficiency.

The power consumption of electrical power distribution and cooling equipment for the purpose of calculating PUE is supposed to be limited to the equipment that is directly supporting the data center. In many, if not most data centers, some portion of the power and/or cooling produced by such support equipment is used for spaces that do not directly support the data center. For example, chilled water systems in dedicated data center facilities often supply cooling to areas such as equipment/parts storage, restrooms, corridors, network operations center, and meeting rooms. While these areas might seem to be directly supporting the data center in such a facility, they should not be

included in calculating PUE. The energy associated with providing cooling and power to these areas is not likely to be metered separately, so an estimate of their contribution must be made to allow adjustment of the PUE calculation. Some government agencies have begun using PUE as an energy effectiveness measurement.

7.3.2.2 Data center infrastructure efficiency (DCiE)

DCiE is simply the reciprocal of PUE, and is expressed in Equation 2.

$$DCiE = \frac{1}{PUE} = \frac{ITE\ power}{Total\ facility\ power} \times 100\% \quad (2)$$

DCiE will result in a number less than 1.0. It is often preferred because, intuitively, it expresses efficiency as a percentage.

Either PUE or DCiE can be used, but the industry seems to favor PUE.

7.3.3 Data center energy saving design opportunities

Data center efficiency is most effectively optimized by concentrating on the areas where the greatest gains are possible. It is frequently stated that the cost of operating infrastructure to support ITE is greater than the cost of operating the ITE itself. This suggests a PUE greater than 2.0.

When designing a data center for efficiency, the techniques listed in Table 3 should be considered. The values given are subjective, but they give a reasonably good comparison of their impact on a design. Most of the techniques are described in more detail elsewhere in this standard.

Additional design guidance to improve energy efficiency can also be found in *EU Best Practices for EU Code of Conduct on Data Centres* and *ASHRAE Best Practices for Datacom Facility Energy Efficiency*.

Table 3: Data Center Energy Saving Opportunities

<i>% of improvement possible</i>	<i>Area for attention</i>
10 - 40%	high-efficiency ITE such as blade servers, and IT management systems such as server virtualization
10 - 40%	hot-aisle or cold-aisle containment systems
10 - 40%	cabinets with isolated air supply or isolated air return
10 - 30%	modular and scalable architecture for power & cooling considering total life-cycle energy savings.
5 – 15%	hot-aisle/cold-aisle equipment rows with optimally located row-oriented cooling
4 – 15%	locating sites where it is possible to take advantage of economizer modes of air conditioning (air-side or water-side)
4 - 10%	selection of high-efficiency power equipment such as UPS, capable of high efficiencies at low loads
0 - 10%	cooling management systems able to prevent demand fighting in which one unit is humidifying while another is dehumidifying
1 – 6%	where under-floor cooling is used, optimized quantity and location of floor vents only in the cold aisles, assisted by computational fluid dynamics (CFD)
1 – 6%	overhead wiring and cabling to prevent blockage of air distribution under access floors (Refer to 14.4.8.1 for considerations of overhead versus under-floor cable routing)
1 – 5% or more	use of blanking panels in equipment racks to prevent mixing of cold inlet air and hot exhaust air
1 – 5% or more	blocking access floor cable cut-outs and sealing floor tile openings to prevent escape of cold air where it is not needed
1 – 3%	use of energy efficient lighting along with timers, occupancy schedules, or motion detectors

7.4 General paths of access

7.4.1 General access

7.4.1.1 Introduction

Once the site is selected, planning the layout of the data center will begin. Access is crucial. The points of access included in this section include main data center personnel access, non-data center personnel access, equipment vendor access, equipment access, access to support equipment such as UPS and batteries, HVAC equipment, miscellaneous electrical equipment repair access, telecommunications vendor access, and separate user group access.

7.4.1.2 Requirements

All entries into the data center shall be secured. The points of access discussed here include main data center personnel access, non-data center personnel access, equipment vendor access, equipment access, access to support equipment such as UPS and batteries, HVAC equipment, miscellaneous electrical equipment repair access, telecommunications vendor access, and separate user group access.

7.4.2 Data center access

7.4.2.1 Requirements

In buildings with a lobby and building guard, direct communications shall be established between the control center of the data center and the building guard station. For high-security sites, communications shall be both audio and visual.

The maximum slope for ramps is 8 degrees from horizontal for movement of cabinets with equipment. However, some accessibility regulations specify a maximum rise of 1:12, or about 4.8 degrees. Additionally the ramp shall be at least 900 mm (36 in) clear width, have hand rails on both sides, and have a 1.5 m (5 ft) clear landing at the top and bottom.

If the computer room has only one ramp, it shall meet AHJ accessibility requirements. One ramp for equipment and an elevator or ramp for wheelchair access is acceptable.

7.4.2.2 Recommendations

The main access to the data center should be secured via some form of access control. This control can be a combination of personnel and electronics, or solely electronics. Each client should consider the level of security necessary for protection of the data being processed.

Sites without a building guard should have both audio and visual controls at the initial point of access to the data center.

In data centers occupied 24/7, it is recommended the initial main access route lead into a secure location outside the computer room that provides additional control prior to entrance into the computer room. Observe life safety code regarding egress.

7.4.3 Equipment access

7.4.3.1 Requirements

The data center shall be within the building to allow for the delivery of computer and telecommunications equipment to the facility. The computer/telecommunications equipment delivery pathway, including doors, shall allow for delivery of equipment as large as 3 m (10 ft) long by 1.2 m (4 ft) deep by 2.4 m (8 ft) high, weighing greater than 3400 kg (7500 lb). The support equipment rooms (e.g., UPS and battery room, HVAC room) typically require access for equipment even larger than mentioned above. The routes for mechanical and electrical equipment shall be large enough to permit installation of new equipment and removal of old equipment—a clear height of at least 2.7 m (9 ft) is typically required along routes from the loading docks to the electrical and mechanical rooms. Clear height requirements shall consider the height of equipment, packaging, and moving equipment.

7.4.4 Telecommunications access provider entry into computer rooms

7.4.4.1 Requirements

The local access providers require access to the telecommunications entrance rooms, but are generally restricted from access to the computer room unless:

- The entrance room is a portion of the computer room.
- The computer room houses access provider equipment such as DWDMs, SONET multiplexers, or other circuit provisioning equipment.
- The carrier demarcation points (e.g., DS-1 or DS-3 DSX panels) reside in the computer room.

7.4.5 Vendor access

7.4.5.1 Requirements

Access control shall allow access by essential vendors that support the processing equipment. These access control system may require that such vendors be escorted. This control shall allow the data center personnel to know when and where the vendors access the data center.

7.4.6 Support equipment service access

7.4.6.1 Recommendations

As much as possible, support equipment that requires servicing should be serviced on the perimeter of the data center to prevent untrained personnel from inadvertently damaging the processing equipment.

7.5 Programming detail

7.5.1 Entry

7.5.1.1 Requirements

Consideration shall be made for the initial entrance through a controlled lobby or vestibule, allowing for the entrance to the computer room to be a distance from the visible exterior. The entry to the computer room from noncomputer room spaces shall lead into a controlled space within the data center, prior to providing access to the computer room areas.

Entry for equipment, if separate from main entry, shall be controlled by the data center personnel only.

7.5.1.2 Recommendations

The entry to the computer room should be positioned away from the direct access to the exterior.

Equipment entry should be located near a staging/storage area for unpacking and preparation of equipment prior to entry into computer room.

7.5.2 Control room and personnel areas

7.5.2.1 Requirements

For data centers that are important or critical to company function, a control room shall be included in the program. This control room should be near the main entrance, and shall house environmental monitoring equipment, computer system monitors, and space for the number of data center operators present at any given time. A console is recommended to house all monitors.

The control room shall be located so that it has direct access to the computer room space.

As needed, office and conference facilities shall be provided adjacent to the control room for supervisory functions and to form a war room or emergency troubleshooting area.

7.5.3 Printer room

7.5.3.1 Requirements

For centers that require printing, a printer room shall be provided adjacent to the personnel areas. The printer room shall be self-contained, with a filtration system on the return air leaving the room. Space shall be provided for paper staging within the printer room to ensure the stabilization of paper.

7.5.4 Media storage room

7.5.4.1 Requirements

Facilities that produce in-house record storage media, a separate room shall be provided for media storage prior to transfer to permanent storage.

Storage of critical media shall be contained within a 2-hour fire rated enclosure.

7.5.5 Restrooms and break rooms

7.5.5.1 Requirements

Restroom and break room areas shall be provided with easy access to the operations and office areas. Restrooms shall be accessible, for both genders per the governing local codes and standards.

7.5.5.2 Recommendations

For 24/7 operations data centers, where practical, access to the restroom and break room should be within the security-controlled area of the data center.

7.5.6 Computer room

7.5.6.1 Introduction

In general, it is anticipated that circulation and support equipment (HVAC floor mounted air handlers, coolant distribution units, electrical PDUs, RPPs, static switches, and distribution, and fire suppression tanks) can require as much as 40 percent of the overall space in the equipment area. In the case of Class F3, and especially Class F4, the physical infrastructure space requirement may be over 50% of the total facility square footage.

7.5.6.2 Recommendations

In planning the rack/cabinet layout, care should be taken to allow for maximum flexibility. A data center may significantly change its ITE inventory every 3 to 5 years.

The data center planner should coordinate early on with mechanical and electrical systems designers.

The computer room should be designed in a manner to provide adequate space for current equipment, growth, circulation, and support equipment.

Production, development, and test systems should be in separate areas of the computer room, preferably in separate rooms served by dedicated networks.

Expansion should be planned into computer rooms. With the multitude of elements that affect the IT environment, it is difficult to plan for exact expansion needs. It is generally good to determine the expected life of the facility, look at the past growth trends, and allow for a minimum of 20 to 40 percent above the trend growth for each 5 to 8 years of life expectancy.

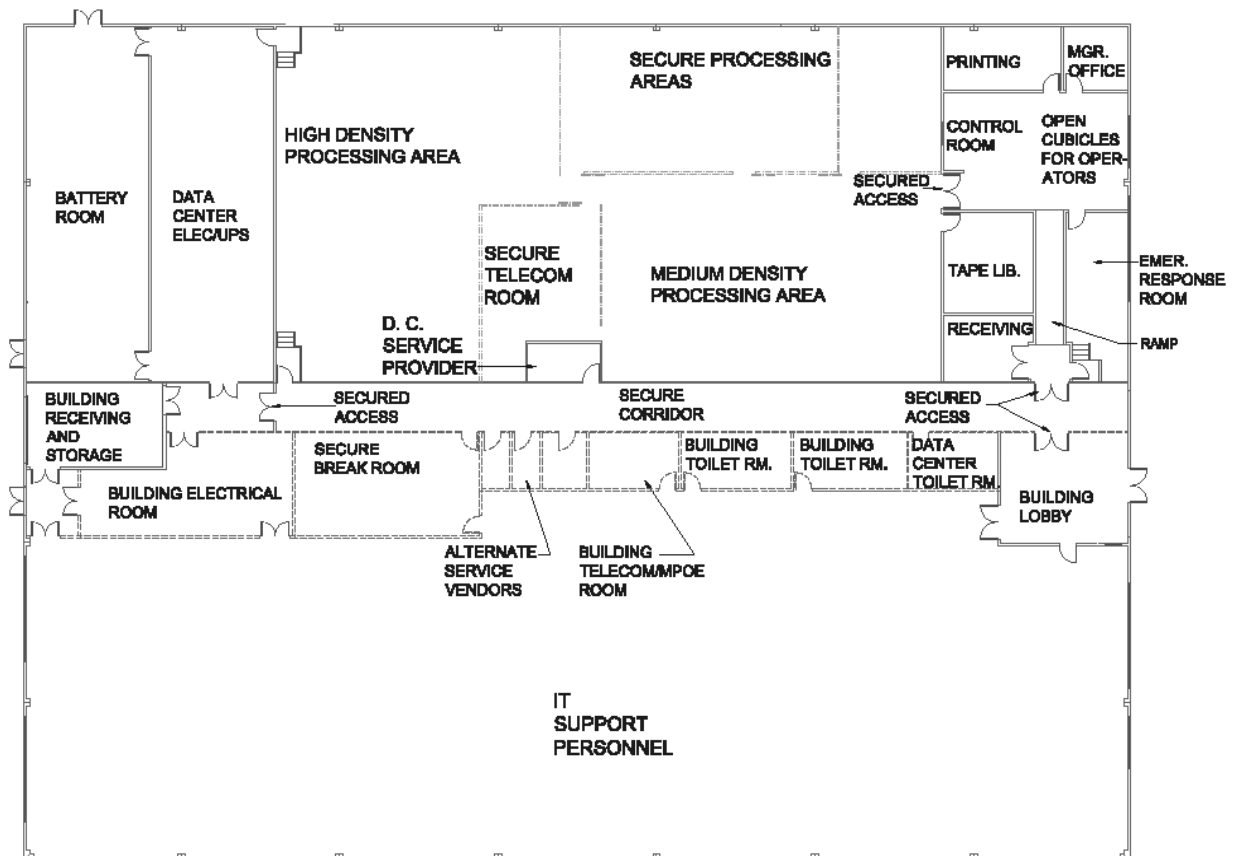


Figure 13: Conceptual Data Center Layout

7.5.7 Entrance rooms

7.5.7.1 Requirements

The entrance room, if separate from the computer room, shall be accessed without going through the computer room.

7.5.7.2 Recommendations

It is recommended that in all data center types, the data center be provided with separate entrance rooms.

The entrance room should be contiguous with the computer room.

In determining the space for the entrance rooms, consideration should be made for the incoming optical fiber and copper backbone and associated electronics, telecommunications switches, telecommunications electronic components, and optical fiber and copper patch and termination panels for distribution to patch panels and racks within the computer room. See Section 14.1 and 14.2 for additional information regarding entrance room planning.

7.5.8 Mechanical equipment space

7.5.8.1 Introduction

Mechanical equipment will be in the computer room (as mentioned), as well as in a mechanical equipment room/area outside the computer room.

7.5.8.2 Requirements

The architect and data center planner shall coordinate with the mechanical system designer for sizing and amount of equipment in the computer room. Outside of the computer room, provide space for the heat ejection equipment and associated pumps, fuel tanks, and controls.

7.5.8.3 Recommendations

Mechanical components within a computer room should be located separate from the equipment rows in order to provide maintenance access. Cooling systems should be located separate from the equipment rows in order to provide for maintenance, unless placement in or close to the equipment row is necessary for enhanced cooling effectiveness.

7.5.9 Electrical room and UPS room

7.5.9.1 Requirements

A separate room shall be provided to contain the data center associated electrical equipment, including the switchboard, various electrical panels, generator automatic transfer switch(es), UPS systems, and input/output boards.

Electrical and UPS room shall be as near as possible to both the main building electrical room and the generator.

7.5.9.2 Additional information

The electrical room may require two exits, with doors opening in the direction of egress from the room and the doors and equipment with panic hardware as required by AHJ. Secondary exit routes may pass through other associated spaces such as the battery room, if permitted by AHJ.

7.5.10 Battery room

7.5.10.1 Introduction

If a centralized UPS system is utilized, a battery room most often accompanies the UPS room.

7.5.10.2 Requirements

Battery rooms with batteries containing liquid, free flowing electrolyte shall include electrolyte spill containment and exhaust systems as required by local codes.

7.5.10.3 Recommendations

If the batteries are in a dedicated battery room, the battery room should be adjacent to the associated electrical room.

The size of the battery room will depend on the type and number of batteries and racks/cabinets.

The battery room should be located at grade level if feasible. Below grade can create a flooding hazard. Above grade can create a floor loading hazard.

The battery room should be designed to accommodate the anticipated maximum floor loading.

The battery room should NOT be located above a computer room space.

The electrical engineer or local codes may prescribe additional requirements regarding the location of the battery room or battery room equipment, Coordinate with the electrical systems designer

Consult applicable IEEE battery installation standards and see the additional battery information in Section 9.5.5.

7.5.10.4 Additional information

The AHJ may require that the battery room have two exits.

7.5.11 Fire suppression room

7.5.11.1 Requirements

For critical (higher Class) data centers, a separate room shall be provided for the preaction sprinkler control valve system.

Space shall be provided for the placement of clean agent fire suppression tanks as required. Tanks shall be located to assist easy serviceability. Tanks shall not be located in the ceiling area above equipment.

7.5.12 Circulation

7.5.12.1 Requirements

Clear pathways allowing for the movement of racks, processing and support equipment shall be provided throughout the space in a direct path.

Circulation pathways shall be a minimum of 1.2 m (4 ft) wide, with a minimum clear overhead of 2.4 m (8 ft).

7.5.12.2 Recommendations

Rows should not exceed 20 racks or cabinets in length. Dead-end aisles should be avoided whenever possible for the safety of personnel. Where dead-end aisles are not avoidable, they should be no longer than 10 racks or cabinets in length.

7.5.13 Equipment staging and storage

7.5.13.1 Requirements

To prevent contaminants in the computer room, arriving equipment shall be stored, uncrated and prepared in a room away from the computer room, with filtration on the return air leaving the room.

For both arriving equipment and backup equipment, such as boards and servers, a storage room shall be adjacent to the equipment entrance of the data center. The storage room can be a component of the staging room, or a separate room near the staging area.

A staging area shall be provided that has space for the uncrating and preparation of arriving equipment.

Provide space for the large amount of boxes and packing material handled by these facilities. Consider fire protection requirements, frequency of removal and recycling to comply with local requirements. Consider dumpster requirements, access and location.

7.5.14 Equipment repair room

7.5.14.1 Recommendations

A separate room for repair should be provided with easy access to both the equipment access pathway and the computer room.

Equipment repair room should have work surface with multiple power and communications connections.

Shelving/caged areas should be provided for spare parts as necessary.

7.6 Construction components

7.6.1 Data center preparation

7.6.1.1 Requirements

If data center is a new building, prepare the slab and all below grade components of the building with a continuously sealed rubberized moisture barrier.

Building slab shall comply with all local building code requirements for protection against flooding, such as height above flood plain and setbacks from a flood plain.

All exterior opening and penetrations shall be sealed prior to work on interior walls or finishes in the computer room.

7.6.2 Floor slab

7.6.2.1 Requirements

Floor slab shall have a minimum thickness of 140 mm (5.5 in). For rooms containing fully loaded high-density racks, floor slab thickness shall be a minimum of 200 mm (8 in).

For elevated slabs, the concrete topping over metal deck flutes shall have a thickness of at least 100 mm (4 in), to allow for the adequate embedment of epoxy and anchor bolts.

The floor slab shall be leveled and sealed with a nonpenetrating seal, such as epoxy, which is a moisture barrier and prevents dusting/particulating.

See Section 8.4.1 for floor loading requirements.

7.6.3 Computer room envelope wall construction

7.6.3.1 Requirements

The perimeter walls to the computer room shall be full height (slab to deck above).

See Table 4 regarding fire rated construction requirements.

All wall penetrations shall be fire sealed, and sealed to prevent chemical fire suppression leaks.

Interior walls shall be constructed with metal studs having a minimum thickness of 0.64 mm (0.025 in / 22 Gauge) for walls up to 3.5 m (11.5 ft), and a minimum thickness of 1.0 mm (0.039 in / 18 Gauge) for walls exceeding 3.5 m (11.5 ft).

Studs shall have a minimum depth of 140 mm (5.5 in) to accommodate boxes and piping to be installed in the wall. Coordinate the thickness, as all electrical and mechanical items shall be recessed or flush mounted.

Walls shall be sheathed in fire rated wallboard, such as 16 mm (0.63 in) type X drywall board.

Where partitions abut the deck or vertical structural members, a joint isolator shall be provided to prevent transfer of vibration and structural loads.

Walls and other structural elements shall be designed for minimum deflection and securely fastened, with isolation from all mechanical units, and isolation pads or caulking at the top of the partitions.

For envelope walls separating the computer room from a nonconditioned or exterior space, insulation is to be provided as necessary to stabilize temperature migration. A minimum of R-3.3 K·m²/W (R-19 $\frac{\text{ft}^2 \cdot \text{°F} \cdot \text{h}}{\text{BTU}}$) insulation is recommended.

7.6.4 Nonrated partitions

7.6.4.1 Requirements

In the interior of the computer room, partitions that are not required for rated separation shall be from top of access floor to ceiling above, unless additional height is required for security or environmental control.

Nonrated walls shall be braced at a distance not to exceed every 3 m (10 ft), and as required to meet lateral bracing requirements of the IBC.

Drywall board for nonrated wall shall be 16 mm (0.625 in) type X.

7.6.5 Vapor/moisture seal

7.6.5.1 Recommendations

A moisture/vapor seal should be provided completely around humidity controlled spaces to prevent vapor infiltration to or from the computer room.

7.6.6 Door and glazed openings

7.6.6.1 Requirements

Doors

Doors shall be large enough to move equipment between various data center rooms. Doors must be high enough to allow equipment entry on pallets without tilting.

Doors shall have a minimum thickness of 45 mm (1.75 in), and be a minimum of 1.1 m (3.67 ft) wide by 2.4 m (8 ft) high for a single door, or 1.8 m (6 ft) wide by 2.4 m (8 ft) high for a pair of doors. Doors shall be mounted within steel frames, have a solid core, and be either wood or steel

The primary access door to the computer room shall be a pair of doors, meeting the requirements listed above. These doors shall have neither a center post nor doorsills.

All doors and frames within a rated partition assembly (1-hour or 2-hour) shall be rated at the code required rating of that assembly for occupancy rated separations (NFPA 76 requires fully rated doors). Doors shall have air tight and fire rated weather stripping all around the opening

Glazed Openings

Glazing within doors shall not exceed 0.065 m² (100 in²). These requirements are for equipment and main exit doors to the computer rooms. Where personnel access is required, it should follow the requirements of Section 12.7.2.7.

Glazing within rated doors shall be fire rated, set in metal frames.

Glazed openings within rated partitions shall not exceed code limitations as set by International Building Code Section 7.

Glazed openings within partitions shall be of metal frame construction, with glazing set in continuous stops (such as neoprene) to prevent vibration.

7.6.7 Fire-rated construction

7.6.7.1 Requirements

Walls separating computer room, electrical rooms, battery rooms, mechanical rooms, and separate TRs from other areas within building shall be a minimum of 1-hour separation or as required by applicable codes and regulations.

Doors and frames within a rated wall shall match the rating of the wall construction.

Glazing within a rated wall shall match the rating of the wall. Electrical rooms and battery rooms, as defined by IBC Table 608.2, shall have glazing within the doors only.

Floors above and below the computer room shall be 2-hour rated as defined in IBC Section 7.

See Table 4 for the fire rating of spaces.

Table 4: Minimum Fire Rating Of Spaces

<i>Area</i>	<i>Fire rating of walls</i>
Around computer room area (separating control, computer room, and entrance rooms from other areas)	1-hour rating, full height, slab to slab
Computer room	No rating, floor to ceiling between other equipment (control, and entrance room) spaces, 1-hour rating to other noncomputer spaces.
Control/operations room	No rating, floor to ceiling between processing equipment room and control room, 1-hour rating to other noncomputer spaces such as corridor areas, electrical rooms, and the toilet areas.
Printer room	No rating, floor to ceiling between processing equipment room and control room, 1-hour rating to other noncomputer spaces such as corridor areas, electrical rooms, and the toilet areas.
Critical media storage	2-hour rating, full height
Electrical room	1-hour rating, full height.
Entrance room	No rating, floor to ceiling between computer room and entrance room, 1-hour rating to other noncomputer spaces such as corridor and electrical room
Battery room	1-hour rating, full height
Staging and storage room	No rating, floor to ceiling between processing equipment room and control room, 1-hour rating to other noncomputer spaces such as corridor areas, electrical rooms, and the toilet areas.

7.6.8 Access control systems

7.6.8.1 Requirements

Access control shall be provided at all entrances to the data center and all entrances to the computer room. A system that allows for multiple levels of controls shall be installed to provide for increased levels of security as moving into the data center.

Access control system shall allow for easy modification of access control, be completely programmable, and provide a digital and hard copy of all access to the data center and its various components.

7.6.9 Access flooring system

7.6.9.1 Introduction

An access floor system can be used for the distribution of power and signal cables, HVAC piping, and cooling air through perforated tiles to equipment racks, if the capacity is sufficient for the load.

7.6.9.2 Requirements

Access floor systems are not required; the requirements of this section apply where access floors are used.

Underfloor concrete shall be cleaned and sealed after all major underfloor work has been done, including installation of the access floor system itself.

The access floor shall be a minimum of 450 mm (18 in) above the slab. For higher power density equipment, the access floor shall be a minimum of 600 mm (24 in) above the slab.

The access floor performance shall meet or exceed the minimum specifications listed in Table 5. Additionally, the floor tile or system must have the ability to withstand two times the loads specified in Table 5 without failure.

While concentrated and rolling loads are dependent on the equipment being placed, any equipment being placed shall not exceed the rolling load and concentrated load listed in Table 5.

The building's structural system supporting the access floor must support the access floor and all imposed loads.

All tiles shall be supported at all four sides/corners and the tile surface shall have anti-static properties in accordance with IEC 61000-4-2.

Removal of tiles in unstringered systems or tiles and stringers in stringered systems in an operational data center will destabilize the structural integrity of the access floor. A structural engineer must be consulted to provide a recommended maximum number of contiguous tiles and stringers that can be removed at any one time, and this information must be incorporated into the operational guidelines for the data center.

The space below an access floor shall include a method of fire detection if required by local codes. See Section 11 for additional information.

Table 5: Computer Room Access Floor Performance Specifications

<i>Performance specification</i>	<i>Minimum (medium duty)</i>	<i>Recommended (heavy duty)</i>
Rolling load (access floor panel) Local surface deformation 0.5 mm (0.02 in) Total permanent set 1 mm (0.04 in)	567 kg (1250 lb)	680 kg (1500 lb)
Impact load (access floor panel) Drop weight, dropped from 305 mm (12 in) height on 645 mm ² (1 in ²) local surface with deformation 1.5 mm (0.06 in)	68 kg (150 lb)	79 kg (175 lb)
Concentrated load (access floor panel) Load on 645 mm ² (1 in ²) point with maximum deflection 2 mm (0.08 in) anywhere on the panel	567 kg (1250 lb)	680 kg (1500 lb)
Uniform load (access floor system) Load rating of access floor system, including panels, pedestals, and stringers	732 kg/m ² (150 lb/ft ²)	1221 kg/m ² (250 lb/ft ²)

NOTE: See Section 7.6.9.4 for additional load information

7.6.9.3 Recommendations

For higher power density equipment where the underfloor space is used for cooling, the access floor should be a minimum of 900 mm (36 in) above the slab.

In locations where seismic activity is present, the access floor selected should be designed by the manufacturer for seismic applications, installed in accordance with the manufacturer's instructions, and certified by a professional structural engineer.

Additional structural and operational criteria/factors to consider should include:

- panel drop tests;
- maintaining panel integrity for a given cut-out size;
- pedestal axial loads;
- pedestal overturning moment;
- stringer midspan concentrated loads;
- permanent sets and deformations of any system components;
- pedestal bases should be glued directly to the concrete slab, and not to the epoxied/painted slab.

Refer to Section 14.7.2 for the access floor grid coordinate system to be used to locate equipment in the data center.

Access floors for computer rooms should use a bolted stringer under structure, as they are more stable than stringerless systems. Additionally, access floor stringers should be 1.2 m (4 ft) long installed in a “herringbone” pattern to improve stability. Pedestals should be bolted or “shot” to the subfloor slab for added stability.

Access floor tile cuts should have edging or grommets along all cut edges. If the edging or grommets are higher than the surface of the access floor, they shall be installed so as not to interfere with placement of racks and cabinets. The edging or grommets shall not be placed where the racks and cabinets normally contact the surface of the access floor.

In the case of floor discharge HVAC systems, floor tile cuts should be limited in both size and quantity to ensure proper airflow. Static air pressure should be controlled at all floor tile cuts and openings. Various methods for containing static air pressure are available, including brush systems that can be field fabricated or are commercially available. It is recommended that the HVAC system be properly balanced once all equipment racks and cabinets are in place. The HVAC system should be rebalanced with the addition and removal of floor cuts, equipment racks, and cabinets.

Floor tile openings under cabinets and racks should be no larger than required for entry of cables to minimize loss of underfloor pressure.

7.6.9.4 Additional information

Access floor performance ratings are based on Ceilings and Interior Systems Construction Association (CISCA) standards and TIA-569-B.

Load information as applicable to Table 5:

- concentrated load: the access floor panel’s capability to handle a point or static load. Use CISCA testing guidelines for concentrated load;
- uniform load: the load applied over the entire area of the panel in lb per m² or ft²;
- rolling load (or dynamic load): the access floor panel’s capability to handle movement of equipment on wheels. Rolling loads are determined by the number of passes, the size and hardness of the wheels. Rolling loads typically have a more damaging effect on a panel than a static load;
- impact load: defined by the weight of the load and the height the object is dropped;
- ultimate load: the load at which the panel structurally fails and is sometimes expressed as a multiple of concentrated load;

Hollow steel panels are light and do not create particulates that wood filled or concrete filled tiles can create, but do not have the static or dynamic load capability of filled tiles. Some data centers use a mix of concrete filled steel tiles (in more heavily trafficked aisles and print areas) and hollow steel tiles.

Damage to access floor tiles during move-in can be reduced by temporarily covering pathways with 13 mm (0.5 in) thick plywood or hardboard.

High-pressure laminate (HPL) is a good material for the top surface covering of access floor tiles, as it is easy to maintain and helps dissipate static electrical charge.

7.6.10 Ceilings

7.6.10.1 Requirements

In data center computer rooms and telecommunications spaces (e.g., entrance rooms, TRs), the minimum ceiling height should not be less than 3 m (10 ft) from the finished floor to any obstruction such as sprinklers, lighting fixtures, or cameras. At least 450 mm (18 in) clearance from sprinklers to raceways, cabinets, and racks shall be maintained to ensure that they do not disrupt the sprinkler distribution pattern, subject to the AHJ.

7.6.10.2 Recommendations

The recommended ceiling height for computer room spaces (from slab-to-slab) is 4.5 m (15 ft or greater).

Office type ceilings should not be installed in new data center spaces. Depending on the design for the cabinets and the HVAC solution, there may be a HVAC solution design requirement to provide a ceiling return air plenum. (Refer to Section 14.4.8 for considerations of overhead cable routing). The materials used and the design of this type of ceiling shall consider any need to support cable trays or other cable pathways for overhead cabling in the data center.

Ceiling requirements should consider nonflaking or dusting tiles, vapor resistance, and hold down clips for gaseous fire suppression discharge or high-volume airflow and acoustics.

7.6.11 Equipment bracing system

7.6.11.1 Introduction

Various locations, including high seismic and wind-loading area, will require special attention to the bracing of equipment.

7.6.11.2 Requirements

Equipment cabinets and racks shall be braced in accordance with local codes.

Cabinets braced at the top can utilize the cable ladder rack system, if present, with an attachment that provides rigid four-directional lateral bracing. Equipment mounted on access floors in seismic areas shall be braced to the underfloor slab with an approved method.

7.6.11.3 Recommendations

The bases of cabinets and racks should be braced to the slab as appropriate for the seismic zone in accordance with ASCE 7.

7.6.11.4 Additional information

As an option, lateral movement at base of cabinet may be controlled utilizing a base isolation platform rated for the loading of the cabinet.

7.6.12 Computer room finishes

7.6.12.1 Requirements

Equipment room and related walls shall be finished with nonparticulating water-based epoxy paint finish, smooth finish. Prior to painting, drywall board shall be sealed with a compatible sealing primer.

All penetrations in the perimeter walls shall be completely sealed up to the deck height.

7.6.13 Roof systems

7.6.13.1 Requirements

Data center roofing shall be designed to handle the loading requirements of the roof top mechanical systems.

The roof system shall be designed to provide a continuous seal above the entire data center. Parapets and coping systems shall be of construction to ensure moisture infiltration is prevented.

No penetrations shall be made in roof over the computer room. Additionally, roof drains and leaders shall be kept away from the computer room.

8 Structural

8.1 Code compliance and coordination

Local building codes shall be consulted in the planning and implementation of changes to the building and its mechanical, electrical, and life safety systems. Code references within this standard are generally to the current edition of the International Building Code.

State and local municipalities often adopt international codes by incorporation them into the state or local building code. However, these adoptions often have amendments to specific sections, and the scope of the amendments may be significant. Always check the local amendments before making decisions based on code requirements.

8.2 Impact of site location on implementation of standards

The magnitude of external forces on any structure is a function of its geographic location. Both ASCE 7 and the International Building Code identify the external forces expected to be applied to buildings. The forces identified include:

- lateral loading due to wind;
- lateral loading due to seismic ground acceleration;
- vertical loading due to rain, ice, or snow;
- vertical and/or lateral loading due to soil and hydrostatic pressure.

The vertical and lateral loads identified above may act alone or in combination to exert force on the building. Codes identify a prescribed reduction in magnitude for loads acting simultaneously.

8.3 Types of loading on the structure

Forces exerted on the structure may be increased or reduced according to the code by the application of the following coefficients:

- importance factor – this coefficient yields a higher loading based on the occupancy of the facility such as hospitals, fire stations, 911 facilities, and police stations. It is generally accepted that because of the importance to the end-users, data centers be treated with the same essential facility importance factor, as hospitals, other public safety facilities;
- P-delta effects – the lateral sway usually associated with taller structures and may contribute to an amplification of the loading on columns and beams;
- impact loads – vertical and horizontal live loads may be increased on elements supporting cranes, hoists, and elevators.

All loads on the structure are divided into the following two types:

- dead loads—these are represented as static loads due to the force of gravity on fixed building elements such as beams, columns, walls, equipment, fixtures, conduits, distribution piping, and finishes;
- live loads—these are represented by either static or dynamic loads. Static live loads include occupants, movable equipment, and storable materials, in the external loads given above due to wind, ice, snow, soil, and hydrostatic pressure. Earthquake loads, although dynamic in origin, may be expressed as static loads through a series of code-derived formulas. Volume change forces to the effects of thermal lengthening or shortening of structural elements may also be expressed as static loads. Dynamic loads are those imparted to the structure by the effects of rotating equipment such as generators, rotary UPSs, fans, chillers, and pumps.

Consideration should be given for providing adequate superimposed collateral dead loads to the floor for those elements supported by the floor or collateral suspended loads for those elements suspended above the floor in question.

8.4 Structural concerns specific to data center design

8.4.1 Floor load

8.4.1.1 Requirements

Floor loading (uniform load) shall be a minimum of 732 Kg/m² (150 lbf/ft²) with 122 Kg/m² (25 lbf/ft²) hanging load (weight that can be supported from the underside of the floor). This floor load is adequate for most data center areas.

8.4.1.2 Recommendations

Although some industry standards specify a minimum floor loading of 732 Kg/m² (150 lbf/ft²) with 122 Kg/m² (25 lbf/ft²) hanging load, the recommendation in this standard is uniform load of 1220 Kg/m² (250 lbf/ft²) with 244 Kg/m² (50 lbf/ft²) hanging load to provide flexibility in the location of higher floor loads, such as large storage arrays, printing facilities, and densely populated blade server cabinets. In specific regions of the access floor area where this equipment is located, the structural engineer should be notified of the specific operating weights.

Floors for battery rooms should be designed for a minimum loading of 1220 to 2440 Kg/m² (250 to 500 lbf/ft²), including deck and joists, and 1950 Kg/m² (400 lbf/ft²) for girders, columns, and footings.

Roof areas over battery rooms should be designed to support a suspended load of 146 Kg/m² (30 lbf/ft²).

8.4.2 Wind

8.4.2.1 Recommendations

Figure C6-3 of ASCE 7 provides a map of the United States that illustrates the tornadic gust wind speeds for various locations ranging from 161 km/hr (100 mph) in the west to a maximum of 322 km/hr (200 mph), including the Gulf Coast states.

In the design of data centers, the Enhanced Fujita Scale level of EF3 is commonly used for wind-loading calculations. EF3 yields a ground wind speed for design purposes of between 219 km/hr (136 mph) and 265 km/hr (165 mph). The wind speed is then multiplied by a set of empirical coefficients to translate the effect into resulting kilopascals (pounds force per square foot) lateral load on the facility.

The load is applied to the leeward and windward walls, as well as a translating into the resulting suction on horizontal roof elements. Pressures may increase in areas of discontinuity, such as overhangs, corners, and appendages. Specific attention must be paid to parapets where the effects of vortex shedding can create substantial suction on roof membranes.

8.4.3 Earthquake

8.4.3.1 Recommendations

As previously indicated, data centers are treated as essential facilities because of their mission-critical use, and therefore placed in IBC Occupancy Category IV. The owner may elect to use a reduced occupancy category rating of II if the facility does not have to operate after an earthquake. This places the facility in IBC Seismic Use Group III—recognition of the increased seismic use represents up to a 50% increase in forces generated as a result of seismic excitation.

Earthquake resistant design of structures is complex, since it is imparted to the structure through the foundation as a dynamic load. This means that the response of the building to the earth shaking will be a function of type of foundation system used, type of soil encountered, the magnitude of the earth displacement, the length of time associated with the earthquake, and the location of the structural or equipment elements within the building. It is common for structural engineers to design facilities in such a way that the facility may undergo a permanent deformation, but remain with columns, beams, and floors intact. While this may be adequate for the code-required design of the building to maintain life safety, it is not adequate design for an essential facility such as a data center to remain functioning through the duration of the earthquake.

For data centers, special attention must be paid to the design of specific elements such as access floor structures that will have a direct impact on the survivability of the computer functions during an earthquake. Depending of the height of the access floor and the amount of mass supported, as well as the magnitude of the earthquake for design purposes, it may be necessary to isolate the access floor from the rest of the structure rather than merely bracing the vertical support elements.

Care must be taken in the anchorage of generators, chillers, fans, switchgear, piping and conduit, and racks. The force on the supports for these elements will be substantially increased as a function of their mass multiplied by the dynamic coefficients addressed in the code enforced earthquake design.

Seismic codes are no longer based on zones per the older Uniform Building Code. As represented in ASCE 7, historical maps have been generated to indicate the maximum considered earthquake ground motion to the associated spectral response acceleration for various sites in the United States and its territories, as well as other sites around the world.

Seismic loadings are also a function of the type of lateral bracing system inherent in the structural design of the building. A facility braced by ductile moment resisting steel frame will have a different response to an earthquake than a facility braced with a rigid concrete shear wall system.

Building lateral force resisting systems (LFRS) shall be concrete shearwall with steel building frame.

9 Electrical systems

9.1 Overview

9.1.1 Introduction

Section 9 explains the application of redundancy and the reliability and availability Classes (described in Annex B) to electrical power distribution and availability within a data center. This section also provides both experience-based suggestions and performance-based metrics for each of the Classes in the standard.

The only criterion for securing a given Class is conformance to the performance metrics and values of this section. No endorsement of a given design style is offered nor is any particular type of technology given preference. The project designer and owner should select the system and topology needs for a comprehensive critical power delivery system, whereas the project team should determine the appropriate MTBF and MTTR figures, when combined with the given set of needs, that will offer the most appropriate solution.

At the end of this section is an extensive table denoting requirements for each Class. Table 13 complements the individual sections, further noting system features and requirements for the Classes.

This section will include references to other systems in this standard that, when considered and used together, will yield a strong, coordinated and appropriate critical environment utility system. In the areas of batteries and stored energy systems as well as in bonding and grounding, this section has attempted to extract relevant information from published standards of the IEEE, UL, and other existing industry organizations.

9.1.2 Requirements

Section 9 defines requirements solely as a performance-based criteria. The purpose of such approach to defining Classes is to uncouple them from electrical topologies and applications. Thus, to achieve a given Class, a proposed design must conform to the normal, maintenance, and failure modes of operation. This provides system designers, owners, and equipment manufacturers sufficient latitude in selecting design or product without stifling innovation.

Unless otherwise specified, a data center shall meet the following three requirements specified in this standard for Class F1 or higher:

- the site must have an alternate source of power to the utility equal to the kW requirement of the critical load and all mechanical and facility loads required to maintain operations;
- the site must have an uninterruptible source of power, ac, or dc equal to the kW requirements of the critical load;
- the site and data center must be safely and properly grounded for an information-processing environment pursuant to all codes and standards.

Any data center that does not meet these minimum Class F1 specifications would be considered Class F0.

9.1.3 Availability and uptime

The presence of single points of failure has a direct bearing on the Class achieved by any given system or design. Single points of failure should be eliminated whenever possible, in order to improve redundancy and reliability, both within the data center and support infrastructure as well as in the external services and utility supplies.

The following issues should be addressed:

- Availability and uptime have been used in the industry on an interchangeable basis. With the varying Class ratings, systems or applications availability may not change state as a result of the failure or maintenance of the supporting electrical infrastructure. During these times, selected portions of the underlying electrical infrastructure may be out of service or unavailable. This would retard the electrical system's ability to respond to any subsequent events or failures, which may result in an outage to the IT systems.
- The minimalization to the greatest extent of single points of failure from the electrical systems is a requirement for Class F3 and Class F4 (explained in Annex B).
- Single points of failure have greater consequences the farther they are upstream from the load. The closer they are to an individual load, the smaller the impact is likely to be on the entire system. For example, whereas a failed single branch circuit might affect one load or one equipment rack, the failure of a main circuit breaker can take down an entire distribution panel and all connected loads.
- Redundancy increases both fault tolerance and maintainability, but it also increases system complexity, which is a leading cause of human error outages in data centers. Redundancy and overall system complexity must be weighed against the system capacity, ease of operation, cost and schedule.

9.1.4 Redundancy

Within this document, the following terms describing levels of redundancy are used

9.1.4.1 N (N=Need) or baseline requirement

System meets base requirements for minimum load kW and has no redundancy.

9.1.4.2 N + 1 redundancy

N + 1 redundancy provides one additional unit, module, path, or system in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any single unit, module, or path will not disrupt operations.

For smaller fault-tolerant system where a single module can accommodate the critical load, the N + 1 and 2N models are synonymous.

9.1.4.3 N + 2 redundancy

N + 2 redundancy provides two additional units, modules, paths, or systems in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any two single units, modules, or paths will not disrupt operations.

9.1.4.4 2N redundancy

2N redundancy provides two complete units, modules, paths, or systems for every one required for a base system. 2N is also referred to as “dual-path topology.” Failure or maintenance of one entire unit, module, path, or system will not disrupt operations.

For smaller fault-tolerant systems where a single module can accommodate the critical load, the 2N and N + 1 models are synonymous.

9.1.4.5 2(N + 1) redundancy

2(N + 1) redundancy provides two complete (N + 1) units, modules, paths, or systems. The failure or maintenance of one unit, module, path, or system will still leave intact a system with full redundancy and will not disrupt operations.

9.1.4.6 Multi-N redundancy (xN)

A multi-N system topology is used primarily in fault tolerant or large-scale power systems where more than two large systems are employed together. In such a system topology, the critical load connection at the PDU or the branch circuiting level is the primary means of achieving the redundancy and Class of the system.

9.1.5 Capacity versus utilization efficiency

9.1.5.1 Definitions

The following terms are used in this section

- Capacity: the kW required to serve the load, plus the design margin and growth factors.
- Module loading ratio: comparison of the power (kW) required by the load (IT equipment) to the total installed power (kW).
- Design utilization ratio: a comparison of the total number of power supplies, including those used for redundancy, to the minimum number required to support the load.

9.1.5.2 Overview

Capacity is the power required by the load and is designated as “N”. High-density loads require substantial kW to operate; therefore, a substantial power system infrastructure is required to support them. Higher levels of availability (based on the criticality of the activity supported by the data center) require higher levels of redundancy, which drives the Class described in Annex B.

The size of the system required to serve the load on an N basis (the capacity) should not be confused with the overall system size that would be required for the selected Class. Because higher Classes require higher levels of redundancy and power protection, the highest level of availability will not always have the highest utilization efficiency.

An effective method for communicating the load-required kW versus the total installed kW is the design maximum module loading ratio. Generally speaking, within a given Class, the higher the ratio, the better. Table 6 shows some examples of design efficiency ratios. Design efficiency or utilization efficiency should not be confused with “operating efficiency”, which is a performance characteristic of an installed device or system.

Table 6 displays four different levels of design efficiencies for an N + 1 topology. If N is 100 kVA, N + 1 redundancy can be achieved in any one of the following ways:

- 2 × 100 kVA modules (50%);
- 3 × 50 kVA modules (66%);
- 4 × 33 kVA modules (75%);
- 5 × 25 kVA modules (80%).

Table 6: Design Efficiency Ratios

<i>Topology</i>	<i>UPS or power systems ratio</i>	<i>Design efficiency (required kW/installed kW)</i>
N	1:1	100%
N + 1	2:1	50%
N + 1	3:2	66%
N + 1	4:3	75%
N + 1	5:4	80%
2N	2:1	50%
2(N + 1)	6:2	33%
N + 2	3:1	33%
N + 2	4:2	50%
N + 2	5:3	60%
N + 2	6:4	66%

Class F3 systems are similar to Class F2 on a systems basis, except they possess the second power path. Class F3 and Class F4 systems rarely have design efficiencies over 66%. There is a mathematical point of diminishing returns for large UPS system with the number of distinct plants versus the power paths to the load.

Increasing the number of components beyond the minimum needed results in more components, which usually implies less reliability and a higher probability of failure. Having two 100kVA modules is typically less expensive and more reliable than having five 25kVA modules. However, other factors might be considered. For example, one might choose a higher number of modules because smaller modules may be easier to install and/or to replace; the consequences of a failure in any one of the modules may be less; smaller modularity allows for scalability; and the overall operating efficiency (and operating cost) may consequently be better.

9.1.6 Electrical Class ratings

9.1.6.1 Introduction

This section expands upon the Data Center Facility Availability Classes described in Annex B and provides specific design information of the electrical system for achieving each Class. The standard includes five Classes relating to various levels of reliability of the data center facility infrastructure. The Classes are completely performance related.

The five Classes are:

- Class F0 - The Single Path Data Center without any one of the following: alternate power source; UPS; proper IT grounding.
- Class F1 - The Single Path Data Center.
- Class F2 - The Single Path Data Center with Redundant Components.
- Class F3 - The Concurrently Maintainable and Operable Data Center.
- Class F4 - The Fault Tolerant Data Center.

Several factors can affect Class over the life of the data center, including:

- redundancy;
- capacity;
- expandability;
- maintainability;
- survivability;
- quality.

While some elements of higher Classes are only more expansive versions of lower Classes, there are segments of the electrical systems that make a specific and notable change when jumping between Classes. This can be seen in the change between Classes in the critical power system.

Classes might not be consistent throughout the utility infrastructure systems. Electrical systems are circuited to the loads that they serve, and specifically the mechanical and electrical systems are matched as an integrated approach for the data center and facility as a whole. For example, if the mechanical ventilation system is offered at N + 2, the electrical system must maintain the mechanical system's Class through the electrical system's normal, maintenance and failure modes of operation.

Oftentimes, the electrical system may not possess a consistent Class between different electrical subsystems. This is completely appropriate. While it is desirable to render the electrical system at a consistent Class for the entire electrical system, in many cases, it is often not practical due to cost, space, operability or reliability. To discover the Class need of a given system, criteria needs to be developed that meets the end user's availability and reliability needs for the facility. The purpose of this evaluation is to discover the actual needs for the critical load or constituent components. This "needs assessment" then allows the end user and system designer to choose the most appropriate system for their particular situation. (See Annex B for the general guidelines for the evaluation process.)

As a part of this evaluation process, the end user and system designer need to determine the ability of a given system to respond to normal, maintenance and failure modes of operation and how that system affects their critical facility operations. Therein lies the performance-based definition. The kinds of questions asked when defining a Class are:

- Is the load disconnected with a given outage?
- Is the load disconnected during a given maintenance activity?
- Is redundancy lost with a given outage?
- Is redundancy lost during a given maintenance activity?
- For components that are deferred from the initial construction, can they be added transparently to the existing, operating loads or is a shutdown or some form of accommodation in excess of optimum facility operation required?
- If the system loading changes on the UPS or generator, will that affect the Class?
- How long can the system run with an absence of utility power?

Redundancy increases both fault tolerance and maintainability. However, it also increases system complexity, which is a leading cause of human error. Redundancy and overall system complexity must be weighed against the overall system capacity, ease of operation, cost and schedule. Therefore, while redundancy and the resulting availability figures might be quite good, the time the system is available might be reduced because of the system's complexity and configuration.

While the concept of Classes is useful for specifying the levels of redundancy within various data center systems, circumstances might dictate a combination of Classes. For example, a data center located where utility electric power is less reliable than average might be designed with a Class F3 electrical system but only Class F2 mechanical systems. The mechanical systems might be enhanced with spare parts to help ensure a low mean time to repair (MTTR).

The total data center Class is only as high as the lowest rated Class subsystem. For example, the overall data center would be rated Class F2, with a Class F2 mechanical system, even though it has a Class F3 electrical rating.

NOTE: There is no allowance for a plus or minus rating to a Class, and the use of terms such as Class F3+ are not recognized by this standard.

It should also be noted that human factors and operating procedures could also be very important. Hence, the actual availability of two Class F3 facilities may vary widely.

9.1.6.2 Class F0 description

Industry description:	Single path
Component redundancy:	None
System redundancy:	None
Power sources available to critical load:	One
UPS sources available to the critical load:	None (Optional)
Ability to be maintained while under load:	No
Ability to recover from failures:	No
Resulting definition:	Single path/single module/single source/no backup

A Class F0 electrical system is an infrastructure with no generator and/or no stored energy system (such as a UPS). The system cannot be maintained while it is operating. A failure of any element in the power path will likely result in the loss of electrical service to the load. Some form of power conditioning, such as voltage regulation or surge suppression, may be available, but a loss of utility power will almost definitely result in dropping the load. Single points of failure are common throughout the system. Any downtime, whether planned or unplanned, will result in critical load interruption.

A representation of a Class F0 topology is shown in Figure 14.

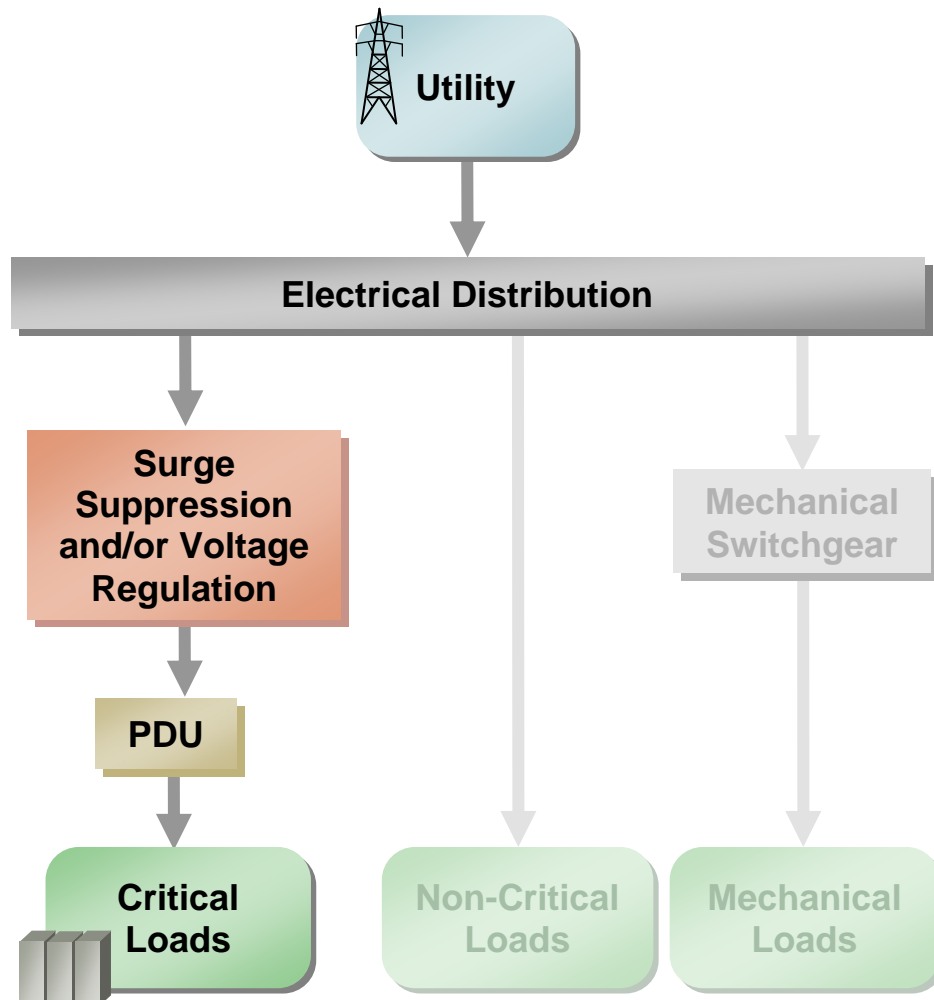


Figure 14: Class F0 Electrical Concept Diagram

9.1.6.3 Class F1 description

Industry description:	Single path
Component redundancy:	N
System redundancy:	N
Power sources available to critical load:	One
UPS sources available to the critical load:	One
Ability to be maintained while under load:	No
Ability to recover from failures:	No
Resulting definition:	Single path/single module/single source

A Class F1 electrical system is an infrastructure with no redundancy. This system cannot be maintained while it is operating and a failure will likely result in a loss of electrical service to the load. Single points of failure are common throughout this system. Critical load interruptions are likely during planned and unplanned downtime.

A representation of a Class F1 topology is shown in Figure 15.

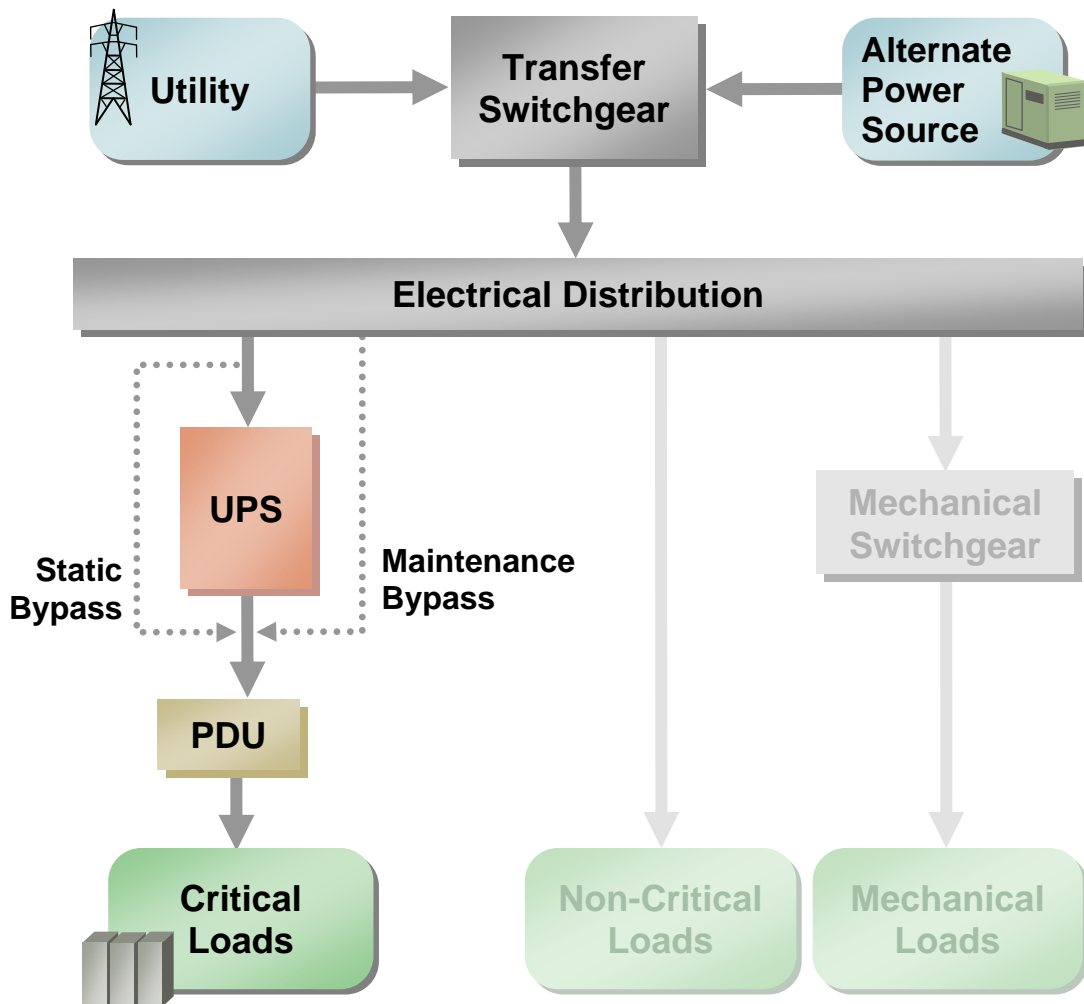


Figure 15: Class F1 Electrical Concept Diagram

9.1.6.4 Class F2 description

Industry description:	Single path with redundant components
Component redundancy:	N + 1
System redundancy:	N
Power sources available to critical load:	One
UPS sources available to the critical load:	One
Ability to be maintained while under load:	At the system level only, but not in the distribution system
Ability to recover from failures:	Only at the system level.
Resulting definition:	Single source/multiple module/single path

A Class F2 system possesses component redundancy but does not have system redundancy. Redundant components may exist on an N + 1 and paralleled basis in the UPS and/or generator systems, but a Class F2 system does not offer redundancy in the distribution system. A failure in the N + 1 components may not result in a load failure, but would reduce the redundancy level in the systems to N. This system has a single electrical supply to the load and no source diversity. Any failure in the distribution system will likely result in a loss of electrical service to the load. Large-scale system maintenance can't be performed without interruption to the load.

Single points of failure are present in the distribution system, and critical load interruptions are likely during both planned and unplanned downtime. A representation of a Class F2 system is shown in Figure 16.

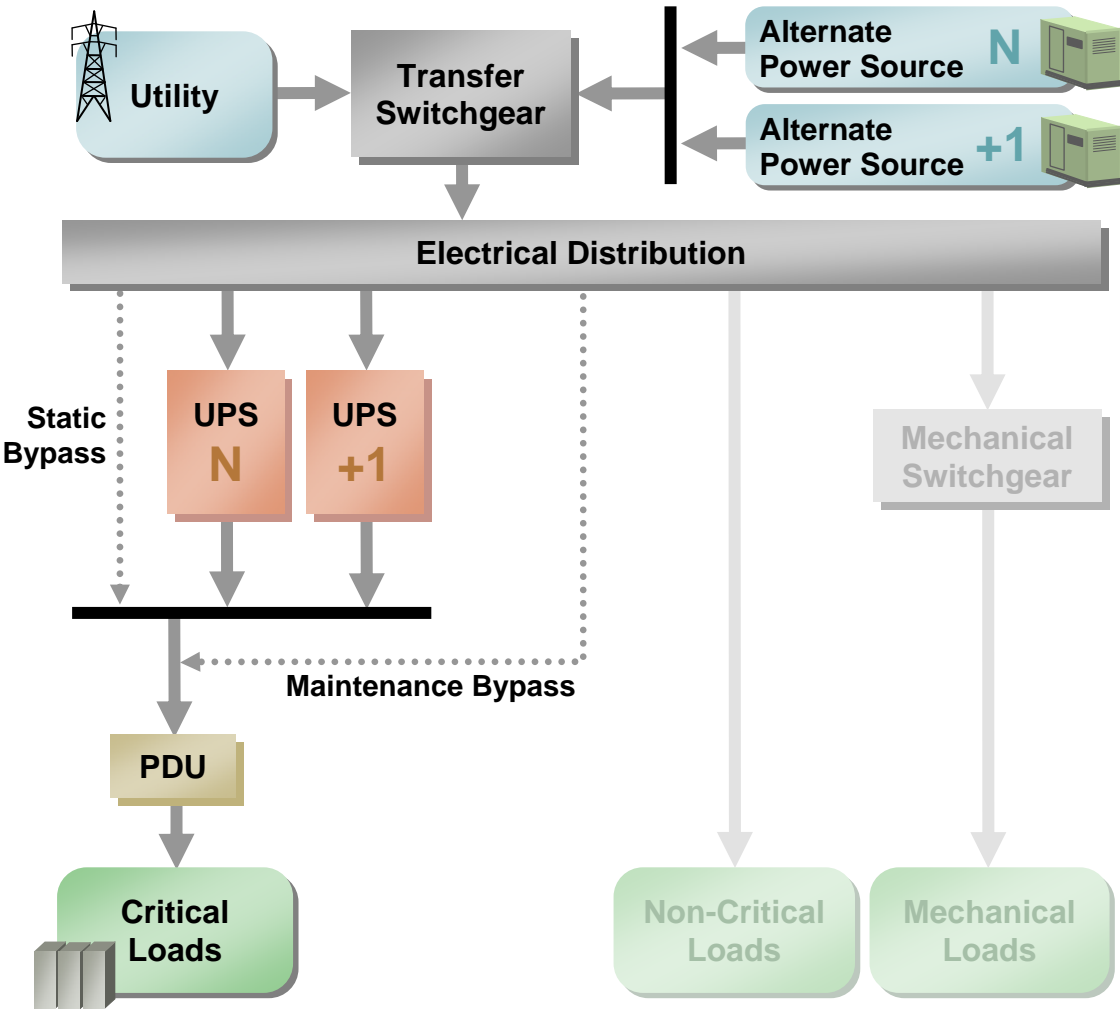


Figure 16: Class F2 Concept Diagram

9.1.6.5 Class F3 description

Industry description:	Concurrently maintainable & operable
Component redundancy:	N + 1, as a minimum
System redundancy:	N
Number of utility sources:	One source with two inputs or one source with single input electrically diverse from backup generator input.
Power sources available to critical load:	Two
UPS sources available to the critical load:	One UPS system with one UPS power path to the load.
Ability to be maintained while under load:	Yes, with a reduction of the system redundancy from N + 1 or better to N during maintenance activities.
Ability to recover from failures:	At the plant and distribution level, but with a reduction of the system or distribution redundancy from N + 1 or better to N after failure and prior to the recovery.
Resulting definition:	Multiple source/N rated single or multimodule system/dual or multiple path

The Class F3 system possesses redundancy in the power paths to the critical load, but only one of those paths needs to be UPS-powered. The alternate path may be UPS-powered, but this Class requires that it only be available and dedicated to the IT load. On a dual-corded IT device, one input would be fed from the UPS power system, while the other input is fed from the non-UPS source.

The individual critical power systems are rated for a portion of the total load, with a common and centralized dedicated UPS system providing the redundant supply to the line systems. The redundant system, similar to the line systems may possess either a single or multiple modules. This concurrently and maintainable system provides load source selection either via static transfer switches or by the internal power supplies in the IT systems themselves. There are no single points of failure in either the critical power system or the power systems supporting the mechanical or vital house/support loads. The Class F3 system allows for complete maintenance during normal operations (on a planned basis), but it loses redundancy during maintenance and failure modes of operations. STSs are required for single corded loads to provide power redundancy where no IT component redundancy exists. STSs are not required for dual-corded loads.

All maintenance and failure modes of operation are transparent to the load.

Two representations of a Class F3 system are shown in Figures 17a and 17b.

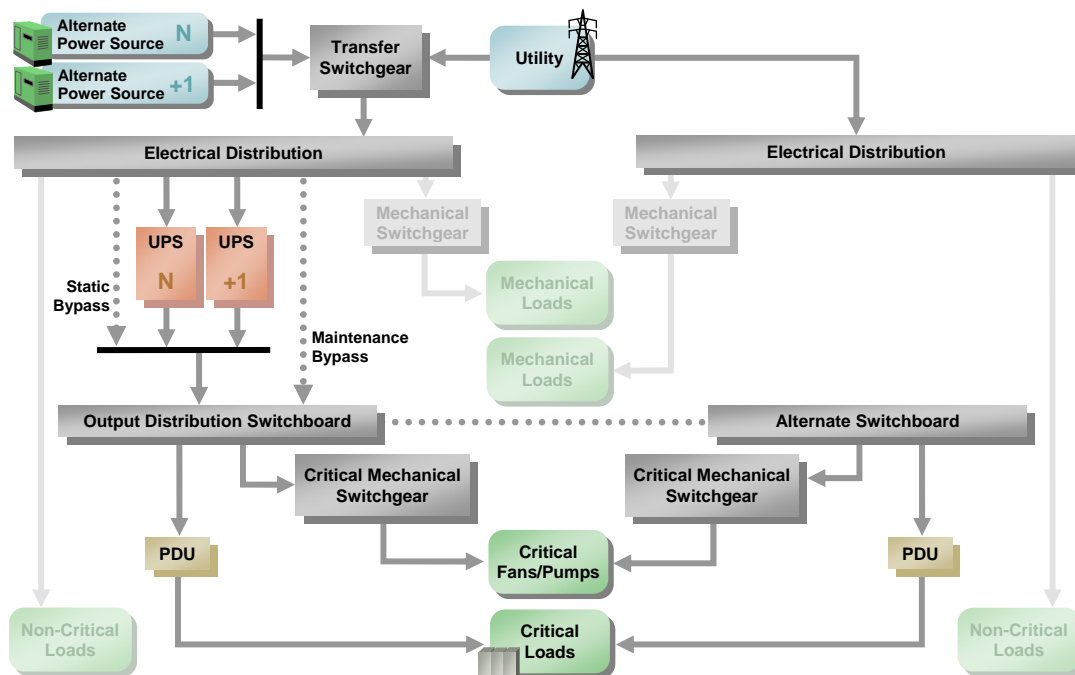


Figure 17a: Class F3 Single Source Single Utility Input

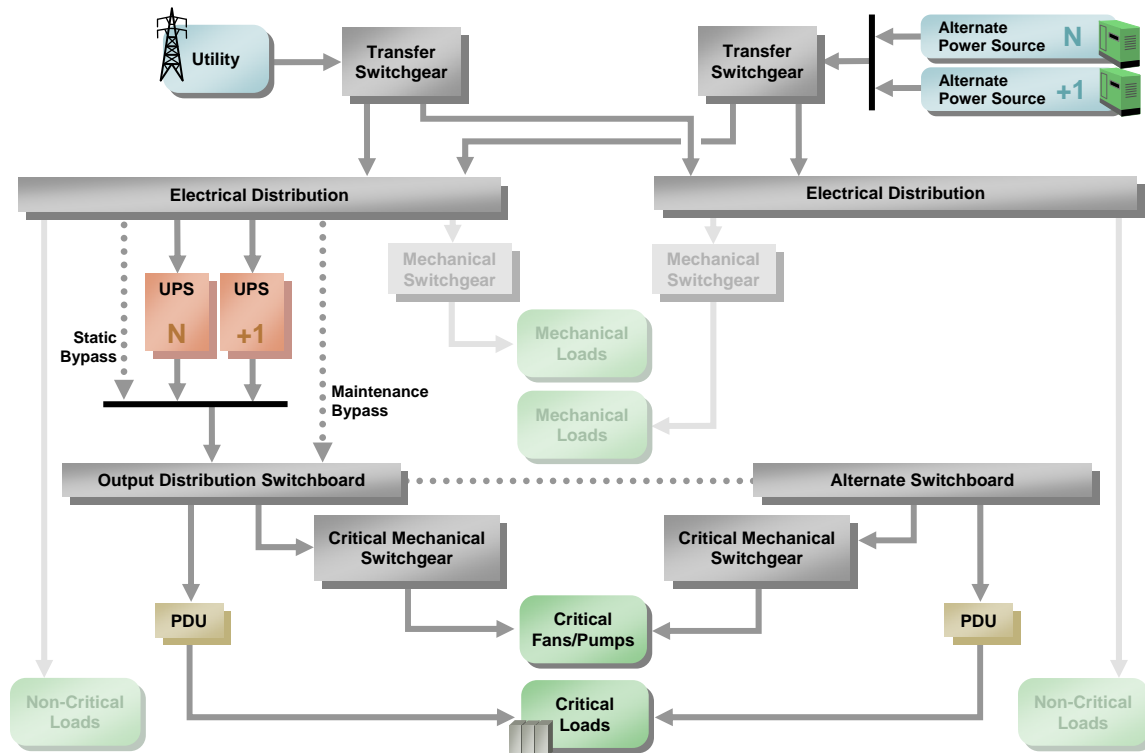


Figure 17b: Class F3 Single Source Two Utility Inputs

9.1.6.6 Class F4 description

Industry description:	Fault tolerant
Component redundancy:	Equal to or greater than $N + 1$.
System redundancy:	Yes
Number of utility sources:	Two or more
Power sources available to critical load:	More than two
UPS sources available to the critical load:	Two or more
Ability to be maintained while under load:	Yes, with a reduction to no worse than $N + 1$ during maintenance activities.
Ability to recover from failures:	Yes, automatically with a reduction to no worse than $N + 1$ after the failure and prior to the recovery.
Resulting definition:	Dual or Multiple sources / 2 ($N+1$ or better) power systems / multiple paths with redundant components.

This system possesses redundancy in the power paths, and there may be more than two independent sources of UPS power to the critical load. The individual critical power systems are rated for the complete load for the $2(N+1)$ /System-Plus-System option. For larger loads, the system may have multiple UPS systems, where the system diversity is provided solely by the connection of the critical loads to the multiple UPS systems. Each UPS system could be a multimodule (paralleled) UPS system or a single/high-kW UPS system. The Fault Tolerant system provides load source selection either via static transfer switches or by internal power supplies in the IT systems themselves. There are no single points of failure in either the critical power system or the power systems supporting the mechanical or vital house/support loads. The Class F4 system allows for complete maintenance during normal operations, and does not lose redundancy during either failure or maintenance modes of operations.

All maintenance and failure modes of operation are transparent to the load.

Redundant components should be compartmentalized and separated in different rooms to enhance survivability.

Continuous cooling is required for ITE. Typically this will require fans and pumps to be on UPS power.

The Class F4 representation for a Shared/Distributed Redundant and $2N$ are described in Figures 18 and 19.

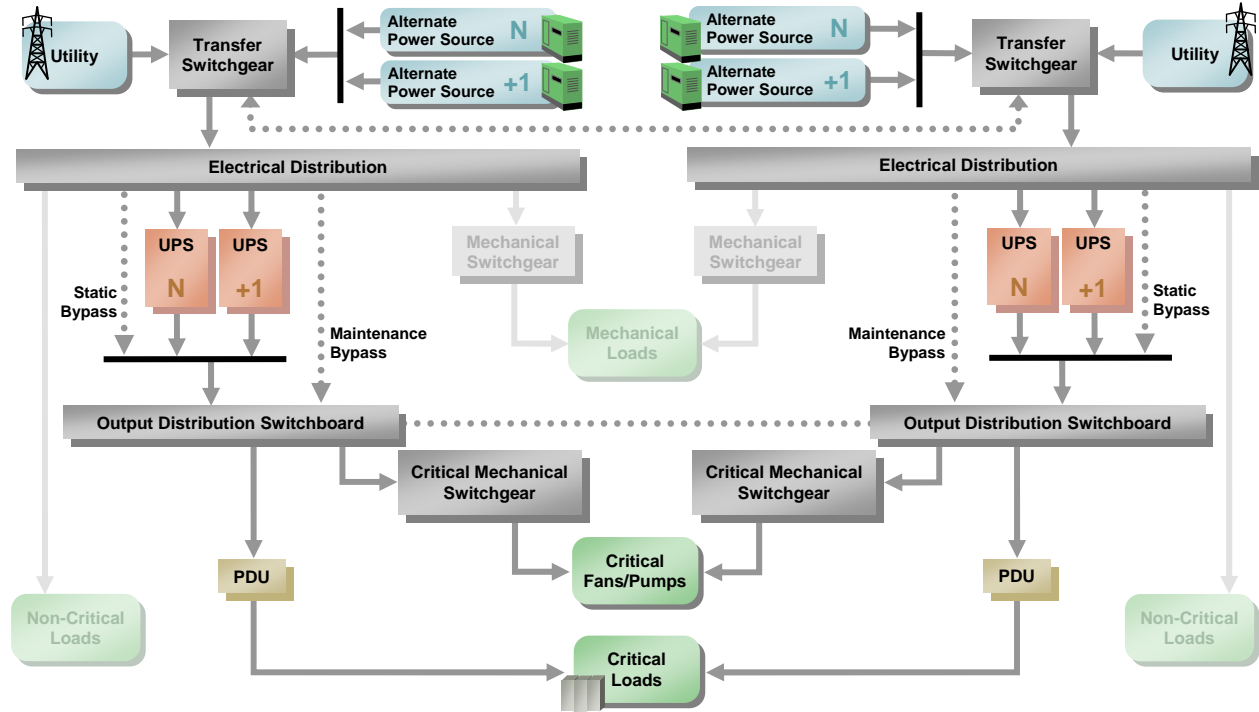


Figure 18: Class F4 Electrical Topology (System-Plus-System)

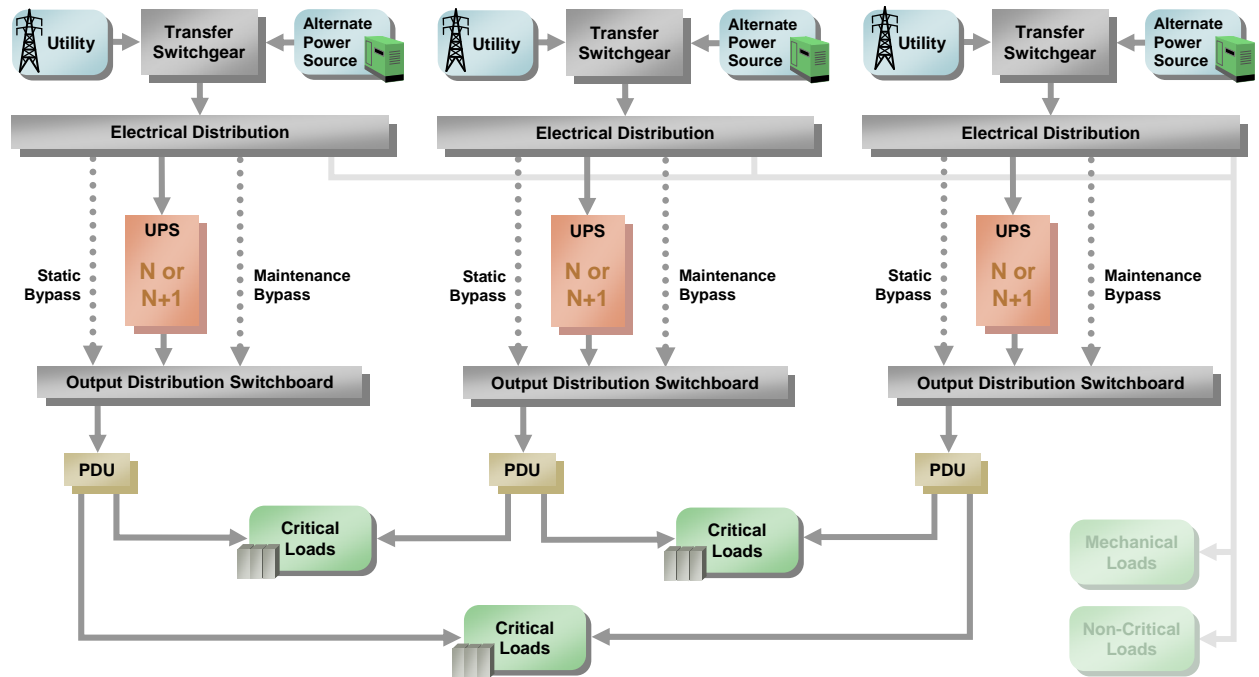


Figure 19: Class F4 Electrical Topology (xN Or Distributed Redundant)

9.2 Utility service

9.2.1 Utility service planning

9.2.1.1 Recommendations

When considering the power services to a given site, the utility should be treated the same as the generator sources. While it is not possible to control the utility, it does constitute an N source to the facility.

Several planning issues concerning the utility service should be considered. For example, consideration should be given to what other utility customers are served by the same utility feeder. Hospitals are desirable neighbors because they typically receive high priority during outages or are classified as a no-shed block in the utility's distribution system. Industrial users are not preferred desirable neighbors, due to the transient voltage disturbances and harmonics conditions they often impose on the feeders and the utility systems. Many of these conditions either can reduce the life of the data center's systems, especially the batteries and UPS modules, or require other sophisticated power quality mitigation measures.

While planning for utility services, the following issues should be addressed:

- Is there a need for a dedicated service based on the load size or redundancy requirements for the site?
- Is the site on a shared service and, if so, is anyone else on the service?
- Are there any high impulse loads on the bulk substation such as foundries, paper plants, and smelters that would have an impact on power quality?
- Is service to the site primarily overhead or underground?
- What are the initial and the ultimate capacities of the service and how can these services be expanded if needed?
- Are diverse services available?
- Are diverse services routed separately to the site?
- What are the service voltages in the area?
- What are the requirements for closed transition operation, if employed?
- What are the circuit protection requirements that the site must provide?
- What are the service construction requirements?
- What are the reliability and availability of the service to the site?
- What is the available fault duty at the main switch?

This analysis occurs during the preliminary project phases with the utility company's service representative to the user or area. The purpose here is to ascertain the electrical performance, short circuit duty, and power quality for the utility.

Underground utility feeders are preferable to overhead feeders to minimize exposure to lightning, weather, trees, traffic accidents, and vandalism.

There is no mandatory service voltage. It is left to the designer and user to select the service voltage that is appropriate for the site's data center power system from among the voltages available from the utility. However, in most countries, the incoming supply voltage options are decided by the electricity supply company based on the required load.

When diverse services are utilized, the designer should establish the point of common coupling of the supplies with the utility company. The supplies should be routed to the site separately and should enter the data center on opposite sides of the property and building. In this situation, a bond is required between systems to ensure an intersystem grounding reference.

An intersystem grounding reference for diverse services can be accomplished by a building ground (electrode) ring. See Section 9.9.6 for requirements and recommendations for a building ground (electrode) ring.

9.2.2 Low-voltage utility services

9.2.2.1 Introduction

Low-voltage utility services do not exceed 600 VAC between line conductors in North America and 1000 VAC elsewhere.

Service entrance distribution equipment provides several functions - the interface between the utility and the site, the distribution of utility power to downstream systems and in some cases, the transfer controls and transfer point between the utility and generator.

9.2.2.2 Recommendations

The distribution equipment should be designed for growth, maintenance, and the ultimate load expected for the facility while maintaining the Class level's redundancy. The utility distribution equipment should either be sized for the ultimate load for the site or should possess the ability to add capacity later without undue disruption to ongoing operations.

When the service entrance distribution equipment is double-ended (with two utility entrances), the tie breakers should be provided in pairs. This allows the complete isolation and maintenance of one side of the distribution equipment, while the opposite side carries the load.

Consider

- using switchgear with compartmentalization in lieu of switchboard with open construction for greater resiliency and separation of components to minimize internal damage due to faults.
- using drawout or withdrawable circuit breakers to allow addition or maintenance of circuit breakers without interrupting power to operating equipment.
- arc flash hazards when designing distribution equipment. Lower arc flash hazard ratings may allow preventative maintenance and infrared scanning to be performed more often and allow safe operation of operating equipment.

Circuit breakers should be interchangeable where possible between spaces and distribution equipment line-ups. Careful consideration should be given to breaker standardization throughout the entire project. Concurrent maintainability of any system is directly related to its Class level.

9.2.2.3 Additional information

Low-voltage services may require utility-controlled disconnecting means at the property line. The local fire department might also require a shunt trip for the complete disconnection of power to the site when they respond to a fire.

Surge protection devices (SPDs) should be provided for all Classes to mitigate problems due to switching surges or transients from sudden power outages.

9.2.3 Medium-voltage utility services**9.2.3.1 Introduction**

Medium-voltage utility services are 601 VAC to 35 kVAC between line conductors in North America. Elsewhere, voltages greater than 1000 VAC are considered to be "high voltage." See Section 9.3.8 regarding service connections.

9.2.3.2 Requirements

A medium voltage service has the same requirements as the low-voltage service but the medium voltage service may have different grounding criteria. The service configuration may be in concert with the generator plant configuration acting together as multiple sources or providing an input to various unit substations located in the data center facility.

9.2.4 Protective relaying**9.2.4.1 Requirements**

The use of protective relaying is based primarily upon how the service is delivered and whether transfer between the utility(s) and the onsite generator plant(s) are either closed- or open-transition. Multifunction relays are typical, but the utility may require utility-grade, individually mounted relays. The utility will also typically extend its relaying specification to any closed-transition systems.

9.3 Distribution**9.3.1 Requirements**

The distribution system shall consider the number and diversity of the power paths to the loads, the ability to readily maintain the loads, and the ability to recover from failures.

Common to all systems is the type of termination for cables and busway connections. See Table 12 for busway and cable connections.

9.3.2 UPS rectifier or motor inputs

9.3.2.1 Requirements

Paralleled module inputs shall be fed from the same unit substation or distribution point, where all modules in the paralleled system must have the same input. Distributed or individual modules in larger UPS systems may be fed from their different upstream substations or distribution systems as long as those systems possess some form of output or load-side synchronization.

9.3.3 Static switch bypass inputs

9.3.3.1 Introduction

All solid state UPS systems and some rotary UPS systems have static bypass capability. Its function is to automatically transfer load between the UPS and an alternate power source without human intervention when the UPS system controls detect a condition in which the UPS cannot function properly.

9.3.3.2 Requirements

For UPS systems with a static bypass switch, either a single power module system's controls or a paralleled system's control cabinet shall be synchronized to the static system input.

9.3.4 UPS system bypass

9.3.4.1 Introduction

A maintenance bypass provides a manually operated and closed-transition power path external to the static bypass power path. A maintenance bypass allows the UPS module(s), paralleling controls, and static switch to be totally deenergized so that unscheduled remedial or scheduled preventive maintenance can be safely performed.

9.3.4.2 Requirements

Maintenance bypasses shall be provided for all Class F1 through Class F4 systems.

Isolating circuit breakers shall be provided to allow for the maintenance of the UPS collector bus, static switch or output breaker.

9.3.5 Power strips

9.3.5.1 Introduction

Power strips allow multiple corded IT devices to plug into a single branch circuit.

9.3.5.2 Requirements

Where used, power strips shall comply with the following requirements:

- Only Code-allowed connections, such as junction boxes, shall be allowed under the access floor.
- Power strips shall be listed for information technology equipment (ITE).
- Power strip ratings shall be coordinated with the upstream breaker and wiring system.
- Power strips shall be positively and mechanically attached to the cabinet interior.
- Multiple power strips mounted in a cabinet shall bear proper labeling and shall be organized not to interfere with network cabling. Similarly, power strips shall be located in order to minimize crossing of the distinct power supply cords (e.g., A and B) as they are routed to the power strip from the IT platform.

9.3.5.3 Recommendations

Where used, power strips should comply with the following recommendations:

- Metering may be provided on individual power strips. The ability to monitor power strip loads remotely via a centralized monitoring system is recommended for high-density and large-scale facilities.
- Power strips should not have internal surge suppression.
- Power strips should not be placed under the access floor.

9.3.6 Input source transfer

9.3.6.1 Introduction

When considering the top layer of the electrical distribution system, the first consideration is the management of the utility and generator sources and the transfer scheme most appropriate for the facility. Similarly, the transfers may occur within a self-contained system such as an automatic transfer switch (ATS) or via a circuit breaker transfer pair. Another consideration is the ability to bypass the transfer location either via a bypass power path in an ATS or in another circuit breaker transfer pair in a separate or double-ended switchboard system.

For many sites, the generator system as a whole powers the entire site or building. Should this be the case, the generator controls, and the input source transfers become part of the utility's service entrance equipment. In this case, the utility metering and circuit protection may be included in the transfer controls.

For transfer protocols, there are four families of controls:

- open transition;
- closed transition/quick transfer;
- closed transition/load walk-in;
- closed transition/parallel operation.

Regardless of the transfer protocol, a utility outage always results in an open transition transfer because of the loss of sources and the resulting utility dead bus.

9.3.6.2 Open transition

9.3.6.2.1 Introduction

Open transition occurs when the transfer between sources breaks before the opposite connection is made. This transfer technique is the most common, requires the least amount of electrical controls and relaying to assure its success, and typically does not require the utility's approval to deploy. The downside to this technique is that any transfer between energized and available sources results in a brief load disconnection. The loss of mains power forces the UPS to draw upon its stored energy source, thereby reducing the UPS battery system's life. It also typically causes the mechanical system (air conditioning systems) to stop and restart, thereby putting stress on the equipment and creating a potentially sharp increase in heat.

9.3.6.2.2 Recommendations

Open transitions should be several seconds long to allow power supply capacitive energy to dissipate.

9.3.6.3 Closed transition/quick transfer

9.3.6.3.1 Introduction

In the closed transition/quick transfer the utility and generator (and consequently, the site) are paralleled for less than 100 ms to up to one minute, depending on the utility provider and designer. The paralleling time is typically the operating time of the ATS or the breaker transfer pair. The primary benefit of this method is that there is no load interruption between the two energized and available sources. The downsides to this technique are that:

- it requires substantially more controls and relaying than open transition;
- the electrical system's short circuit duty must account for both the utility's and the site generator's contribution;
- the transfer can hang up if the sources are present and do not remain synchronized within voltage and frequency tolerance (which would prevent the transfer);
- capacitive or harmonic feedback from the load(s) can sometimes cause logic errors;
- the utility may not always allow this type of operation in a customer's system.

9.3.6.3.2 Recommendations

Close coordination with the utility is vital in this instance.

9.3.6.4 Closed transition/load walk-in

9.3.6.4.1 Introduction

The closed/transition/load walk-in varies from the closed transition/quick transfer technique in that the generator and utility share load for a period of several seconds or as long as a minute or two. This can be very desirable, as it places a substantially less amount of stress on the site's electrical system and eliminates load inrush. The downside is that it requires a substantial amount of relaying and forces a complex sequence of operation in the electrical system.

9.3.6.4.2 Recommendations

Close coordination with the utility is vital in this instance.

9.3.6.5 Closed transition/parallel operation

9.3.6.5.1 Introduction

In the closed transition/parallel operation the generator and utility share load for an indefinite period of time. This can be for peak shaving or cogeneration purposes. The downside is that it requires a substantial amount of relaying and forces a complex sequence of operation in the electrical system.

9.3.6.5.2 Recommendations

Close coordination with the utility is vital in this instance. Review of environmental restrictions will be required.

9.3.7 Generator controls and paralleling

9.3.7.1 Introduction

Generator systems can be either distributed or paralleled for any of the Classes. Some generator control systems consist of traditional switchgear systems, while some systems utilize controls on board the generators and ATS's. Regardless of the method or technology used, the controls must match the Class requirements to achieve the overall availability demanded by the critical, mechanical, and house power systems. Specific consideration should be given to paralleling switchgear systems that might represent single points of failure. While a paralleled generator system may offer an N + 1 or N + 2 level of redundancy for components, the single paralleling bus or the master controls may represent a single point of failure. Paralleling switchgear should be provided with fully redundant paralleling controls for Class F3 and Class F4 applications. Generator controls address numerous critical functions for the site and generator systems.

These functions may include:

- automatic load control and assumption upon loss of the utility source;
- retransfer to utility once it is restored after a preset retransfer delay;
- exercise and maintenance rotation of the engine(s);
- distribution of generator power to any remote source transfer locations.

9.3.7.2 Recommendations

Generator controls for individual machines should not be centralized, and each controller should be completely contained on the generator skid or within the generator control module in the switchgear line-up. The generator control section or module should possess all controls and metering for the individual machine, and will not require any form of outside influence or connection for its individual operation. Individual machines should be able to operate regardless of the availability of the paralleling controls.

The enclosure or room where generators are installed should be temperate, but not necessarily conditioned. Draw-out type switchgear is recommended for Class F3 and Class F4 facilities, but also may be used for lower Classes. Standby power systems should be installed in a manner that allows for 360-degree maintenance and technician access to the machine, both while it is operating and while it is not.

The primary switchgear should be designed to handle all projected requirements, as this equipment is difficult to replace once the data center is in operation. The system should be designed to allow for maintenance and expansion pursuant to the site's ultimate load requirements.

Paralleled generators should be capable of manual synchronization in the event of failure of automatic synchronization controls. Consideration should be given to manual bypass of each generator to feed directly individual loads in the event of failure or maintenance of the paralleling switchgear.

See Sections 9.3.16, 9.7.2, and 9.10 for other requirements.

9.3.8 Unit substations

9.3.8.1 Introduction

Unit substations may combine several functions at one location: the medium voltage input selection or utility input, a step-down from the utility or site's medium to low voltage, utility metering, low-voltage power distribution, and input source control. These systems can utilize multiple medium-voltage inputs from different upstream sources, provide medium-voltage transfer systems (primary selection) or a low-voltage transfer system (secondary selection), and may be double-ended for further source and distribution redundancy.

9.3.8.2 Recommendations

The unit substations may be located where the normal-alternate transfer is addressed on the input side of the system, or serve as the upstream input to downstream ATSs. For larger systems, the input source transfer may occur at the input main (one from the utility, and one from the generator or alternate system) where it is coupled with a dedicated alternate power input. Unit substations are routinely located immediately upstream of the UPS power plant, major mechanical loads and the noncritical systems.

See Sections 9.3.16, 9.7.2.1, and 9.10 for other requirements.

9.3.9 UPS system

9.3.9.1 Introduction

The project designer and end user should determine the precise distribution topology that is most appropriate to the final design based on the client's needs.

While the static UPS system is the prevalent technology used, the requirements of this section apply to all types of UPS technology.

Power system distribution addresses six areas:

- UPS module rectifier inputs;
- static system inputs;
- maintenance and external bypass inputs and configurations;
- output switchboard configuration;
- output switchboard ties and alternate power paths;
- multi-system UPS power system synchronization.

These systems are considered to reside between the unit substations and the critical power distribution switchboards.

One of the key issues for UPS systems is grounding simplicity and the prevention of harmonic circulation (this problem is reduced for modern IT loads). In this case, the discussion for all of the UPS power system assumes a 3-wire input and output, with 4-wire systems only being used for stand-alone UPS systems where the step-down transformer is part of the output transformer function of that module and for 400/230V UPS systems.

For Class F1 and F2 systems, UPS power distribution is basically linear, with no crossties or mixing of loads. For Class F3 systems, multiple second power paths emerge (albeit not all required to be UPS-powered). The goal for the Class F3 model is to provide multiple power paths as close to the critical load as possible.

For the Class F4 model, UPS power topology may include different numbers of UPS power plants versus the number of UPS power delivery paths. For example, there may be a site with 3 or 4 distinct UPS plants but many more individual UPS power distribution systems. Therefore, numerous UPS power distribution systems can be connected below a given UPS plant.

Bonding and grounding is further discussed in Section 9.9.

9.3.9.2 Bypass switch inputs

9.3.9.2.1 Introduction

The bypass system directly affects the Class of any UPS system. The static bypass, the maintenance bypass, the output breaker, and any load bank testing connections can all have a direct impact on the maintenance and failure response of the UPS system.

Class F0 systems (in which a UPS is optional) and Class F1 systems might have a single input into a UPS system in which a static bypass circuit is tapped internally to the UPS module (see Figure 20). For all other Classes, the static bypass has a dedicated input circuit.

As with all components of the electrical system, the ability to maintain a system while operating is a foundation of Class F3 systems, and maintaining a power path and redundancy are required for a Class F4 rating.

Bypass configurations can affect UPS functionality as follows:

- combining maintenance bypass and static bypass paths will typically result in a lower Class because it reduces the ability to remove a module or system without interrupting the service to the downstream critical loads;
- load bank connections that are independent of the UPS output source can contribute to a high Class because they allow for testing without interrupting the service to the downstream critical loads;
- locating circuit breakers on the collector bus or on the output bus of paralleled UPS systems rather than making them internal to a power module will contribute to a high Class by allowing a module to be removed from the service without shutting down the entire system. These are also known as Isolation breakers.
- The presence of a maintenance bypass will allow for the removal or testing of a UPS module or for the replacement of a static switch in the event of a catastrophic failure. This has a dramatic effect on the Mean Time To Repair (MTTR), and as a result, the ultimate Sigma figure.

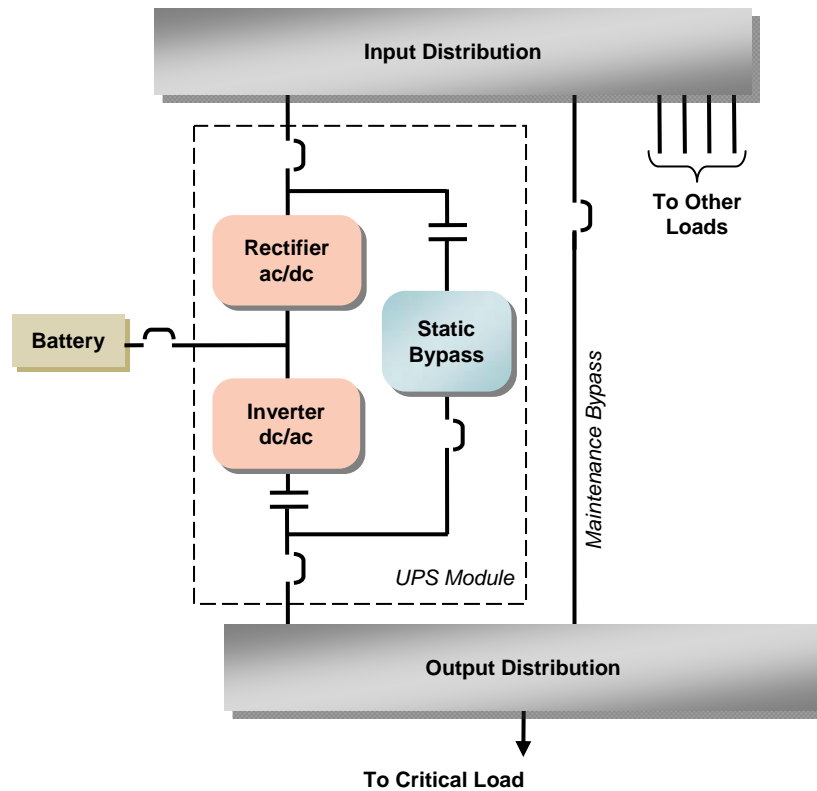


Figure 20: Single-Module UPS With Internal Static Bypass And Maintenance Bypass From The Same Source

External maintenance bypasses (see 9.3.4) are optional for Class F0 (when UPS is present), Class F1, and Class F2 systems. Maintenance bypass is mandatory for all Class F3 and F4 applications and for system control cabinets. As discussed in the preceding paragraphs, static bypass inputs may be combined with the rectifier inputs on Class F0, Class F1, and Class F2 applications. The static bypass is the recommended means by which to synchronize the UPS to its maintenance bypass (see Figures 23 and 24 and discussion on figures 25 and 26). Classes F1 through F4 all require some form of maintenance bypass (whether it is factory provided in the bypass cabinet/system or externally developed).

Permanently installed load banks are optional for all Classes and are included at the discretion of the designer. They are not included in all of the examples in the figures below.

9.3.9.2.2 Requirements

Refer to Figures 21 and 22. When the inputs to the rectifier, static bypass and maintenance bypass are from the same input distribution bus, the designer shall consider the capacity of the input distribution bus and how the critical load could be affected during testing. The capacity of the input distribution bus shall be able to support the critical load on the maintenance bypass plus the full load testing of the UPS system. Also, if the input bus supports other loads, such as in a Class F1 or Class F2 design, those loads shall be considered in the capacity calculation of the input bus. The designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS.
- Testing of other loads connected to the same bus.
- Turning on and off other loads connected to the same bus.
- Fault conditions.

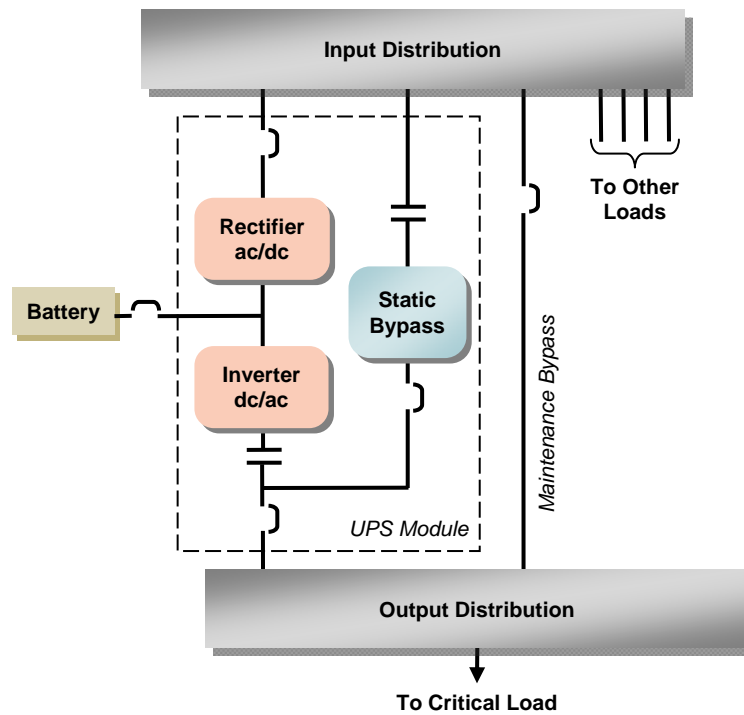


Figure 21: Single-Module UPS With Inputs To Rectifier, Static Bypass, And Maintenance Bypass From The Same Source

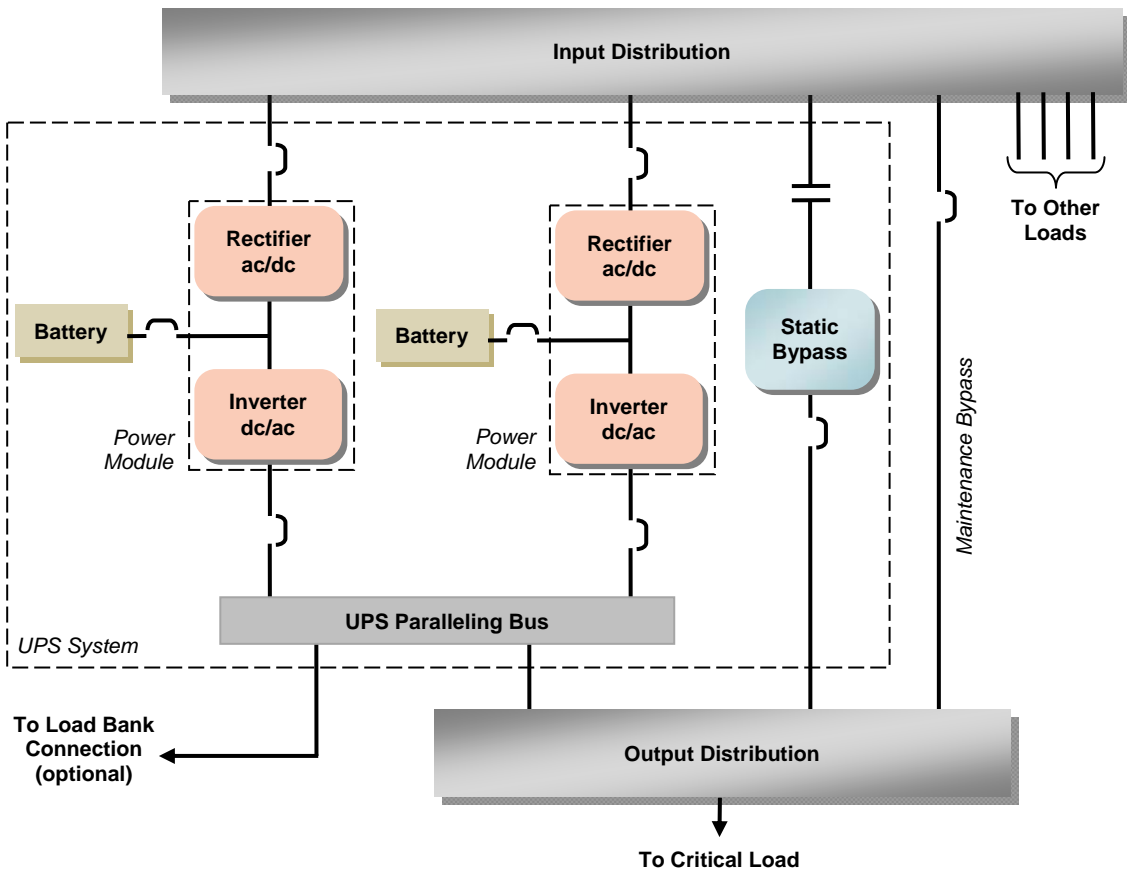


Figure 22: Multiple-Module UPS With Inputs To Rectifier, Static Bypass, And Maintenance Bypass From The Same Source

Refer to Figures 23 and 24. When the input to the rectifier is from one bus and the static bypass and maintenance bypass originate from a different bus, the designer shall consider:

- the capacity of the input distribution bus;
- the sources of power to the static and maintenance bypasses; and
- how the critical load could be affected during testing or if a fault were to occur on that bus.

For testing purposes, when the two bypasses are derived from the same input distribution bus, then the capacity of the input bus should be able to simultaneously support the critical load on the maintenance bypass plus the full load testing of the UPS system (e.g., full load transfers to and from static bypass). In addition, if any other loads are present they shall also be considered in the capacity calculation of the input distribution bus. The designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS.
- Testing of other loads connected to the same bus.
- Turning on and off other loads connected to the same bus.
- Fault conditions.

In normal mode, the UPS shall synchronize its inverter to this bypass source. Therefore, if the bypass source has a disturbance the UPS will more than likely go into an alarm state. When the static bypass input is lost for a system, the UPS system shall run in a free mode until either the static bypass input has been restored or the paralleled UPS controls asserts a lead module on the system. There is one additional scenario to consider for this configuration. In the event a repair or fault removes the input distribution bus from service, the static bypass source will be lost and will place the UPS system into a less reliable operating mode.

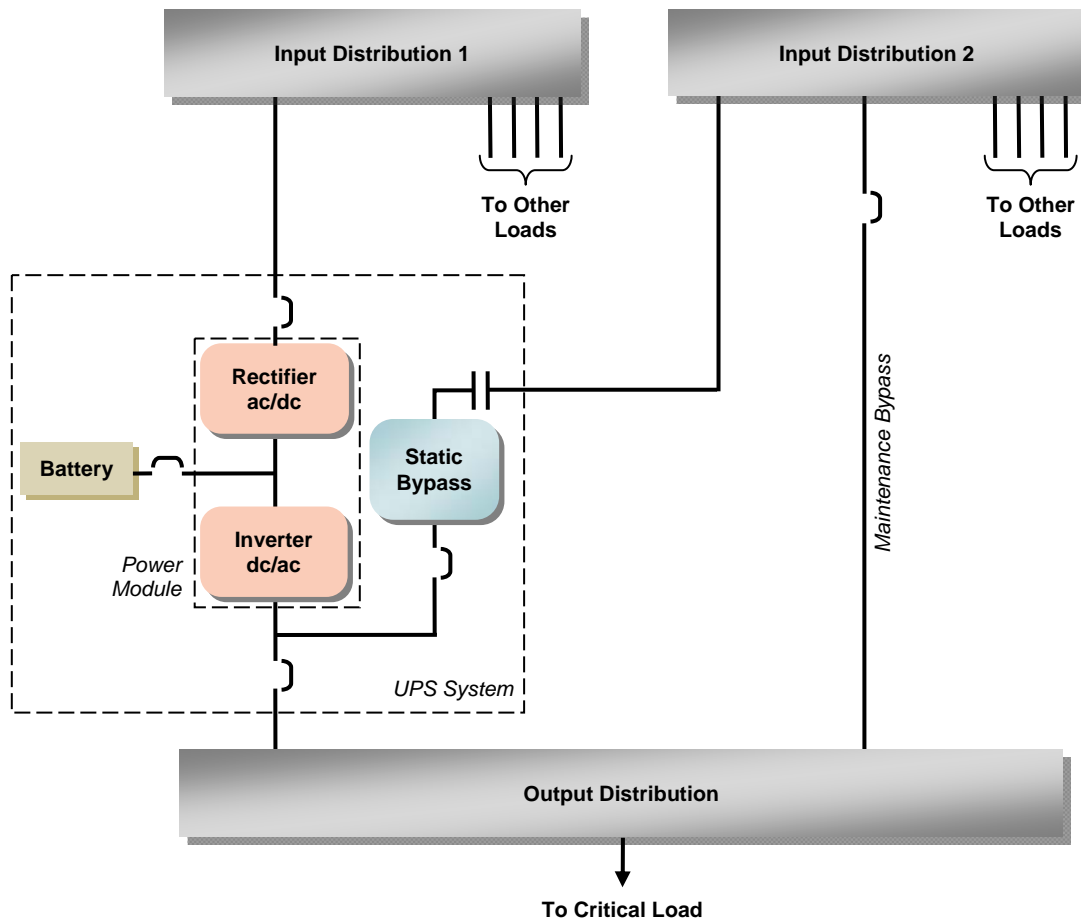


Figure 23: Single-Module UPS Bypass—Alternate Bypass Source - Input To Rectifier From Primary Source; Inputs To Static Bypass And Maintenance Bypass From A Second Source

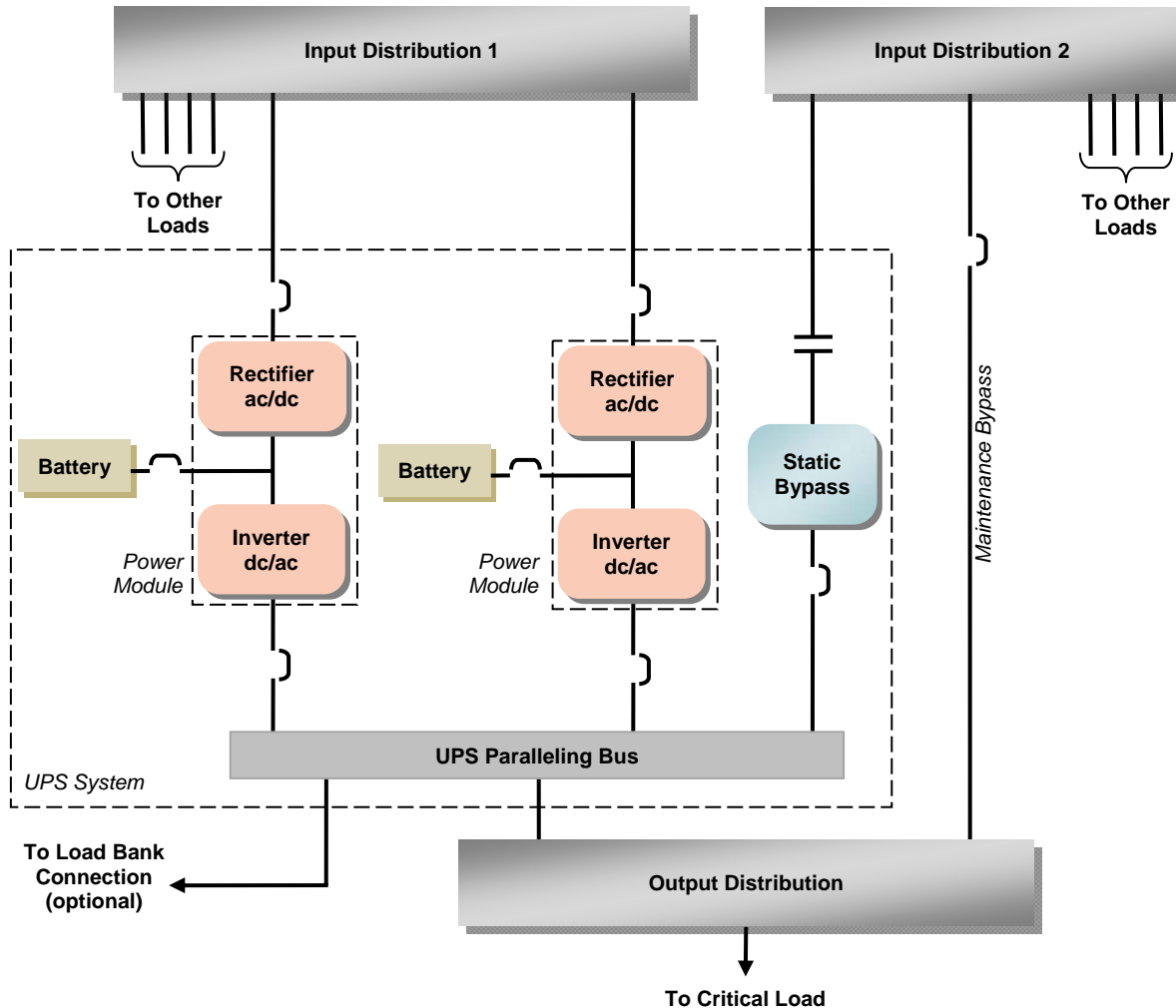


Figure 24: Multiple-Module UPS Bypass—Alternate Bypass Sources - Inputs To Rectifiers From Primary Source; Inputs To Static Bypass And Maintenance Bypass From A Second Source

Refer to Figures 25 and 26. When the input to the rectifier and the static bypass originate from one bus (Input Distribution 1) and the maintenance bypass originates from a separate bus (Input Distribution 2) the critical load shall be transferred without interruption or disturbance to an isolated source, either utility or generator depending on the design, while the UPS is repaired or tested. When other loads are connected to the bus that supports either the rectifier and static bypass (Input Distribution 1) or the maintenance bypass (Input Distribution 2), the designer should also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS.
- Testing of other loads connected to the same bus.
- Turning on and off other loads connected to the same bus.
- Fault conditions.

Inputs to the static bypass and maintenance bypass shall not be derived from separate sources, as shown in Figures 25 and 26, unless the two sources are synchronized in phase and frequency. Lack of synchronization will result in an unreliable design that should require open transition (i.e., shut down the loads and then restart from the alternate source).

Note that synchronization of sources is difficult because load imbalances and phase shifts (such as transformers introduced downstream) can force circuits out of synchronization. The best practice is to power both the static bypass and the maintenance bypasses from the same source as shown in Figures 23 and 24. (See also 9.3.9.3).

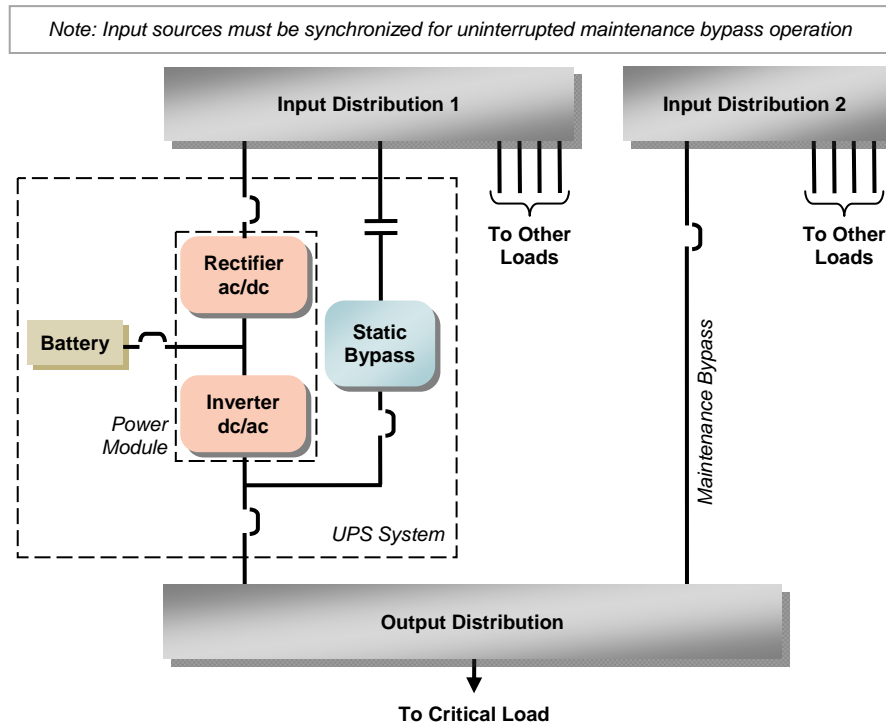


Figure 25: Single-Module UPS Bypass—Multiple Bypass Sources - Inputs To Rectifier And Static Bypass From Primary Source, And Input To Maintenance Bypass From A Second Source

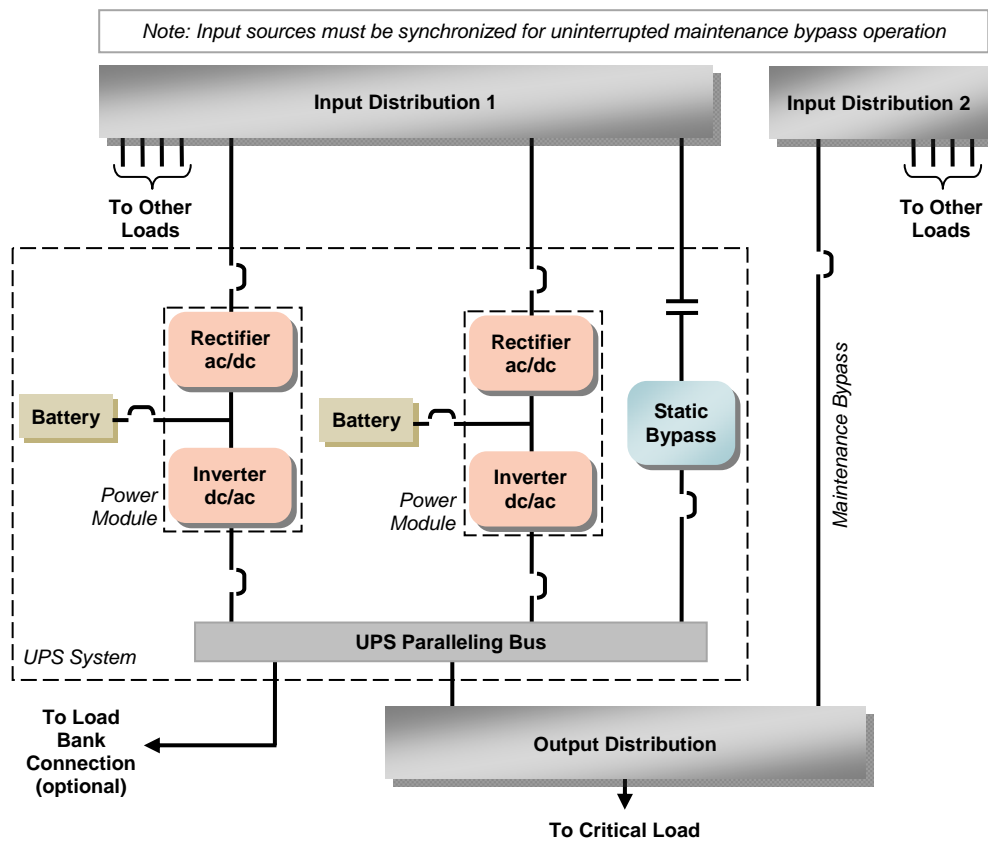


Figure 26: Multiple-Module UPS Bypass—Multiple Bypass Sources - Inputs To Rectifiers And Static Bypass From Primary Source, And Input To Maintenance Bypass From A Second Source

9.3.9.2.3 Recommendations

The UPS system static bypass and maintenance bypass designs should consider the following:

- Closed transition transfer mechanisms should be fed from the same source or type of source. Normally this would require the power module inputs, static bypass input, and the maintenance bypass input to be synchronized to the same source. Depending upon the configuration, some UPS could be excepted from this rule when the static bypass input and the output of the UPS are synchronized. For example, input to power module inputs could be fed from utility 480 VAC wye source “A” while the static bypass and maintenance bypass could be fed from utility (or generator) 480 VAC wye source “B”. This is explained in more detail in subsequent paragraphs.

A dedicated input to the static switch that is separate from the rectifier input allows the critical load to further sustain faults that could be associated with the rectifier. In Class F0 and Class F1 applications, a single source of input power for both the rectifier and the static bypass is permitted (see Figure 21).

In Class F2 applications, a single source of input power to the rectifiers and to a static bypass is permitted (see Figure 22), but best practice is to provide an input path to the static bypass that is discrete from the rectifier input (see Figure 23). Momentary-duty equipment is allowed where designs incorporate individual modules into the topology.

Fully-rated static bypass switches with dedicated inputs are recommended for all Class F3 and Class F4 applications and for all paralleled system control cabinets (see Figure 23).

If proper breaker coordination has been completed, the input(s) to the rectifier(s) should be selectively protected from a static input breaker failure.

Table 7: Static Bypass Switch Input, By Availability Class

<i>Class</i>	<i>Description and Input source(s)</i>
F0	(UPS optional) Single power module with a single input to both the rectifier and the static switch
F1	Single power module with inputs to both the rectifier and the static bypass switch from the same source
F2	Single or multiple power modules; all power module inputs from the same source; static bypass switch input may be from the same source as the power modules or from a separate source
F3	Multiple power modules; all power module inputs from the same source; static bypass switch input from a separate source
F4	Multiple power modules; all power module inputs from the same source; static bypass switch input from a separate source

9.3.9.3 Synchronization

9.3.9.3.1 Introduction

Synchronization can occur in one of two ways for UPS systems:

- actively based on some form of external control system;
- passively by the management of the static switch inputs to the given modules or via active systems specific to the UPS manufacturer, depending upon the chosen UPS topology.

The active systems offer excellent synchronization functionality, especially when the UPS system uses batteries. The passive system is important, as vital system transfers are assured to be coordinated when the static inputs are managed and considered in the design. A lack of input or output synchronization could result in a failure of ASTS operation or an out-of-phase transfer, thereby resulting in a dropped load and possible equipment damage.

9.3.9.3.2 Requirements

UPS systems shall be synchronized in one of two ways:

- Line-side (source) synchronization.
- Load-side (output) synchronization.

In either event, synchronization is vital and shall be required for a high-reliability system at the Class F3 and Class F4 levels. Since Class F0, Class F1, and sometimes Class F2 systems are single module/single plant systems, no external synchronization is required.

When system-level synchronization is not possible, static switching at the loads or critical power buses may be required.

9.3.9.4 UPS output switchboards

9.3.9.4.1 Recommendations

Output switchboards directly support the PDU and ASTS systems downstream of the UPS power plants. For Class F1, F2, and F3 systems, UPS outputs should be vertically organized to the UPS output distribution system downstream. Simpler electrical topologies may not have separate UPS output switchboards and critical power distribution switchboards.

For Class F3 systems, the second path may be derived from a non-UPS source. For Class F4 systems, there may be multiple power paths, but these are kept separated until they meet at the critical load.

Section 9.3.14 discusses the UPS power distribution downstream from the UPS output switchboards and how these loads are served by these diverse power paths.

9.3.9.5 Ties and interconnections

9.3.9.5.1 Introduction

As long as the UPS sources are synchronized and are not overloaded, UPS systems may transfer load between each other. Except on a plant level, the UPS is the foundation of the multicorded system for critical loads. All transfers are done via closed-transition, and the control systems for this type of operation are typically redundant or offer some other form of manual operation in the event that the control system fails.

9.3.9.5.2 Requirements

System ties are common in system-plus-system configurations, and several UPS system manufacturers offer pre-engineered solutions for this design feature. For xN or other types of UPS topologies, the system designer must engineer a solution for the given UPS module and plant configuration.

9.3.9.5.3 Recommendations

Ties and interconnections should also prevent the propagation of failures and should limit short circuit fault current. See Section 9.7.2 for monitoring requirements.

9.3.10 UPS output distribution

9.3.10.1 Introduction

UPS output distribution switchboards are located immediately downstream of the UPS Power plants and extend to the PDU or data processing room levels. One important consideration for these systems is that they do not have to follow the redundancy level or plant counts found in the UPS Power plants.

For example, for Class F1 systems, the UPS output distribution switchboards are single units. For Class F2 systems, there may be module redundancy, but there may not be UPS power path redundancy. In both cases, UPS systems would match the total UPS power paths. In a Class F3 system with a single UPS power plant, there are at least two UPS output powered critical distribution switchboards, one on the active path and one on the alternate, or non-UPS path. For a Class F4 system, there are at least two critical power switchboards, if not more.

A summary of the UPS output distribution switchboard counts and configurations for each Class are shown in Table 8.

Table 8: Summary Of UPS Output Switchboard Counts For Classes

<i>Class</i>	<i>UPS power plants</i>	<i>UPS power paths</i>	<i>UPS output switchboard count</i>
F0	One	One	One
F1	One	One	One
F2	One	One	One
F3	One	One or two	Two
F4	Two or more	Two or more	Two or more

9.3.10.2 Recommendations

UPS output distribution switchboards may come in numerous specifications and configurations, all depending on the maintenance and failure mode of the critical loads downstream and UPS systems upstream. The UPS output distribution switchboards may be in any of the following configurations:

- standalone or double-ended:

Standalone switchboards are typically used for Class F1 and Class F2 applications, or for Class F3 and F4 systems where load is not shared amongst UPS system in pairs. Double-ended or interconnected switchboards are typically found in systems where critical load is shared between a pair of systems or UPS power paths, where they may be interconnected for inter-UPS output distribution redundancy. The switchboard configuration is most centrally related to the ability to shift load off an individual switchboard for maintenance. Some designs use the UPS paralleling switchgear or the UPS output distribution switchboard as a vehicle for closed transition load transfer and sharing either via chokes or static switching. This switch is located between the output buses and acts as a tie between them. The switch may feed the load directly or just provide lateral relief for maintenance or failure recovery. This concept is illustrated in Figure 27.

- automatic versus manual controls for source transfer:

As this section has stated, controls are locally operated. Failure mode response is always automatic (and that might mean doing nothing and letting other system components swing the load around), while maintenance mode response is always manual.

- always closed transition to avoid load interruption:

Since the UPS output distribution switchboards are located downstream of the UPS system, any switching operations need to be closed-transition (make-before-break) to avoid load interruption.

The diversity and configuration of the UPS output distribution switchboards is at the discretion of the system designer and user.

An example of critical power switchboard interconnection and diversity is shown in Figure 27.

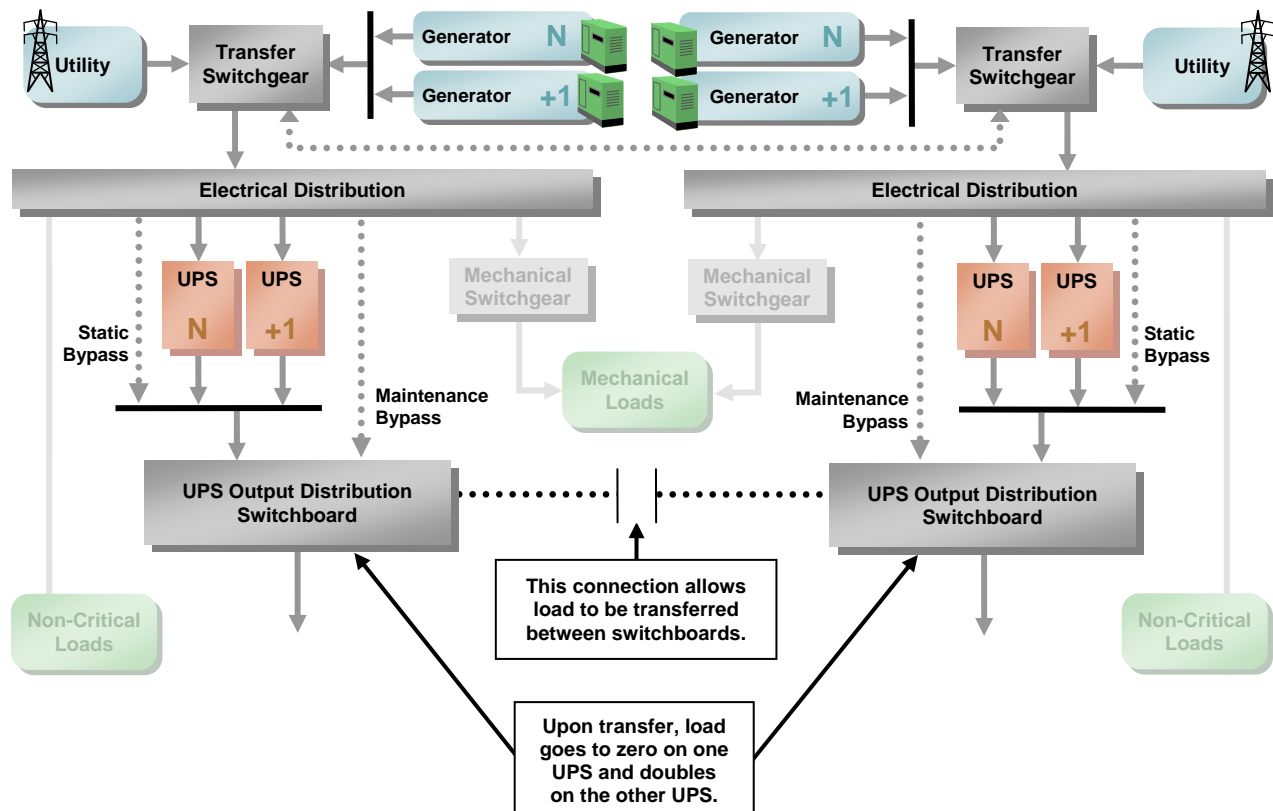


Figure 27: An Example Of An Approach To UPS Output Switchboard Load Management

9.3.11 Power distribution units (PDUs)

9.3.11.1 Introduction

While most PDUs in North America have transformers, this is not typical in countries where the nominal voltage is already 230/400 V. PDUs with an isolation transformer create a separately derived neutral for downstream loads, although this may not be necessary for 3-phase loads or for a systems in which the load utilization voltage is created at the UPS. PDUs with transformers convert the output voltage of the UPS system to the utilization voltage of the critical loads as needed. Regardless of the application, the PDU always has output branch circuit panelboards or distribution circuit breakers that serve the downstream critical loads or subpanelboards serving downstream critical loads. The overcurrent protective devices are usually circuit breakers, although fuses are sometimes used for dc distribution systems.

9.3.11.2 Recommendations

A PDU is usually provided as a fully integrated, factory-tested, and listed product. In addition, the term “PDU” can be applied to a combination of site-connected elements, including a transformer, metering, controls, and power distribution panelboards. Where harmonics could be a concern, a K-factor rated transformer or a harmonic cancelling transformer may be used.

If the PDU has an isolation transformer it should be coordinated to UPS inrush tolerances for normal, failure and maintenance modes of operation. Low inrush transformers may also be employed depending on the UPS system’s design. Where it is anticipated that one or more loads will generate large harmonic currents, a K-factor transformer may be rated to K-9, but may also be as high as K-13 or K-20. Although some legacy equipment may generate harmonic currents, most ITE today creates little or no harmonics, so a K-factor-rated transformer may not be cost justified.

The PDU may possess the following attributes:

- It may be a stand-alone system or may be coupled with a static switch for the management of single- or poly-corded IT loads.
- It may have single input or dual input depending on the UPS system topology.
- It typically has a harmonic-tolerant transformer, coordinated to UPS inrush tolerances for normal, failure and maintenance modes of operation, rated to K-9, but may also be K-13 or K-20. Low inrush transformers may also be employed depending on the UPS system’s design and circuit breaker selection.
- It should have larger-than-standard wiring gutters for easy circuiting.
- Consider efficiency ratings at the expected operating loads, pursuant to local energy guidelines. Specify no load and loaded losses at 25%, 50%, 75%, 90% and 100% loads.
- It should have taller base plate for the ready connection of conduit for underfloor cabling applications.
- It should be located where thermographic testing can observe all critical connections, circuit breakers and transformer cores while operating.
- PDUs can be grouped together with other PDUs from alternate UPS power output sources, such as the A and B systems collocated for matched circuit impedance and direct wiring. However, for higher Classes it may be desirable to maintain physical separation of all elements in the critical power path as much as possible.

For a PDU pair using a static switch, the load connections for single-corded and dual-corded devices might appear as illustrated in Figure 28. Within a rack or cabinet, an automatic transfer switch (either separate or integrated within a power strip) should be installed for all single-corded loads.

See Sections 9.3.16, 9.7.2, and 9.10 for other requirements.

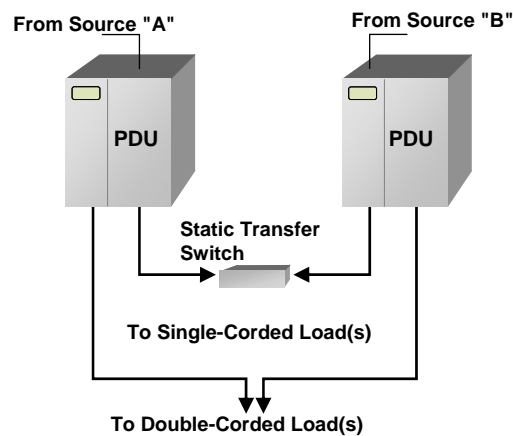


Figure 28: PDU Configuration: Single-Corded And Poly-Corded Devices

9.3.12 Automatic static transfer switches

9.3.12.1 Introduction

Automatic static transfer switches (ASTS) are used in power systems where subcycle, high-speed source switching outside of the ITE is desirable. The operation of ASTS's is similar to that of mechanical ATS's in that the ASTS automatically transfers on loss of preferred source or retransfer on loss of alternative source when preferred source has returned. A majority of ITE comes either single- or dual-corded with some newer systems IT devices requiring multiple-corded loads (some IT devices require 3, 4, 5, or more cords). When this occurs, the ASTS allows for a multiplication of the UPS power distribution paths without the multiplication of the UPS plants.

Other loads vital to the data center's operation include temperature control and building monitoring systems, operation or control room video and control systems, security systems, and single-corded IT systems. At the Class F0, F1 and F2 levels, where the UPS power distribution and circuiting systems are single path, static switches are not typically utilized.

9.3.12.2 Recommendations

Since ASTSs represent a single point of failure (because they, like the loads they support, are single output systems), their use needs to be balanced with the overall reliability and failure mode analysis for the critical power distribution system. The ASTS can provide reliable recovery for an unexpected input source loss, but by its nature, it is a complex system that will cause the loss all of the downstream loads if it fails.

Features of the ASTS might include:

- Solid state transfer systems (e.g., silicon control rectifier [SCR]), instead of mechanical contacts seen in ATSS.
- Dual-input and bypass-able for all loads—some ASTSs have been specified and built as three input systems, but these are typically custom units.
- Rack-mounted or floor-mounted options.
- Control systems that allow for transfer control within a few phase angle degrees.
- Fault-tolerant internal controls and wiring systems if needed.
- Mated to PDUs for numerous transfer and distribution options.

See Figures 29 and 30 for examples of transformer and distribution system configurations utilizing ASTS.

See Sections 9.3.16, 9.7.2, and 9.10 for other requirements.

9.3.13 Direct current power systems

9.3.13.1 Introduction

DC power systems that serve critical loads are common in two forms:

- the primary power source for access provider and carrier equipment;
- as an alternative to ac power in computer rooms because of energy efficiency, design simplification, and ease of paralleling alternative energy sources.

9.3.13.2 Recommendations

Direct current power systems that serve critical loads have the same availability requirements as ac power systems, with additional consideration given for personnel safety. Traditional power distribution methods may not be adequate for higher voltage dc power systems (as defined by AHJ).

While substantial research is underway, few sites have begun deploying critical dc power systems. Some have done so in an effort to improve data center power efficiency (a dc power system removes at least two levels of power conversion - the dc-ac conversion at the UPS output and the ac-dc conversion at the ITE), to reduce feeder critical power counts and to improve power quality.

While dc-based critical power systems are an emerging and potentially viable option for the mission-critical environment, insufficient data exists to offer design guidance in this standard.

9.3.14 Computer room equipment power distribution

9.3.14.1 Introduction

Unlike upstream UPS plants and critical power distribution, distribution to the critical loads must be exactly mapped to the redundancy of those loads and the cord and circuit diversity that they require.

The upstream systems must be able to deliver the source diversity to the computer room circuiting under normal, maintenance and failure modes of operation as prescribed in the Class performance descriptions.

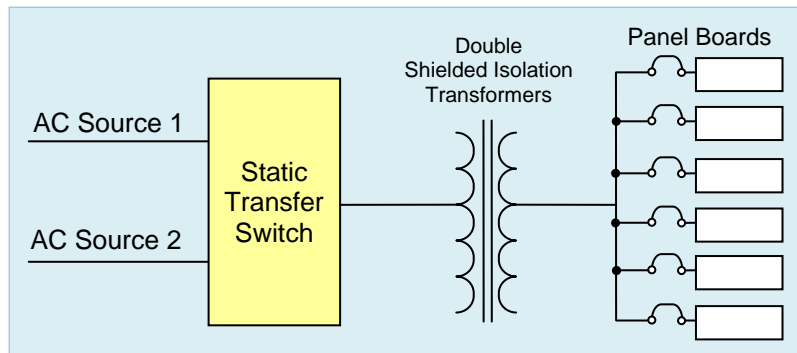


Figure 29: Automatic Static Transfer Switch - Single Transformer, Primary Side Switching

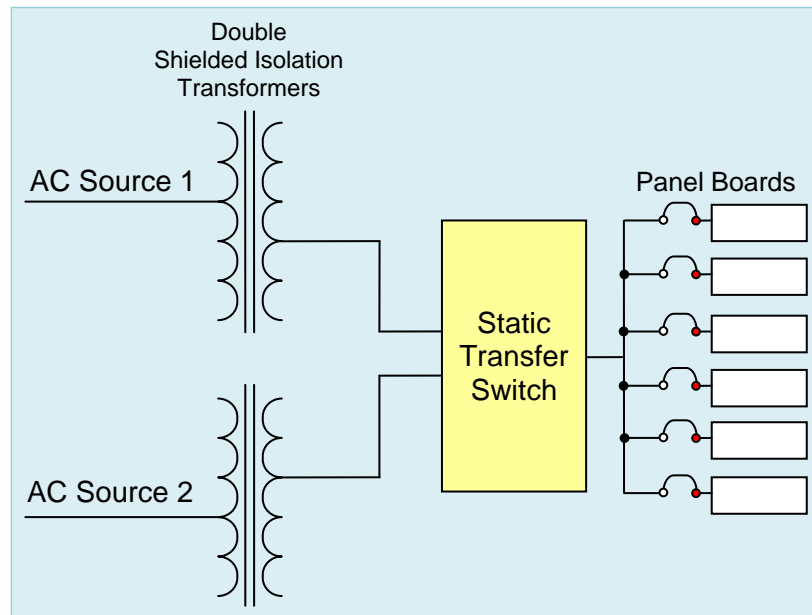


Figure 30: Automatic Static Transfer Switch - Dual Transformer, Secondary Side Switching

At this level, the electrical system is downstream from the PDU or transformer level, and this system is typically operating at the utilization voltage level for the ITE or critical equipment. This distribution can be present in several forms, such as busway or individual circuits.

For high-density loads, a given design may separate the panelboard sections of the PDU into cabinets near the critical loads. These systems may have either single- or dual-inputs and are commonly known as a remote power panel (RPP). RPPs reduce installation labor and reduce the cable and circuit length to the load.

Distribution to the loads may be either overhead or underfloor. Underfloor power distribution is most commonly accomplished using liquidtight flexible metallic conduit, although in some jurisdictions, hard conduit may be required. IEEE 1100 recommends hard steel conduit with an AHJ-approved insulated grounding wire for added safety, performance, and EMI protection. Power distribution should be located under the cold aisle and telecommunications cabling located under the hot aisle to minimize air blockages. Overhead power distribution can frequently eliminate the cost of conduits (with the addition of cable tray or busway) and can have the added benefit of eliminating cables as a cause of under-floor air blockage. Overhead cabling, if used, should be planned to minimize blockage of airflow above the floor. Refer to 14.4.8.2 for considerations of overhead cable routing.

For future and high-density loads, traditional 20A circuits may not be sufficient for power strips in the IT cabinets, and in some installations, 3-phase power strips with appropriately sized circuit capacity may be required to support the load. To accommodate future power requirements, [anticipate](#) installation of three-phase cabling at an ampacity of up to 50 or 60A, or at utilization voltages of around 400 VAC, even if such power is not immediately required.

9.3.14.2 Load connections

9.3.14.2.1 Recommendations

Load connection best practices for facilities in the United States are listed below.

- Twist-lock receptacles and plugs for all underfloor or overhead receptacles, without exception. Receptacles on the power strip within a rack or cabinet do not require locking-type receptacles. Some systems use a plug-in busway system installed adjacent to the loads or cabinets. The busway's design should allow new load taps to be installed while the bus is energized without creating any arcing or transients.
- Locking receptacles should be used for connecting the input cords of the power strips and for larger ITE. For in-rack loads using straight-blade cords, anti-pullout tie downs should be used where cords plug into the power strips.
- Power distribution cables originating from different source PDUs, RPPs, electrical phases, taps off the same PDU, or electrical panels should be clearly identified as to their source, phase, and load capacity. If permitted or required by the AHJ, cables from different sources may have different color jackets and/or connectors.
- Branch circuit overload protection devices should be de-rated by a design factor of 20% (e.g., be at least 25% larger than their connected IT load) to ensure that circuits are not operating at the edge of their circuit breaker trip rating.
- For equipment and systems that require power feeds from more than one power source to provide availability (typically Class F3 or Class F4), the power cords should be split across two of the cabinet power strips. To provide availability for single-corded equipment and for equipment that utilizes multiple cords but is not power feed-fault tolerant, these items should be plugged into a rack-mounted power strip or receptacle fed by a larger upstream, automatic static transfer switch (ASTS) or some other point-of-use ASTS.
- Equipment with three power cords should have one of the three plugs on a rack-mounted power strip or receptacle fed by a static transfer switch or point of use switch. The other two plugs should be plugged into receptacles supported by different PDUs. These other two receptacles should not be on static transfer switches.
- Power cords should be secured at the point of entrance into the rack or piece of ITE.
- Pair or group UPS sources together, represented by the individual panels or remote power panels, for ease and clarity.
- Plugs and rack-mounted power strips should be located where thermographic testing can observe all critical connections and overcurrent protection devices while operating.
- Cable management should be used.
- Minimize disruption to future operations by locating distribution equipment to permit expansion and servicing with minimal disruption.
- All power receptacles and junction boxes should be labeled with the PDU/RPP/panel number and circuit breaker number. All PDU/RPP/panel circuit breakers should be labeled with the name of the cabinet/rack or grid coordinates of the equipment that it supports.
- All power receptacles and junction boxes installed under an access floor system should be attached to the access floor or the structural floor per manufacturer's recommendations when required by the AHJ. Receptacles and junction boxes should be mounted on channel to keep raceways and equipment above the sub floor. This attachment may be made mechanically via concrete anchors, brackets attached to the access floor pedestals or even industrial hook-and-loop NRTL-listed fasteners, which make an excellent, dust-free alternative to drilling in an anchor or adhesives. Additionally boxes and other electrical devices may be mounted at least 25 mm (1 in) above the sub floor to prevent water intrusion in the event of a leak.
- Every computer room, entrance room, access provider room, and service provider room circuit should be labeled at the receptacle with the PDU or panelboard identifier and circuit breaker number.
- Receptacles on UPS power should be color-coded, have a color-coded label, or have a colored dot to indicate the specific upstream UPS power source.
- Unused or abandoned cables not terminated at equipment or marked for future use shall be removed.
- Supply circuits and interconnecting cables identified for future use should be marked with a tag of sufficient durability to withstand the environment involved.

See Sections 9.3.16, 9.7.2, and 9.10 for other requirements.

9.3.14.3 Data center load management and circuiting protocols

9.3.14.3.1 Introduction

Data center load management deals with the physical connection of critical loads to the critical power system in a manner consistent with the normal, failure and maintenance modes of operation. At this level, it is assumed that the IT load's internal power supplies will switch between the input sources independent of the critical power system's response to a failure. Knowing this, the data center or critical environment circuiting must agree with the response of the systems serving them. This is known as circuit mapping, and the same thinking that applies to all other parts of the critical power system applies here.

9.3.14.3.2 Data center load management

9.3.14.3.2.1 Requirements

Once equipment has been selected, continuous duty and design safety factors must be prudently applied to the critical power system. Safety factors are explained in more detail in Section 9.5.2.2.2. The maximum power required for a given critical power topology is then applied to the combined duty cycles and safety factors, resulting in the practical loading of the system. This practical loading accounts for all normal, failure and maintenance modes of operation of the critical power system.

This calculation varies depending on the Class and UPS topology. Most importantly, a facility operator needs to understand how this factor is applied at the PDU and critical power branch panelboard level in their facility, so that they can readily and most efficiently use the critical power they have available.

The formula for rating a critical power system is:

$$\text{System kVA} \times \text{continuous duty factor (if not rated for 100\% duty)} \times \text{design safety factor} \times \text{system power factor} = \text{usable kW of critical power} \quad (3)$$

For example, suppose the project involves consolidating a data center and there are six existing UPS power modules rated at 800 kVA for 100% duty (continuous operation) with a 90% power factor and a 90% safety factor. This would yield a UPS module with 648 kW of usable critical power capacity ($800 \text{ kVA} \times 1.0 \times 0.90 \times 0.90 = 648 \text{ kW}$). Placing six such modules into a Class F3 or Class F4 model could result in a variety of UPS System capacities as described in Table 9. Also, assume the use of a typical PDU rating of 225 kVA (more PDUs of smaller rating could theoretically be used). Table 9 shows how many PDUs could be used assuming a 90% safety factor.

Table 9: Example UPS/PDU Capacity Calculations

<i>Class/Critical power topology</i>	<i>UPS module quantity</i>	<i>UPS system capacity</i>	<i>PDU rating</i>	<i>PDU capacity *</i>	<i>Max PDU count per UPS system</i>
Class F3/N + 1	6	$648 \times 5 = 3,240 \text{ kW}$	225 kVA	202.5 kW	$648 / 202.5 = 3$
Class F4/N + 2	6	$648 \times 4 = 2,592 \text{ kW}$	225 kVA	202.5 kW	$648 / 202.5 = 3$
Class F4/2N	6	$648 \times 3 = 1,944 \text{ kW}$	225 kVA	202.5 kW	$648 / 202.5 = 3$

* The PDU capacity defines how much power can be deployed from it in the data center.

9.3.14.3.3 Data center circuiting protocols

9.3.14.3.3.1 Introduction

For this portion of the section, Class F3 and Class F4 system arrangements with more than two circuits per cabinet will be examined in order to demonstrate how the data center loads should be arranged.

One of the most effective methods for preventing system overloading is the management of IT loads in the critical environment. While it may be difficult to overload a PDU or UPS system, improper cord management may lead to a lack of adequate circuit diversity for the IT loads. As a result, the failure mode response of the IT loads may be compromised.

To graphically represent how Class characteristics are manifested in the data center's circuiting environment, each system offers different options. For Figures 31–34, following assumptions are valid:

- UPS “N” module size is 820 kVA/738 kW (0.9 power factor, 888 A);
- the UPS output distribution panel is rated at a standard 1200 A;
- each UPS system supports four PDUs, each rated 225 kVA;
- each equipment rack holds 4.5 kW of ITE;
- three separate 20A, 120 VAC, single phase circuits will run from each PDU to each equipment rack (one per phase).

NOTE: Best practice would be to run a single 3-phase circuit to a rack-mounted power strip with single-phase outlets, but for illustration purposes assume all single-phase circuits.

For Class F1 and Class F2 systems, the data center circuiting methods are identical because there is no redundancy in the critical power system's pathways until Class F3 is realized.

The model for the Class F1 and Class F2 critical power systems would be as shown in Figure 31.

With the diversity in the critical power paths in the Class F3 and Class F4 systems, the complexity of the circuiting systems in the data center becomes more complicated. The key point to the higher Classes is that the circuits that serve the IT must be derived from separate sources. In the following models, these examples will be demonstrated.

Figure 32 shows a model for circuiting a Class F3 critical power systems.

For the Class F4 model, the model changes a little bit depending on if it is an xN distributed network or a 2N environment.

Figure 33 shows a model for circuiting an xN Class F4 critical power systems. In this case, it is the N + 2 environment.

Figure 34 shows a model for circuiting a 2N Class F4 critical power system.

Data center circuit mapping normally will not follow the Class pathway requirements. The circuiting map is focused on maintaining the platform via its own internal power supplies switching mechanisms. In today's IT environment, the following IT load power requirements are common:

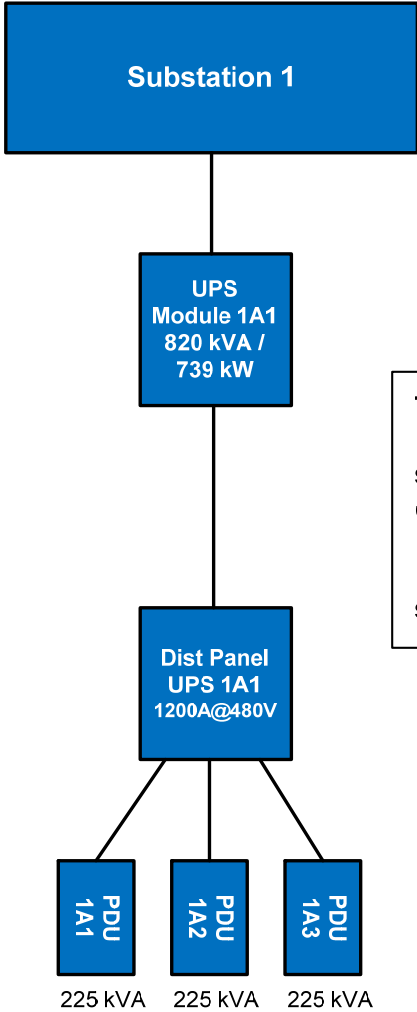
- single cord, single power supply required;
- dual cord, single power supply required;
- three cord, two power supplies required;
- four cord, three power supplies required;
- six cord, four power supplies required.

A facility may experience a situation where the critical power system paths are mismatched to the UPS power plant counts. This is a common condition in all sizes of facilities. In this case, the N capacity of the UPS systems serving the loads must be matched to the failure and maintenance modes of operation for the independent critical power distribution systems. The key is how the IT loads connect to the critical power system. This means that each IT load cord would be connected to a separate PDU. In turn, these PDUs would be mapped up to the critical power distribution system and UPS plants.

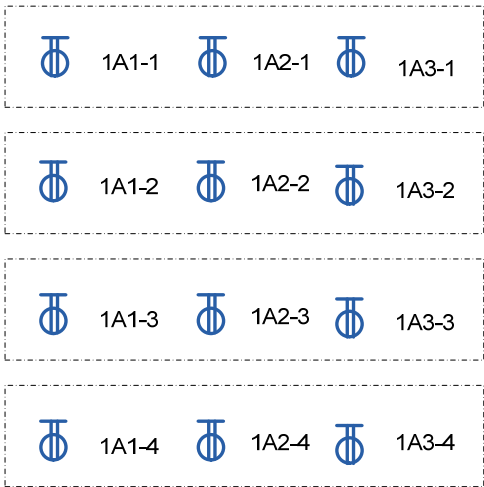
When examining the IT loads, there is typically platform diversity for smaller server-based systems. However, for larger, enterprise-type servers, mainframes or large disc arrays, there may not be physical diversity of equipment. The electrical designer must consider the virtual, application and platform diversity within the critical environment, but in the end, should not rely on the IT systems' diversities to make the Class work. The designer must address the circuit diversity as fully as possible in concert with the IT loads requirements.

For example, if the cabinet load is a 4-circuit rack containing numerous single-corded servers, each cabinet would then require that any three of four circuits be available at any time. By extension, this would mean that any three of the four PDUs must be available for the load at any time.


If four circuits are required for a cabinet or load, with three circuits as a minimum to render an N electrical service, the minimum number or N number of PDUs for the load would be three during a failure or maintenance activity. With four distinct circuits for normal operations, four PDUs are required.



The Class F1 and Class F2 models do not offer critical power distribution system diversity. The loads are connected to the UPS systems to the kW rating of the upstream system, but UPS power is on only one supply source.



LEGEND

 1A3-1

Color = Macro UPS Serving the Load

"1" = Discrete UPS Serving the Load

"A" = Module Serving the Load

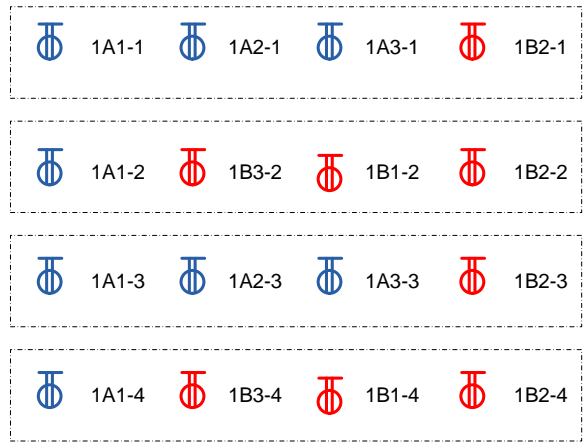
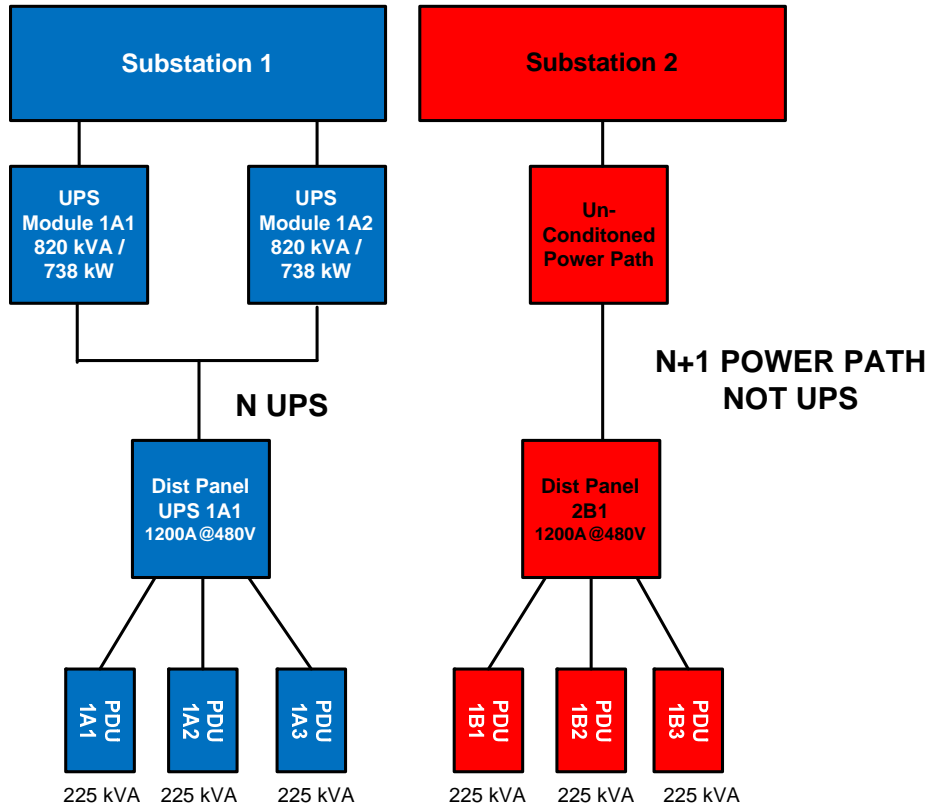
"3" = PDU Serving the Load

"-4" = PDU Circuit Serving the Load


Typical 3 circuit cabinets

Figure 31: N Circuit Map With 3 Circuits Per Cabinet (Class F1 And Class F2)

The Class F3 system offers redundant power paths. In these cases, with 1 redundant UPS system and 3 circuits per cabinet, the net count to complete a balanced system would be 6. Like Class F2 systems, the UPS components are redundant. Like Class F4, the rating of the Substations are equivalent.



LEGEND

 1A3-1

Color = Macro UPS Serving the Load

"1" = Discrete UPS Serving the Load

"A" = Module Serving the Load

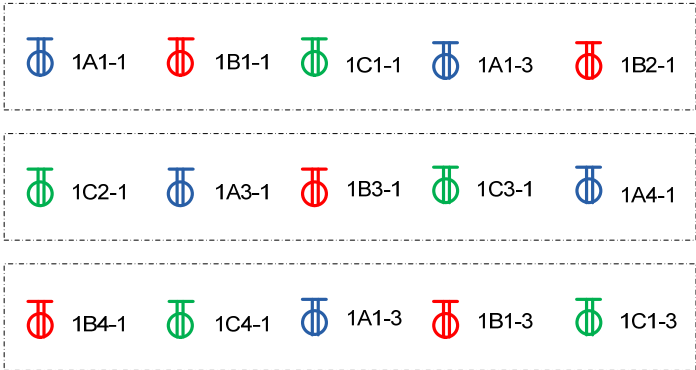
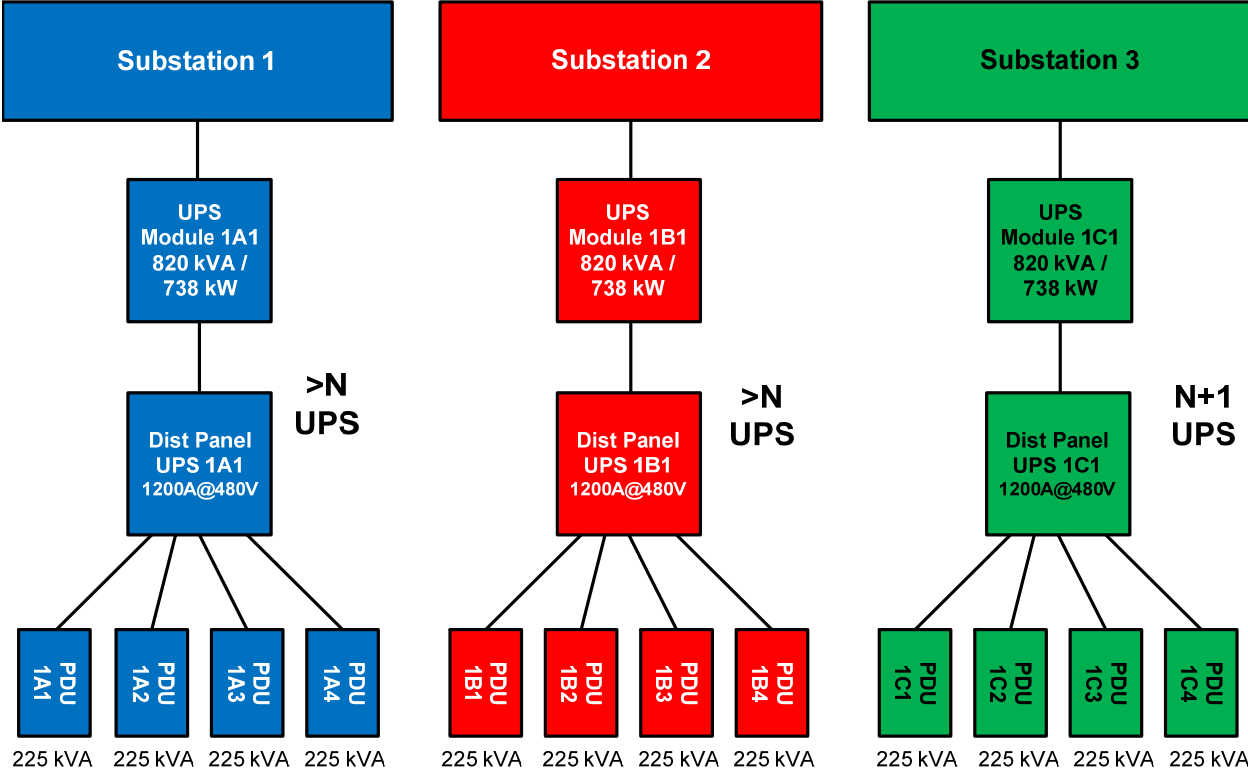
"3" = PDU Serving the Load

"-4" = PDU Circuit Serving the Load

Typical 4 circuit cabinets required - 4 circuits provided

Figure 32: N + 1 Circuit Map With 3 N circuits Per Cabinet/4 Required (Class F3)

The Class F4 Distributed Redundant system requires that the circuiting be balanced between the UPS systems. In this case, with 3 circuits per cabinet and five circuit being required (n+2 minimum), the net count to complete a balanced system would be 15.

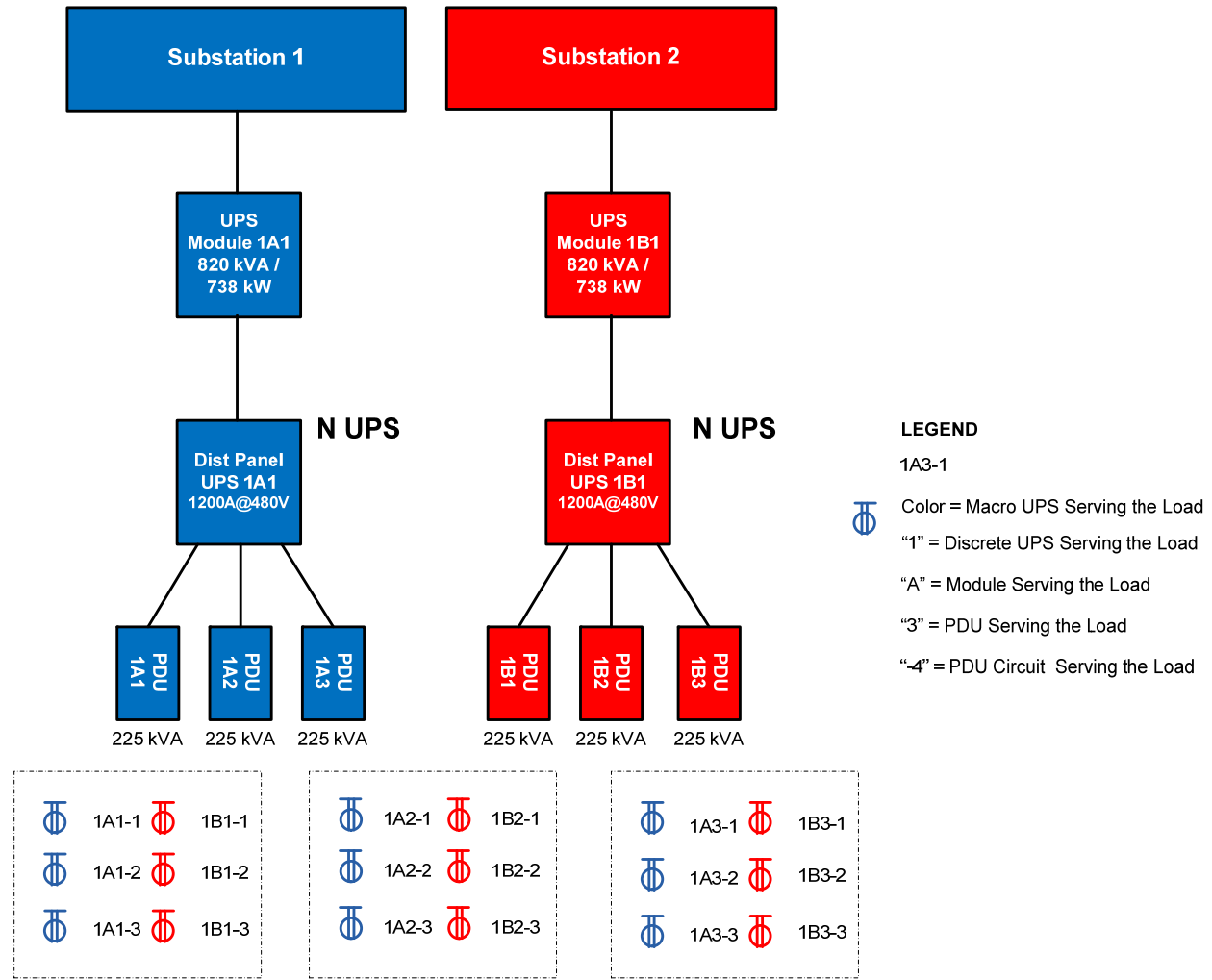


LEGEND
 1A3-1
 Color = Macro UPS Serving the Load
 "1" = Discrete UPS Serving the Load
 "A" = Module Serving the Load
 "3" = PDU Serving the Load
 "4" = PDU Circuit Serving the Load

Typical 3 circuit cabinets - 5 circuits per cabinet required (n+2)

Figure 33: xN Circuit Map With 3 N Circuits Per Cabinet/5 Required (Class F4)

The Class F4 models offer complete system and active UPS power pathway redundancy. In this case, with 2 UPS systems and 3 circuits per cabinet, the net count to complete a balanced system would be 6.



Typical 3 circuits required per cabinet - 6 circuits provided per cabinet

Figure 34: 2N circuit Map With 3 N Circuits Per Cabinet/6 Required (Class F4)

There will be occasions where the failure or maintenance modes of operation for the circuiting do not meet the availability requirements for the project with single path circuiting from dedicated PDUs. In this case, some form of automatic load switching via automatic static transfer switches or maintenance bypasses to the circuit level (executed typically at the RPP or panel level) are needed.

The 2N topology may be confusing when comparing the UPS systems with the generator and utility plants. The thought here is that the capacity of the utility and generator systems must carry the load in a manner consistent with the given Class.

9.3.14.3.3.2 Requirements

Each of the power input conductors to a single multi-corded ITE device shall be of equal capacity. The size shall be of adequate capacity to serve the loads under normal, maintenance and failure modes of operation. IT loads from individual circuits shall be segregated up to the PDU input level.

Once the maximum loading is determined for a given PDU or critical power distribution panelboard in the data center, the proper critical power circuit distribution in the facility may then be determined.

If a heterogeneous ITE census is presented, the data center operator would simply have to circuit the critical power system as the loads are brought in and organized.

In a homogeneous IT environment with a large set of equipment requiring identical electrical services, a basic circuit map can be developed and deployed for the facility. To begin, determine the circuit count and rating required for each cabinet or load.

Like all critical power system applications, circuiting must be deployed to align with the worst-case scenario for the Class. If the Class calls for a N + 1, N + 2, or a 2N power system topology, the circuits for the data center would be deployed the same way.

The example shown in Table 10 demonstrates how to evaluate this type of deployment in several Class situations.

Assumptions are that:

- cabinet load is 4.5 kW (based on user's planned deployment);
- voltage and phasing required is three separate 20A, 120 VAC, single phase circuits from each PDU;
- maximum rating of a 120 V, 1P 20A circuit is 1500 W or 1.5 kW
[maximum ampacity on a 120V/20A circuit is $120V \times 20A = 2400 W \times 0.80$ safety factor $\times 0.80$ design factor = 1536 W, rounded to 1.5 kW];
- all equipment is dual-corded (even though in practice one would probably not use dual corded equipment in a Class F1 environment because it adds cost but little or no increase in availability).

PDU capacity would simply be the arithmetic calculation of the PDU kW capacity divided by the circuit kW of the load, less the spare capacity an owner or designer may wish to leave in the PDU. For example, if the PDU is rated for 202.5 kW, with a 20% spare capacity and an average circuit load of 1.5 kW, the circuit capacity of the PDU would be:

- PDU kW rating is 202.5 kW.
- Spare capacity is 20% or 40.5 kW.
- Actual PDU capacity for the load is 162 kW.
- 162 kW/average IT circuit load or 162 kW/1.5 kW or 108 circuits.

The only caveat here is that if the load is shared across several systems and the systems are not rated for the same output kW, either a lower overall kW for the critical power system is realized, or more likely, the smaller system is skipped once it reaches its kW design limit and the circuiting protocol is changed. Either approach is acceptable.

Table 10: Example Of UPS/PDU Capacity Calculations

<i>Class/Critical power topology</i>	<i>Cabinet kW</i>	<i>Power requirement</i>	<i>N circuits/cabinet</i>	<i>Circuits required for Class</i>	<i>Additional circuits</i>
Class F1/N+1	4.5	120 V/1P = 1.5 kW	4.5/1.5 = 3	3	Not required
Class F2/N+1	4.5	120 V/1P = 1.5 kW	4.5/1.5 = 3	3	Not required
Class F3/N+1	4.5	120 V/1P = 1.5 kW	4.5/1.5 = 3	4	Add for failure or maintenance mode as required
Class F4/N+2	4.5	120 V/1P = 1.5 kW	4.5/1.5 = 3	5	Add for failure or maintenance mode as required
Class F4/2N	4.5	120 V/1P = 1.5 kW	4.5/1.5 = 3	6	Add for failure or maintenance mode as required

9.3.15 Surge suppression/surge protection devices (SPDs) for ac circuits

NOTE: Surge protection and mitigation is discussed in depth in Section 9.9.4.

9.3.15.1 Introduction

Surge suppression, in the vernacular of this section encompasses all surge protection devices or SPDs. The first is that SPDs and large-scale surge suppression is an integral part of the lightning protection for facility. The second is the voltage transient mitigation typical for a facility of this type.

Surge suppression for low voltage ac power circuits is historically known as transient voltage surge suppression (TVSS) as this terminology was used by the NEC and the NRTL. The term TVSS is no longer used by the NEC or the NRTL as it is replaced by the term surge protection device (SPD).

For increasing Classes, SPDs become more prevalent throughout the power system. For lower Classes, SPD is located on the utility entrance, with transients not being addressed, unless the site demands it. As the Classes increase, SPDs may be found in the following locations:

- utility service entrances;
- generator buses;
- UPS inputs;
- UPS outputs;
- UPS power distribution switchboards;
- PDUs and critical power distribution panels.

9.3.15.2 Recommendations

To protect against the event of an internal or explosive MOV failures, SPDs should not be mounted inside or upon switchgear, unless specifically designed, manufactured, NRTL listed and properly installed for integral installation, or compartmentalized. SPDs are also sensitive to the conductor length, so the conductors to the SPDs should be kept as short as possible pursuant to the manufacturer's recommendations and should avoid unnecessary bends.

SPDs should meet the following minimum criteria:

- listed to UL 1449 Edition 3 or later or equivalent AHJ requirement;
- provide surge current diversion paths for all modes of protection:
 - L-N, L-G, and N-G in WYE systems;
 - L-L and L-G in DELTA systems.
- modular in design with redundant protection circuitry;
- visible indication of proper SPD connection and operation;
- audible alarm for diagnostic monitoring, activated upon a fault condition;
- EMI/RFI filtering using MIL-STD-220A methodology or equivalent AHJ requirement.

For application guidance on the use of facility level SPDs for ac power systems, see IEEE C62.72, IEEE 1100 and NFPA 70, Article 285.

9.3.16 Emergency power off (EPO) systems

9.3.16.1 Introduction

A means of disconnecting the electrical supply, more commonly known as emergency power off (EPO), while not mandated by standards, is sometimes required by local codes. An EPO presents the greatest risk to electrical system availability in the data center, as an EPO activation can be intentional, caused by sabotage, or accidental, via physical contact, mechanical failure, and human error during maintenance (such as the manipulation of the EPO system's link to the fire suppression system).

9.3.16.2 Requirements

Local codes or insurance carriers often require EPO for the safety of firefighters, but they may allow some exceptions (such as when "orderly shutdown" is necessary). When not required by code, the owner must carefully balance the needs of business continuity with personnel and building safety. When an EPO system is to be installed, a number of features can be included to make it more reliable:

- EPO systems should be three-stage systems, with Off, Test, and Armed modes of operations.
- EPO activation stations should require multiple steps to operate them such as lift-hold-and-pull or the simultaneous operation of two buttons (when not prohibited by ADA and/or similar accessibility regulations).

- EPO activation stations should offer a pre-alarm function, in which an audible and visual alarm is activated when the EPO button cover is lifted. This allows someone who has accidentally lifted a cover to know that there is a danger of activating the EPO system.
- EPO activations may be on a time delay, zoned to deactivate smaller areas of the data center or centralized as part of an integrated electrical system. All of these techniques should be reviewed and approved by the local jurisdiction prior to implementation.
- EPO systems should not be installed in UPS, chiller and battery rooms, unless required by code or the local jurisdiction.
- Security cameras should be installed at EPO stations so that the face of the operator of the EPO can be clearly seen.
- EPO stations should not be located near light switches, phones or any other device that is routinely touched.
- EPO systems should be isolatable from the fire alarm system, so that when the fire alarm system is undergoing routine maintenance, the EPO is not accidentally activated.
- Do not specify or disconnect onboard, device-specific EPO buttons, if present, from UPS modules, UPS control cabinets, PDUs, static switches and any other factory-installed EPO button. If the EPO's can't be safely removed, the covers should be tied down to prevent accidental activation. These EPO's are not required if the room they reside in has one, since they disconnect only one system or device as opposed to all of the room's equipment
- Multiple disconnecting means may be used to de-energize IT equipment and cooling equipment.
- Activation of an EPO circuit should also remove power to all power to dedicated HVAC systems serving the room, and should cause all required fire or smoke dampers to close.
- The disconnecting means may be permitted to be located in a secure area outside of the computer room, but this should be reviewed and approved by the local jurisdiction prior to implementation. Consideration should also be given to security risks if the EPO is not in a controlled access space.

Organization of an EPO system is illustrated in Figure 35.

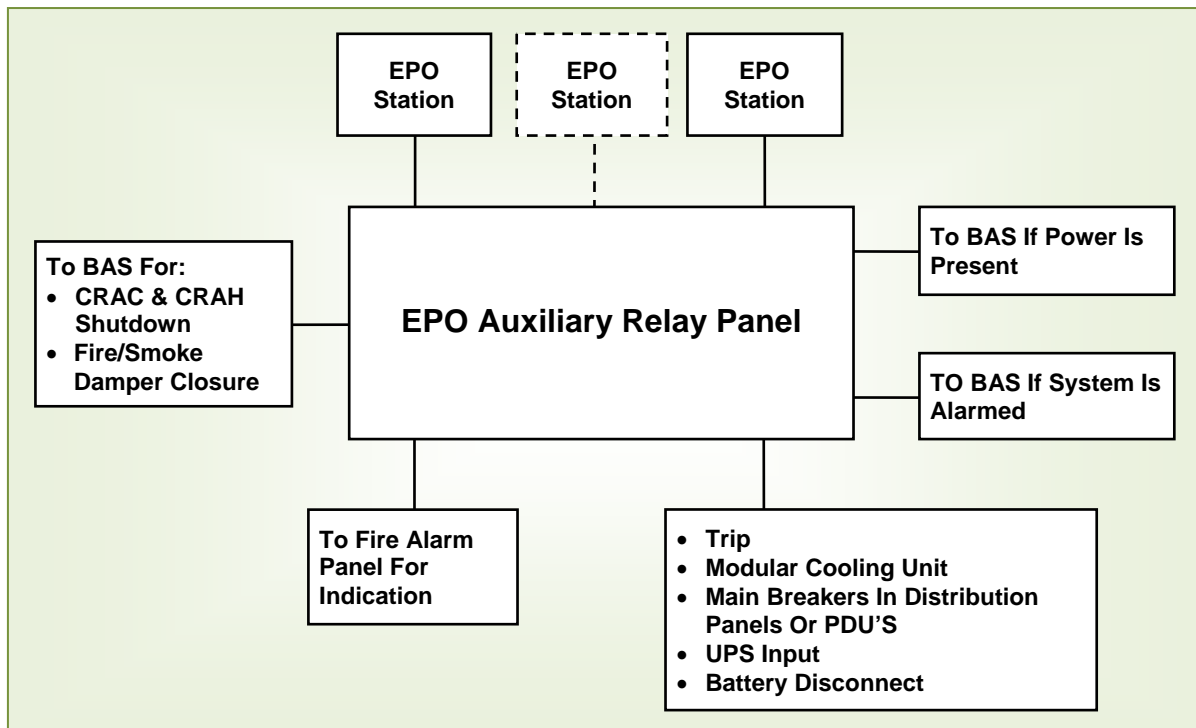


Figure 35: EPO System

9.4 Mechanical equipment support

9.4.1 Introduction

Mechanical systems are as vital in the data center as the UPS systems that serve the ITE. The ability to have little or no interruption to the cooling services while maintaining temperature and humidity within relatively narrow band is vital for the operation of most high-performance computing systems.

There have been several instances of thermal runaway where the heating of the data center could not be stunted in time to prevent the ITE from shutting down on a high temperature condition.

Some computing systems consume so much power and operate at such a high-power density (as viewed in W/m^2 , W/ft^2 , $kW/cabinet$ or $kW/floor\ tile$) that an interruption of cooling medium for only one minute can result ITE shutting down. In this light, ITE requires uninterruptible power and nearly uninterruptible cooling.

There are two considerations for the electrical system when it supports the mechanical system - the restart of the cooling system (viewed in its entirety from the cooling plant to the ventilation systems) and the diversity of the electrical paths to the mechanical systems that matches the redundancy of the given mechanical components being served.

In traditional chiller plants (not including slaved DX units to a given air handler), the compressor restart time for the chiller can lead to thermal runaway in the data center during a power failure. This is caused by the IT loads still operating under UPS power, while the chillers, powered by the generator system, undergo a complete and protracted restart cycle following a power interruption.

While the restart control sequence is the purview of the mechanical designer, careful consideration needs to be paid to the following as soon as possible after an outage or retransfer from generator to normal power:

- keeping chilled water moving in the system;
- keeping the ventilation systems operating;
- reestablishing the cooling plant (regardless of its design).

Generally speaking, a Class F4 mechanical system does not have the same topology as a Class F4 electrical system. Since the Class F4 mechanical system must meet the performance definitions defined for Class F4, the electrical system that supports the mechanical system must map to the normal, failure and maintenance modes of operation for the mechanical system.

In many ways, the circuiting of the mechanical system is similar to circuiting of multicorded equipment loads in the computer rooms; multiple power paths must be used to ensure a given piece of equipment survives a failure or is still on line during maintenance. Since Class F1 and Class F2 systems do not offer load supply redundancy, these Classes are not offered as solutions. The circuiting pathway for support of mechanical loads for a Class F3 facility is illustrated in the Figure 36:

An example of a power distribution system supporting a Class F4 mechanical system is illustrated in Figure 37.

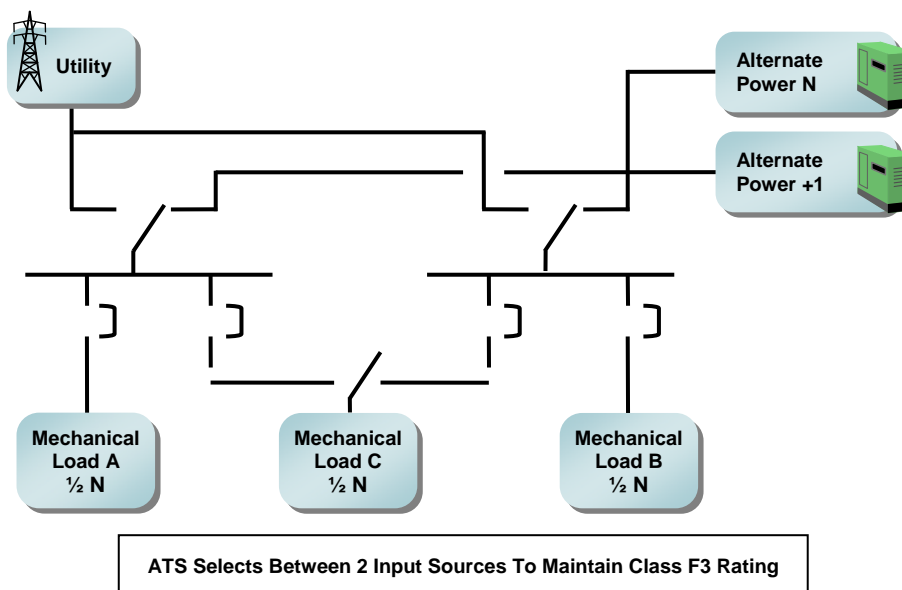


Figure 36: Sample Power Circuits For A Class F3 Mechanical System

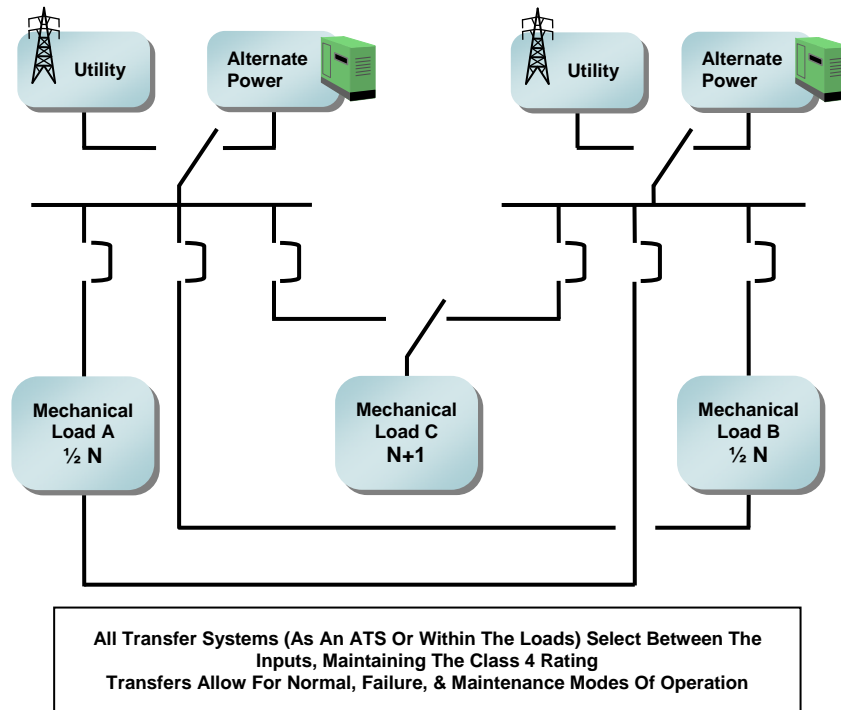


Figure 37: Sample Power Circuits For A Class F4 Mechanical System

9.4.2 Requirements

Temperature controls shall to be maintained during normal, maintenance and failure modes of operations. Since the mechanical system controls are vital to the operation of the cooling system, they shall be placed on UPS power. Where redundant temperature and cooling plant controls are provided, redundant circuits shall be provided commensurate with the diversity of the control system.

Cooling water pumps may require uninterrupted power. If the decision is made to support motors and pumps without interruption, they shall have a dedicated UPS suitable for the high inrush currents characteristic of such loads. Motors and pumps shall not share the same bus as IT loads. (See Figure 17 and Figure 18).

9.4.3 Recommendations

9.4.3.1 General considerations

Chiller and cooling systems often require substantial restart time, and these systems will take some time to return to full operation. This demands a few considerations:

- While the cooling systems are restarting, the UPS systems are still providing power to the load. Heat generated by the IT loads operating on that UPS power will build in the data center spaces. Cooling plant restart times are often much longer than the time it may take for heat to rise sufficiently in the room to a point where ITE will shut down.
- The diversity of the electrical systems serving the mechanical plant must address maintenance and failure modes of operation to ensure that the cooling system restart time does not cause IT loads to fail due to overheating.
- Substantial cooling water may exist in the cooling water piping system to help bridge the time or capacity gap for the cooling plant restart. In this light, keep cooling and condenser water pump running at all times.
- Some heat transfer may take place by simple ventilation, so keeping the fan system running will mitigate the heat rise in the room.
- For cooling plant restart, the following sequence of load additions to active service are recommended (all loads on alternate power):
 - ventilation,
 - pumps,
 - chillers and cooling plant.

- For higher power densities there may be only a couple of minutes or dozens of seconds before the room heat “runs away” to a point where, even if cooling is restored, ITE may drop out or be damaged due to temperature. In this case, some of the mechanical support loads must be maintained on a 24/7 basis and may require UPS power in support of the IT mission. For high-density loads, some pumps and fans will require power from a dedicated UPS.
- Prudent design calls for the ability, first, to determine the rate of heat gain in the data center, versus the restart time in failure or maintenance modes of operation, and second, to ensure that the electrical system offers sufficient capacity and diversity to prevent thermal run away in the facility.
- For fast chiller restart the chiller controls (but not the pumps) should be on UPS.

9.4.3.2 Chillers and central cooling plant

Chiller and cooling plants have particular challenges to overcome for high-availability applications. Chillers, towers, and pumps tend to be single input type of machines, with only a single feeder serving them. For open-circuit cooling systems utilizing cooling towers, chillers are sometimes paired with a cooling tower and pumps, while in other cases they work independently from each other. Whichever the case, the chiller input power must be coordinated with the mechanical plant’s chiller redundancy scheme. For some high-availability sites, heat exchangers and thermal storage systems are employed and must be considered in the circuiting of the cooling plant.

In all events, the pumping and other supporting systems, such as controls, must also be energized and maintained during normal, maintenance and failure modes of operation. Dual input to the chillers, cooling towers, and associated cooling equipment via automatic or manual transfer systems may be required.

For high-density computing environments, it is essential that some form of cooling be maintained during the generator start and mechanical cooling plant restart cycles. Some form of cooling equipment may have to be placed on UPS power in order to maintain temperature and humidity control in the data center.

9.4.3.3 Pumps

Pumping systems for data centers come in numerous forms: chilled water primary and secondary, condenser water, make up water, well water, and booster pumps. Most of these systems are configured as parallel redundant systems, operating on an $N + 1$ or $N + 2$ basis. Occasionally, a $2N$ system might be seen as well. Pumping systems typically operate much like paralleled generators or UPS modules might, sometimes equally sharing the load and sometimes not, depending on the drive and control configuration. Therefore, each pump for a given system needs to be powered independently of its partners. The circuit mapping also needs to follow the Class requirements and maintenance and failure modes for the equipment.

For high-density computing environments, it is essential that water flow be maintained, possibly requiring that some water flow systems be placed on dedicated UPS power.

9.4.3.4 Air handling systems

Air handling systems typically possess a higher degree of diversity than any other mechanical load in the data center. For example, 10 air handlers might be required for the load, and 13 are installed. This can be due to air distribution, the designer’s preference, or the room’s physical organization or dimensions. Serving that from two or three mechanical load buses poses a challenge without the use of manual or automatic transfer systems for individual or groups of air handlers. Similar to chillers and pumps, the air handler diversity and N or $N + 1$ count must be known. Then the electrical system circuiting should be overlaid to support them.

For high-density computing environments, it is essential that air circulation be maintained, possibly requiring that some air handling systems be placed on UPS power.

9.4.3.5 Humidification

Humidification can occur either locally or centrally in a data center, depending on the mechanical designer’s technique. If the humidity control is local to the air handler, the power for the humidity system may be integral to the air handler. If so, the air handler’s circuiting will accommodate it pursuant to the Class’ requirements. If the humidification is not powered by the air handler, a separate circuit for the humidifier is needed and the same set of circuiting requirements for the given Class. The same can be said for humidification or dehumidification systems that are independent of the air handlers that are mounted either in the data center itself or in the air supply ductwork.

9.5 Uninterruptible power supply (UPS) systems

9.5.1 Introduction

UPS systems were discussed in 9.3.9 as part of the distribution system. Using an analogy in which the electrical distribution system can be considered the arteries of the critical power system, the UPS systems are the heart – the nexus of power conversion and continuity. While there are several methods and designs for achieving a topographical standard that will meet a given Class goal, the sizing and considerations of the UPS power plant itself has several common issues. This section will address the varying technologies, design applications and other considerations for the UPS plant. These include:

- sizing and application;
- technology;
- paralleling and controls;
- batteries and stored energy systems.

Appropriate selection of the UPS topology depends on the criticality of the applications supported by the data center. It is acknowledged that every business demands different levels of criticality, and that the topology chosen has substantial impact on cost, space, complexity of operation, cost of operation, and expected lifespan.

NOTE: The remainder of Section 9.5 may be treated as recommendations

9.5.2 Sizing and application

9.5.2.1 Application

UPS and critical power system applications are focused on delivering quality power, whether originating from an electric utility or from internal energy storage, on an assured, 24/7 basis. While there are several issues related to loading and topology, the primary concern of UPS system design for Class F3 and F4 systems is the maintenance of critical power services while accommodating known failures or allowing for safe and logical preventive maintenance. There are several points to consider when selecting equipment or employing UPS systems and critical power components into a cohesive critical power system.

Similarly, system bypasses, whether they be static or external/maintenance, must offer a safe and clear method for rolling load on and off the UPS module or system. System designs should be arranged so that a failure in a single module or system is not allowed to propagate to adjacent or paralleled systems. Failure compartmentalization should also be used for other portions of the critical power system.

The main design and application considerations for UPS and critical power systems are:

- automatic, single-step response to a failure;
- failures limited to system that broke;
- UPS power plant maps correctly to the critical power distribution system;
- stored energy system able to carry the critical load during all input power failures.

9.5.2.1.1 Automatic, single-step response to a failure

System failures should be automatically corrected without risking the load. Failure response should allow the UPS system to settle into a steady state, as expeditiously as possible. The response to a fault may transfer the load from the UPS module or system to another UPS system or to an unconditioned bypass source. Regardless, the UPS system has its highest chance of maintaining the critical power load's continuity with a single transfer or operation, also known as the "one step save". If the UPS system requires several steps to arrive at a revised steady state, it may fail in the transition process, resulting in a critical power load loss.

9.5.2.1.2 Failures limited to a system that broke

Failures should be limited to the system or portion of the critical power chain that experienced the failure. For example, a failure of a single module in a multiple module, paralleled system should limit the failure to the module that failed. In the case of a distributed system, the interconnection of the systems should not allow a failure to cause a failure in the supporting systems. This only speaks for system changes of state, and not the normal, customary, and predicated load transfer to the other UPS systems that are expected based on the Class or system constitution.

There is a word of caution for some of the UPS plant designs that seek to establish a "ring" bus to share redundancy for multiple UPS power plant outputs or in the distribution system. Power quality, especially switching transients, resonance or "ringing", need to be carefully examined to assure that the UPS waveform is not corrupted by the failure mode operation of any portion of the system

9.5.2.1.3 UPS power plant maps correctly to the critical power distribution system

There are several instances when the N count of the UPS systems may not agree with the N count of distinct critical power distribution channels downstream of the UPS plants. IT loads are typically dual-corded, with many systems being more-than-two-corded. This brings up the phenomenon where the UPS plants' pathways do not directly map to the number of pathways of the downstream power distribution system. An easy plant-to-distribution map is a 2N system, with a PDU capacity matching the UPS system (not considering the idiosyncrasies of the individual PDU setups).

For distributed systems, the failure modes of the individual critical power circuits need to be mapped upstream to the PDUs, then the PDUs need to be mapped against the critical power distribution systems or switchboards, and then the critical power distribution switchboards need to be compared against the UPS plants to which they are connected. While this is a straight forward exercise for normal operations, the failure and maintenance modes of operations need to be examined for loading and change of state operations as well to assure that the critical power is maintained at all times, under all modes of operations.

9.5.2.1.4 Stored energy system able to carry the critical load during all input power failures

Since an alternate source of power is an integral part of the data center's design, a utility power failure should result in the generator starting and the facility being transferred to the generator or that alternate source of power. The ability to carry vital IT loads and critical support loads during the power resumption on the Generator or maintaining services during the retransfer from Generator to utility is necessary for any data center design.

With the advent of the high-density computing environment, the maintenance of cooling systems and the room environment is as vital to maintaining the IT processes as the UPS systems' stored energy systems.

The stored energy systems for the UPS modules and systems will be discussed in detail in Section 9.5.5. Every UPS power system must have some form of stored energy to bridge the transfer to the alternate source of power and the retransfer to utility and normal operating conditions, or for any situation where the input power falls outside of the system's tolerances. For single corded loads, subcycle static transfer switches may be employed where the IT loads themselves do not offer redundancy. In many cases, the IT loads themselves will arbitrate which power input is most appropriate for its use.

For certain computing environments, UPS power may be derived from batteries, flywheels, or another stored energy system that provides the ability for a power or cooling system to maintain or restart loads before an impact to the computing environment. In some cases, this might mean that the chilled water pumping systems or chiller water storage system must be on UPS power. In other cases, the ventilation system must be maintained on the UPS power system.

In any event, these collateral, nontechnology loads must be added to the IT loads to arrive at the proper UPS plant size for the facility.

9.5.2.2 System sizing

System sizing is linked to the Class, system design, and topology chosen by the designer. The UPS system design should be based on kilowatts (kW) with consideration given to kilovolt-amperes (kVA) and the resulting power factor.

The critical power system sizing is based on fully meeting the critical power load with the fewest modules or pathways available during maintenance or failure modes of operation (fairly assuming that the normal mode of operation always has more systems or pathways than failure or maintenance modes of operation).

The UPS power system capacity is always determined at the output of the UPS system. PDU or transformer losses related to generating ITE utilization voltage are to be considered part of the IT load and are not to be included in the power capacity calculations. This method considers all UPS module and system losses but does not penalize critical power distribution systems that may not employ PDUs or transformers or any further voltage conversion below the UPS systems. When determining power density (rendered in W/area), the output kW rating of the UPS power system is to be utilized for the calculation.

9.5.2.2.1 Loading levels

As for many power systems, there's fine balance between an overloaded and an under loaded electrical system. While the issues of overloading are clear (heating, breaker tripping, and reduction of Class), under loading may lead to system instability or, for some older system, an inability to operate.

While this is not a big issue for a single module system, this can be a huge issue for large-scale paralleled or distributed-redundant systems where load is being shared equally among several, equal components. Loading levels must be considered for normal, maintenance and failure modes of operation. The fact is that for higher Class rated

systems, there are often many systems sharing a modest critical power load sometime during the lifespan of the facility.

Overloading factors are noted below in the next section, and it is recommended that a given UPS system be operated at no less than 20% and no more than the Safety Factor discussed below under normal, maintenance and failure modes of operation.

Critical power system loading is load growth versus the Class. For example, a Class F4 system, when it passes a certain loading level, may revert to a Class F3 level. This occurs, because power modules that were formerly used for redundancy may now be required for capacity (i.e., to serve a larger critical power load).

9.5.2.2.2 Safety factors

It is impractical to load any electrical system to its full capacity. While some manufacturers have purported or proven 100% system rating, and a resulting 0% safety factor when weighed against the critical power load kW rating, best practice is to always apply a safety factor in system design. This addresses unanticipated load fluctuations, inrush currents, and code-required continuous-duty system ratings. See the previous discussion in 9.3.14.3.2.1 on how to apply the safety factor in a sizing calculation.

A suggested load factor of 90% is recommended, with a 95% maximum, leaving a design of 10% to 5% safety factor. This does not include the continuous-duty rating demanded by the Code. For most designs, the Code-mandated safety factor required for continuous load could also be used as the design safety factor.

9.5.2.2.3 Maximum critical power load

The UPS plant and systems must be designed to accommodate the maximum critical load that the facility is expected to require during its useful life. These loads include IT loads, critical cooling systems and other supporting systems. This maximum critical power load must be supported by the utility and alternate/generator power plants as well.

9.5.2.2.4 Scalability

Modular system architecture may allow a UPS system to defer system components for both design efficiency and cost effectiveness. The initial, interim, and final system configuration must anticipate the maximum capacity. The design must offer a system count that logically addresses system loads at any time during the system lifespan while offering an individual module size that is neither too large nor too small to achieve the Class specified for the system.

The key point in system sizing and application is that the system design and configuration must address both the normal mode as well as failure and maintenance modes of operation. The resulting system capacity must be sufficient to support the load that is present at any point in the systems life during all modes of operation.

9.5.3 Technologies

9.5.3.1 Technology considerations

For UPS systems, several criteria must be met regardless of manufacturer, system organization or type of UPS system technology being employed. UPS systems may consist of individual UPS modules, individual UPS systems, or a group of several paralleled modules. However, the recommendations for the performance of these systems regarding maintenance, failure and normal mode responses are going to be similar:

- The UPS technology should compartmentalize failures so as not to allow failures to spread to other modules or systems.
- Each module should be provided with a means of individual isolation without affecting the integrity of operation, overall redundancy, or Class.
- Each system should be capable of both automatic and manually-initiated by-pass, and should be provided with external means to bypass the system to avoid interruption of power in the event of system failure or maintenance.
- Modules and systems should possess an ability to be isolated from the critical load as well as from its input. This allows the module or system to be fully isolated from power and control input for safety, maintenance, or to replace the UPS module or system.
- The UPS system always possesses some form of stored energy system using batteries, mechanical stored energy systems such as flywheels or clutched-based systems for momentary ride-through of the critical load.

9.5.3.2 UPS system types

UPS systems use numerous technologies and configurations to support critical loads.

While the technology is important, designers fashion all forms of critical power systems from all types of UPS technologies, thereby meeting the needs of their clients and the attendant critical load. For this section, technology is not as important, as how that technology is employed to address the normal, maintenance and failure modes of operation.

However, this standard is predicated on the use of on-line systems such as traditional static or rotary UPS systems or integrated continuous power technologies like the coupled engine/motor/ flywheel systems. Offline” systems are “voltage and frequency dependent” (VFD) upon the input power source. They typically provide less than optimum power conditioning and switch to inverter operation only when suitable input power has been lost. By comparison, “online” systems are “voltage and frequency independent (VFI). They provide fully conditioned power all the time. Some UPS systems can automatically switch between online and offline mode (possibly termed “economizer mode”) in order to maximize efficiency but at the risk of exposing the critical load to less than optimum power quality. Offline systems are not suitable for data centers rated greater than Class F1.

For the purposes of this standard, three technologies will be presented: static, rotary and hybrid.

9.5.3.2.1 Static UPS systems

Transistors or other types of power electronics convert ac power to dc power. The dc power is stored in a power storage device (such as a battery string or flywheel), and then a second power electronics string converts the dc power back to ac. This technology is known as double-conversion technology; this technology is voltage and frequency independent. This conversion isolates the input and output for the most part.

Some static technologies use the same fundamental ac output, but use delta-conversion technology for the dc-ac conversion; this technology is not frequency independent. DC power may be stored using traditional chemical batteries or inertial stored energy systems such as high- or low-speed flywheels, compressed air, or other technology.

9.5.3.2.2 Rotary UPS systems

In some machines, the conversion and isolation are accommodated via a synchronous machine. Like static systems, dc power may be stored in flywheels, batteries, or other technology.

9.5.3.2.3 Hybrid UPS systems

This is known by several trade names such as battery-less flywheel, and others. This UPS technology provides power conversion, power continuity, generator backup and in some cases, an ability to derive both UPS and generator power from the same system or skid. Stored energy is provided via flywheel systems identical to the static or rotary UPS power system or via an inductive coupling system coupled to the generator.

9.5.4 Paralleling and controls

Paralleling and controls should follow the rules set forth in Section 9.7, which calls for local operation and automatic response to failures. While bypasses may be rated for momentary duty for some UPS systems, Class F3 and Class F4 systems have a continuous-duty rated bypass. Controls should present a clear and concise message and exact system presentation to the operator, denoting the power flow, metering levels of all electrical values, summary functions, and alarms. This is traditionally done via some form of graphical user interface (GUI), each unique to the given system manufacturer.

For paralleled systems with a single control all available power modules should share load equally under normal operating conditions and under failure and maintenance modes of operation. For physically paralleled system, where the outputs are connected directly and physically to a single collector bus, the controls are traditional and are built into the PLC or control logic of the UPS system’s control cabinet.

The challenge resides in virtually paralleled system, such as the xN Distributed Redundant Class F4 system. In this case, there is no centralized load balancing and control like the system control cabinet of the physically paralleled system. For the xN system and those like it, the control system is actually the sequence of operations for the system. In summary, the virtually paralleled system’s controls are based on how the individual UPS systems respond to external changes in the other systems.

See Sections 9.7.2 and 9.10 for other requirements.

9.5.5 Batteries and stored energy systems

9.5.5.1 Introduction

Batteries, flywheels, thermal, compressed gas, and induction clutch systems are all examples of viable stored energy sources for UPS systems. The critical points are (1) a stored energy system must be appropriately matched and engineered to the UPS power system it serves, and (2) a stored energy system must carry the critical load until the input source is restored and the UPS systems returns to its particular form of ac power input.

Although a generator or alternate source of power must be present to apply a Class F1 or greater classification, the stored energy system may vary in its capacity, known as the watt-hour rating. The watt-hour rating is related to the stored energy technology used and the amount of backup time required by the system's design.

9.5.5.2 Applications

9.5.5.2.1 Risk analysis

A well-constructed risk analysis (see 6.4) will be crucial in the determination of a data center Class, which in turn will drive decisions on specifications for an energy storage solution. The probability of power interruption factored against the criticality of the load will influence the type, duration, and investment in energy storage.

9.5.5.2.2 Common versus distributed energy storage systems

While using a common energy storage system to serve several UPS modules can reduce the installation cost, this introduces a single point of failure and reduces overall reliability. Thus, a common energy storage system is strongly discouraged and should not be used for higher Classes.

For distributed energy storage, individual battery strings should be provided for each power module. Multiple battery strings may be provided for each power module for additional capacity or redundancy.

9.5.5.2.3 Runtime and overall capacity

If the only requirement was to ride through a transfer from one ac input source to another (e.g., between a generator and a utility), only a few seconds of stored energy would be required. However, one must weigh the possibility of failure or unavailability of the transfer mechanism or the alternate power source. For example, if the standby generator failed to start, would it be feasible for the stored energy source to support the loads until they could be gracefully shut down or to transfer data to a hot site? If so, one must calculate the time required to respond and accomplish the necessary activity.

Some mechanical and hybrid systems are quite effective at riding through the few seconds required to bring the alternate power source on line. For longer ride through times, the more common approach has been to use a chemical energy storage device such as a battery or a hybrid chemical/mechanical system. Some chemical technologies are comparatively unstable at the low end of watt-hour requirements, so the technology itself can dictate a longer backup time. For example, lead-acid batteries are rarely recommended to be sized for less than five minutes. As most chemical energy storage devices lose capacity as they age, one should size the battery ride-through time based on the nominal capacity at the predicted end-of-life. Other sizing considerations can include derating batteries and cables for extreme temperatures and dc voltage drop over cable runs between the battery and the UPS.

While a specific minimum backup time is not stated in this section, a system capacity of 5 minutes is a safe minimum rating for most applications. Some facilities, such as access provider central offices, primarily use dc power systems and have several hours of batteries. Attention should be paid to paralleled systems or redundant modules systems where the battery strings of the "greater than N systems" offer greater run time than the sum of the rating of the individual modules. For example, a four module, N + 1 paralleled UPS system with individual 15 minutes batteries can yield a battery backup time well above 15 minutes, as long as all battery strings are connected (e.g., not taken out of service for preventive or remedial maintenance).

9.5.5.3 Choice of stored energy technology

The choice of stored energy technology will significantly influence the design, construction, and operation of the data center. Most UPS systems can only work with one energy storage technology, so the energy storage decision can greatly influence the type of UPS system that is selected. The following paragraphs summarize a few of the factors that must be considered.

9.5.5.3.1 Physical, regulatory, and environmental considerations

The following are considerations for the deployment of battery systems:

- Hazardous materials—does the solution include materials that could be hazardous to operators and technicians and under what conditions?
- Hazard class—does the solution create a condition that will require special construction and/or occupancy requirements (such as special room or container construction) and can it be collocated with other equipment?
- Hazardous conditions—what conditions can lead to heightened safety concerns (such as off-gassing during overcharge or destruction due to vibration)?
- Disposal and recycling requirements—does the solution require recycling or return to manufacturer at end-of-life and are recycling plants available?
- Space construction—does the solution require special room construction (e.g., fire resistance, restricted access); can it be installed inside or outside; how much space will it take up; what is the footprint; can the floor support the weight?
- Ventilation and/or exhaust—does the solution require special ventilation or air conditioning?
- Gas detectors—does the solution require gas detectors to prevent build-up of toxic or flammable gasses under any operating conditions; who is responsible for installation, maintenance and calibration? (NOTE: Hydrogen detectors are sometimes considered for lead-acid batteries, but due to a high false-positive alarm rate and frequent recalibration their use is discouraged.)
- Spill containment—does the solution include hazardous liquid that would require containment in the event of a container breach?
- Safety equipment and materials—is special personnel protective equipment (PPE) required for personnel near the energy storage device; are eyewash stations required; is it necessary to keep chemicals in the space to render harmless any chemicals that might be released from the solutions; who can use them; what are the qualifications to become certified?
- Floor drains—does the solution require floor drains to redirect any hazardous liquid or fuel?
- Temperature and humidity controls—does the solution require a narrow temperature and/or humidity environment; What are the penalties for operating outside the thresholds?
- Fire protection—does the solution introduce unique fire protection requirements (such as water-reactive materials)?
- Code requirements—are there local code requirements (e.g., fire, mechanical, electrical) that impose special requirements?
- Audible noise and vibration—does the solution create noise or vibration that could be harmful or annoying to operators or occupants?

9.5.5.3.2 Performance considerations

These are the performance considerations when selecting battery systems:

- Cycling ability—how many times can the solution be discharged and recharged before it must be replaced; what is the significance of shallow (short-duration) and deep (long-duration) discharges?
- Recharge characteristics—following a discharge, how long does it take to recover to full rated capacity; does the recharge affect other systems (such as draw high current or create excess heat)?
- Life expectancy—how long can the solution be expected to be used before it must be replaced under the expected operating conditions; what is the warranted life, and what is the depreciation rate?
- Maintainability—Who can maintain the solution (e.g., can the owner perform routine and/or emergency maintenance, or does it require certified technicians); how often is remedial maintenance required; can the solution be monitored remotely?
- Demonstrated reliability—Does the solution have a proven performance record?
- Availability—Is the solution available from more than one supplier; are repair parts readily available?
- Lifecycle cost—Over a defined life expectancy for a data center (e.g., 20 years), what will be projected cost of installing, operating, maintaining, replacing, removing and recycling the solution?

9.5.5.4 Chemical energy storage options**9.5.5.4.1 Lead-acid batteries**

Although many stored energy technologies exist, the great majority of UPS systems rely on some form of batteries. Lead-acid batteries are unquestionably the most common energy storage solution, even though other batteries are available that can provide higher power density, lighter weight, or other benefits. They get the name because the active material of the positive electrode is lead dioxide, the active material of the negative electrode is lead, and the

electrolyte is dilute sulfuric acid. Lead-acid batteries generally come in two form factors – vented and valve regulated—although there can be significant variations in materials, construction, and suitability for any given application.

A lead-acid battery is considered to have reached the end of its life when it cannot deliver more than 80% of its rated capacity. Other chemical battery technologies allow for adequate operation with lower capacities. Temperature affects the life span or capacity of a battery string (optimum is around 20 °C to 25 °C [68 °F to 77 °F]), with long-term excursions above or below the rated design temperature significantly affecting the battery string’s capabilities. Generally, the life of a lead-acid battery is cut in half for every 8 to 10 °C (14 °F to 18 °F) rise in continuous operating temperature above rated optimal temperature. Lower operating temperatures will cause a lead-acid battery to deliver less than its rated watt-hour capacity and thus give reduced backup time but can have a positive effect on battery life. The opposite happens at high temperatures; backup time is increased, but life expectancy is decreased as temperatures rise.

It is also the nature of a lead-acid battery to take a large dip in voltage when it is first discharged, after which it recovers to or near its normal float voltage. This phenomenon is called *coup de fouet* and can cause some systems to shut down if the dc voltage drops below a threshold. For this reason, lead-acid batteries are rarely rated for operation below 1 to 5 minutes.

Lead-acid batteries should be recycled. Recycling centers are readily available in most countries.

A note of caution about AHJ requirements and code enforcement: some battery regulations are based on the volume of the electrolyte (which is mostly water) in a liquid-filled battery, while some others are based on the actual hazardous material (such as sulfuric acid in a lead-acid battery or potassium hydroxide in a nickel-cadmium battery). The electrolyte volume triggers various storage, installation, ventilation, and reporting requirements for the stationary battery system:

- vented (flooded) lead-acid (VLA) batteries—so called because the byproducts of electrolysis, hydrogen and oxygen, continuously escape into the atmosphere through vents. VLA batteries are also called flooded because the plates are immersed in free-flowing liquid electrolyte. These types of batteries are further defined by the types of alloys used in their grids, such as lead-calcium, lead-antimony, lead-tin, and many others. Because they continuously vent flammable gas, VLA batteries require dedicated rooms with spill containment, dedicated ventilation and exhaust. VLA batteries require regular maintenance and water replenishment. Because they are liquid-filled, VLA batteries are always installed upright, usually on open racks, and require spill containment. Because of potential exposure to high energy and hazardous chemicals, they must be installed in spaces with controlled access;
- valve-regulated lead-acid (VRLA) batteries—derive their name from valves that prevent gas from escaping except when internal pressure builds too high. VRLA batteries recombine hydrogen and oxygen back into water. Their electrolyte is immobilized, either by a gelling agent (gel), which is popular in Europe, or by absorbed glass mats (AGM), which is more common in North America and the rest of the world. Many VRLA batteries can be installed sideways and can be stacked, creating a greater power density. Because VRLA batteries take up less space, require less maintenance, require no spill containment, and are sealed under normal operating conditions, they are often preferred, despite a shorter life span (hence more frequent replacement and higher life cycle cost) compared to VLA batteries. Cabinet-mounted VRLA batteries are often used inside computer rooms.

9.5.5.4.2 Nickel-cadmium (Ni-Cd) batteries

Ni-Cd batteries are usually “flooded” batteries that vent gas in much the same way as lead-acid batteries do. The active material of the positive electrode is nickel oxyhydroxide, the active material of the negative electrode is cadmium, and the electrolyte is dilute potassium hydroxide.

Because they continuously vent flammable gas, Ni-Cd batteries require dedicated rooms with spill containment, dedicated ventilation and exhaust. Ni-Cd batteries require regular maintenance and water replenishment. Note that the electrolyte of a Ni-Cd battery is highly alkaline, so safety precautions differ from lead-acid batteries.

Primarily because of their comparatively high price, Ni-Cd batteries are uncommon in UPS applications except where extremes of temperatures and/or frequent discharges are expected. Ni-Cd batteries are popular as starting batteries for generator systems.

Because they are liquid-filled, Ni-Cd batteries are always installed upright, usually on open racks, and require spill containment. Because of potential exposure to high energy and hazardous chemicals, they must be installed in spaces with controlled access.

Ni-Cd batteries should be recycled. Because of the cadmium content, recycling centers may not be readily available in all countries.

9.5.5.4.3 Monitoring

Like every component of the data center electrical system, the battery systems should be monitored. Most UPS modules have a built-in, proprietary monitoring that indicates string voltage, run time and other basic battery monitoring functions. Battery monitoring is required for Class F2 and higher. Monitoring is required for the individual modules, for paralleled systems, and the entire set of battery strings. However, UPS-based battery monitoring systems may not be capable of detecting individual battery cell failure, which can greatly affect runtime and reliability of an entire battery system.

For Class F3 and Class F4 systems with lead-acid batteries, strong consideration should be given to a battery monitoring system capable of recording and trending individual battery ohmic values. A standalone battery monitoring system, capable of monitoring the ohmic values of each individual battery cell or container as well as predicting and alarming an impending battery failure, provides much greater detail on the actual battery status. Such systems are most effective when comparing a data point against an established base line, which requires comprehensive record keeping and trend analysis. These systems are desirable for Class F3 systems and are required for Class F4 systems. Systems capable of providing cell charge equalization and charge management are desirable for Class F3 and Class F4 systems.

9.5.5.5 Mechanical energy storage options

- Flywheel—flywheels have been around for many years to ride through short duration sags or interruptions (subsecond to many seconds). Advances in composite materials have allowed some systems to achieve minutes of ride-through. However, price and complexity of controls have limited their widespread adoption. Flywheels are almost immune to heat, but can be affected by seismic activity.
- Flywheel/battery hybrid—for some hybrid UPS systems, very specific systems are provided and coupled with a power conditioning system (typically a mechanically-isolated synchronous machine with a variety of input and output filtering) with a generator system and some form of bridging system that allows for an expedited generator start and load assumption. These clearly and fully satisfy the need for the stored energy system to carry the critical load until the failed utility input is replaced by the Generator or some other planned input. In this case, the UPS is a systems-based solution that meets the requirements of the critical load.
- Other variations allow the mechanical inertia to sustain conditioned power to the load for short duration (subsecond) disturbances, but will switch to battery backup for longer power interruptions. The battery sustains the load until the primary or alternate source of ac input power is available or until all useful energy is removed from the battery.
- Induction coupling—This sort of batteryless UPS marries a generator and a prime mover (usually a diesel engine) into a single system via an induction coupling system. The prime mover sits idle until the main input power is interrupted. An inner rotor of the induction coupling stores sufficient energy to bridge the prime mover start time. The generator provides electrical power to the load during an outage. In normal mode, the generator acts as dynamic filter and provides power factor correction.

9.5.5.6 Emerging energy storage technology options

The following technologies collectively represent less than 10 percent of the installed base at the time of this standard but are expected to increase market share in the coming years:

- Stationary lithium ion batteries—Primarily known for their versatility, high- energy density, excellent cycling capabilities, and lightweight in small, portable applications, lithium ion batteries are starting to penetrate the stationary battery market. There are many variations of lithium batteries, with some performing better than others in high-rate UPS applications.
- Stationary lithium polymer batteries—These batteries are known for their flexibility in form factor and shape, as well as their versatility, high-energy density and lightweight in small, portable applications. Lithium metal polymer batteries show promise for high temperature environments.
- Stationary nickel-metal hydride batteries—Although they are not as small and light as Li-Ion batteries still have many advantages over lead-acid in space and weight, and appear to perform better than Li-Ion batteries in UPS applications, especially for applications with constantly changing loads.
- Supercapacitors—A supercapacitor or ultracapacitor is an electrochemical capacitor that has an unusually high-energy density when compared with common capacitors. They are of particular interest in UPS applications as a supplement to batteries. They are able to ride through thousands of short duration power sags or interruptions (subcycle to a few seconds) without forcing the UPS to exercise the battery and can be rapidly recharged. At the present time, supercapacitors are not seen as a practical replacement for most battery systems.

- Fuel cells—Fuel cells are gaining more interest as a replacement for standby and emergency generators because of they are quiet and efficient, have no byproducts harmful to the environment, and can be put in places where a generator cannot go. Because fuel cells cannot supply energy instantly upon demand, they still require a battery or supercapacitor system to bridge the time period required for the fuel cell to ramp up to full capacity.
- Compressed air storage—An energy storage system that uses compressed air as the storage medium.

9.5.5.7 References

For full details on battery systems, the reader is directed to the IEEE standards, recommended practices, and guidelines as in listed in Table 11.

Table 11: Battery Standards Cross-Reference table (IEEE Standard Number)

	<i>Lead-acid batteries</i>		<i>Nickel cadmium (Ni-Cd)</i>	
	<i>Vented (flooded)</i>	<i>VRLA</i>	<i>Normal use</i>	<i>Photovoltaic (PV)</i>
Selection/sizing	IEEE 485	IEEE 1189	IEEE 1115	IEEE 1013
Installation	IEEE 484	IEEE 1187	IEEE 1106	IEEE 1145
Maintenance/testing	IEEE 450	IEEE 1188	IEEE 1106	

	<i>UPS</i>	<i>Monitoring</i>	<i>Spill Control</i>	<i>Ventilation</i>
Special interest	IEEE 1184	IEEE 1491	IEEE 1578	IEEE 1635*

* Not yet released at the date of this publication

9.6 Standby and emergency power systems

NOTE: Section 9.6 may be treated as recommendations

9.6.1 Sizing and application

Standby power systems are intended to support the data center in the event of a loss of primary power lasting longer than the capacity of the UPS battery (e.g., utility outage lasting for hours or days). Interest in fuel cells and other sources of on-site generation is growing, but the penetration of such emerging technologies into the IT space is still only a small percentage. The overwhelming preference is for generator systems, usually diesel, but turbine and gasoline-powered systems are also in use, especially in smaller data centers. For purposes of this document, assume that the standby power source is a generator system.

The generator plant is a site-controlled power system that offers a stable, reliable power supply during critical maintenance operations and in the absence of utility power. For some installations a campus-based power plant or some other legitimate, alternate power source can satisfactorily substitute for a generator plant.

The rating of a generator or the entire generator system requires consideration of the harmonic content and power quality of the load itself as well as starting and transfer requirements of the IT, mechanical and noncritical loads. When addressing starting current, the maximum droop typically seen is 15%. It is not suggested that this large a droop be allowed, as with voltage drops of this magnitude, running systems can drop out unexpectedly. Conversely, lightly loaded generators operate poorly, tend to wet-stack (the buildup of particulate on the fuel injection, valves and exhaust system due to lower operating temperatures of the engine) and eventually operate at a lower capacity.

The following conditions should be considered when sizing individual generators and when using paralleled systems:

- Transfer scheme – closed or open transition
- Harmonic content of the load
- Allowable voltage sag or droop for the mechanical and lighting systems
- Generator system topology and unit count – how many units are required for the load, maintenance rotation and for redundancy
- Inrush and motor starting loads on the initial outage as well as when loads are being brought back on manually after maintenance

- Operating humidity and temperature – based on ASHRAE, or local equivalent, extreme temperature for the area of operation
- Altitude of the site
- Pollution abatement – air quality, location in relation to building ventilation
- Noise abatement
- Expected run time for the system
- Minimum and maximum load levels, and the specification of standby-, continuous- or prime-rated systems
- Coordination of reactors and high-resistance grounding with the remainder of the electrical system
- Coordination of UPS battery recharging loads

The generators should support all loads related to the data center – process or IT loads, cooling and ventilation as well as noncritical and building loads. For larger campuses where the data center is an important but not the largest tenant, the generator plant may be sized to accommodate other loads on the site requiring standby power.

Generators supplying the entire load of a data center that is identified as an emergency system as defined in the AHJ electrical codes and in prevailing standards such as *NEC* Article 700 must be equipped with separate ATSS. The Emergency System loads must be separated from the rest of the data center loads, with their own ATSS.

For all Classes, the generator load is suggested as the entire load of the data center, as well as any other loads required to support the data center, such as well pumps, security systems and other campus- or site-based systems. When data centers are installed in health care facilities, the data center load qualifies as an equipment branch load for the nonessential emergency power system.

When the application of a data center affects life safety, the generator and the downstream power distribution system will be given an “emergency” designation, in which its use can be dedicated to specific loads and not shared with other loads. Two systems might be required - one for standby operations and one for emergency operations. This may be accomplished with a separate life-safety branch, that exclusively serving life-safety loads, while data center loads would be served by other systems under a single generator or generator system.

Most jurisdictions have substantial planning and operating requirements for stationary generator plants. These requirements include noise abatement, pollution allowance and/or abatement, fuel storage, operating hour limitations, structural attachment, fire suppression and operating permits. Check with your local jurisdiction during the planning phase of your data center project in order to ascertain the precise requirements for your undertaking and to determine who is responsible for reviewing and approving your installation.

9.6.2 Starting systems

The most common generator problem is a failure to start. Larger generators tend to have multiple starters based on the size of the engine, but the multiple starters offer nothing as far as starter redundancy – the multiple starters simply get the engine turned over more quickly.

For data center applications where the restoration and continuity of power is vital, the site’s generator(s) need to start, and assume the facility’s load as quickly as possible. Faster starting can be attained by numerous methods such as larger-than-standard starters, stronger/higher ampere-hour, or redundant starting systems. In all instances, starting systems can be upgraded using marine-grade starting systems in lieu of standard commercial or industrial systems. Like all batteries, the batteries’ onboard the generators do best at their rated temperature. Higher or lower temperatures will result in shorter battery life or lower cranking power. For high availability applications, battery systems can be combined using a best battery selector or auctioning bridge.

9.6.3 Fuel system

Poor fuel quality is a leading cause of system interruption during extended generator runs. Poor fuel quality tends to clog injectors and filters, thereby strangling the fuel supply to the generator. Fuel quality is managed in three, separate ways – fuel additives, fuel treatment and fuel filters on the generators.

Bulk fuel storage can be compromised by water, microbes or particulates that infiltrate the fuel tank under normal weather and operating conditions. Fuel additives and treatments can help mitigate this condition, but do not offer a foolproof method of safeguarding the fuel supply.

Fuel treatment takes place in a separate fuel polishing system on the primary fuel supply lines to the generator(s). The polishing system removes a bulk of the particulates and water from the fuel and takes the pressure off the generator-based fuel filters as the single point of fuel cleaning. Fuel polishing should allow the filters to be bypassed if they become clogged, reverting to the generators for the primary fuel filtering function. The fuel polisher should be able to be serviced while fuel is passing through the system on the bypass loop.

The final stage of fuel filtering is the onboard fuel filters on the generator itself. Three-stage, spin-on-type fuel filters (100 micron, 30 micron, and 10 micron) with individual valves for removal while the engine is operating are

required for Class F3 and Class F4 facilities. Marine-grade systems are recommended for all installations, and mandatory for Class F3 and Class F4 facilities.

Single-stage spin-on-type fuel filters (100 micron or 30 micron) with individual valves for removal while the engine is operating are the minimum requirement for Class F1 and Class F2 facilities.

Generators should each have their own day tank to allow for fuel cooling when the engine is consuming fuel at less than rated levels and to avoid having the fuel tank being a single point of failure. While it is sometimes not practical to divide the main bulk fuel storage tank into individual or partitioned tanks, this is highly desirable for Class F3 and Class F4 facilities.

The data center's fuel supplier should have a large reliable source of fuel that is available for delivery of fuel 365 days/year, 7 days/week, 24 hours/day. The supplier should be able to continue to supply the data center with fuel if there is an area disaster. Alternatively, the data center's fuel tanks need to have enough capacity to provide electricity during an extended power outage caused by an area disaster such as an earthquake, flood, or hurricane.

Fuel lines on the generators should be marine-grade, with all connection points to the chassis routed through insulated bushings.

9.6.4 Exhaust system

Exhaust systems are linked to two issues for the site – the pollution abatement system and the sound abatement requirements. Silencers come in four types: none, residential, industrial and critical grades. The silencers affect engine efficiency, with quieter silencers affecting engine capacity. Sound abatement on the air intake and radiator exhaust system can also affect the airflow to the engine. The silencers are linked to the overall noise abatement plan for the site.

In addition to silencers, pollution abatement systems may be required by local and regional authorities. Pollution abatement addresses two forms of emissions—particulate emissions and NO_x emissions. The engine specification itself will need to be coordinated with any low emission site. Also, scrubbers (devices to remove impurities) may be required on the exhaust.

The exhaust system is typically airtight, with welded construction and flexible metal connections between the engine exhaust manifolds, the silencers, and abatement systems. Exhaust piping that terminates horizontally is typically angle cut to prevent water infiltration, while vertical piping is provided with a flapper- or hat-style cap. Flapper or hat style caps can obstruct air flow and may not be allowed due to air emission restrictions. In areas with freezing temperatures consider the possibility of the flapper freezing in the closed position and not allowing the engine to start.

9.6.5 Cooling system

The cooling system should ensure that the generator windings and engine block water jacket remain within the manufacturer-specified temperature ranges.

Cooling systems can be via skid-mounted radiators, remotely mounted radiators, or high-reliability central water system. For higher reliability applications, cooling systems are typically automotive-type glycol/water-based fluid radiator systems with crank-driven cooling fans that are isolated to the individual machine. If centralized cooling for the engine blocks is being considered, the water delivery system must possess redundancy in the pumping and piping systems.

9.6.6 Mounting

Generators offer the compounded issue of large live loads that vibrate while operating. Substantial foundations are required for any generator system, and this is coupled with some form of vibration isolation. Vibration isolation could be in the form of pads or spring-isolation devices. In areas subject to seismic events, snubber-type bases that allow for operation while the unit is being shaken are typical and are used pursuant to the site's given seismic risk.

9.7 Automation and control

9.7.1 Introduction

Monitoring is defined as the telemetry and ability to view what is going on in a given system, and in some cases, integrates and manages alarm and trouble signals from the monitored systems.

For the purposes of this section, control is defined as any device that directly regulates a change in state in a given system. Controls are an active system, and may be either be:

- manually initiated and automatically operated based on human input or decision, or
- automatically initiated and operated based on a predetermined script or response to a failure or external change of state.

9.7.2 Monitoring

9.7.2.1 Requirements

Without monitoring, operators are not able to respond to failures or to determine the loading or operation of their systems. Monitoring is mandatory for all Classes, with increasing levels of observation scope and granularity with increasing Class.

9.7.2.2 Recommendations

As Class level increases, monitoring increases by replacing summary alarms with individual alarm points, and by presenting systems virtually for the system operators. For Class F4 systems, a virtual single line, which clearly shows system loading and power flow, should be provided. In some instances, a simulator is also provided where changes of state can be tried in a virtual setting to see the outcome prior to employing them in the live, working environment. Electrical systems should divulge all changes in state, alarms, pre-alarms and positions of all breakers, and switches as well as general system information.

Power quality monitoring (PQM) for data centers is recommended, since IT systems may be sensitive to power quality, transients, harmonics and other types of waveform disruption. Power monitoring is also vital as waveform disturbances offer a precise definition of experienced failures and outages. When addressing power system monitoring, there are three facets of observation:

- power levels noting voltage, current, and frequency;
- harmonic content;
- waveform imaging and capture.

Power monitoring offers sampling of the power system's quality in a manner similar to a mechanical system's monitoring of temperature or water chemistry to the chiller/cooling system. PQM should be located at portions of the electrical system that offer a complete view of the vital locations where power is being converted. No particular favor is made over switchgear-integrated monitoring or stand-alone systems. The key element is how they are used.

For the varying levels and locations for PQM, as well as systems and component monitoring for each of the Classes, see Table 13 (located in Section 9.13).

9.7.3 Control

9.7.3.1 Recommendations

The operation of electrical systems should be automated to the extent possible to minimize human error, which is the predominant cause of system outages. The system should be thoroughly documented, and maintenance staff should be thoroughly trained. Training should include a good understanding of automated procedures and manual override procedures if it is necessary to override the control systems.

Power system control offers substantial challenges to both physical safety and operational assurance. Remote control of critical power systems offers an opportunity to remotely respond to changes of state. However, remote control also offers the hazard of operating large power systems without clear, in-person visual indication as to the result or consequence of the action. Remote control also introduces security concerns and will require provisions to prevent unauthorized access via the internet or other means.

Power system controls should follow these guidelines:

- Local control only.
- Remote monitoring always.
- Control methodologies that react only to the attendant system. Upstream and downstream systems should react to the changes in state of adjacent or attendant systems, without a direct, physical control connection. Controls should be autonomous from any centralized controls, unless the facility chooses to operate the system remotely.
- Control interfaces on each piece of equipment should be clear and concise. Color-coding equipment to denote the particular system, internal switchgear busing (known as mimic busing), position indicating lights, and clearly written labels and nameplates, usually in English and/or local language, are best practices.
- standard operating procedures should be posted on each piece of equipment.

9.7.4 System integration

9.7.4.1 Recommendations

Some form of system integrator is typical for more complex or widespread monitoring systems. The electrical system should integrate to a single “electrical” supervising management system. This system may be a stand-alone, dedicated electrical monitoring system or may be integrated into an overall monitoring and control system that addresses temperature and mechanical system control and monitoring.

The integrator offers a lower workload and database function that categorizes alarm and trouble signals by time or system. Aside from that, the electrical system’s monitoring integrator should also mask and manage duplicate alarms for subordinate systems through consolidated control points such as paralleled UPS modules or generators.

9.8 Lighting

9.8.1 Introduction

Lighting systems are to be designed to provide lighting levels sufficient in output and quality for the task in each area, while being of maximum energy efficiency. Elements to be considered are:

- Fixture types
- Lamping types
- Ease of relamping
- Emergency lighting capabilities
- Lighting controls for both safety and for energy efficiency

9.8.2 General Recommendations

The following are recommended to be considered when planning lighting:

- Day lighting of personnel areas such as command center, offices, conference rooms and break areas, with day lighting interface controls is recommended where at all practicable.
- Indirect or a combination of direct/indirect lighting is recommended for personnel and processing equipment areas.
- Switching and/or controls are recommended to be located so as to be convenient for all of access points to equipment rows and working areas.

It is recommended that a three-level lighting protocol be used in data centers depending on human occupancy.

- Level 1: When nobody is scheduled to be in the data center space, the lighting level should be just high enough that security personnel (stationed outside the unoccupied data center spaces) can monitor the space with surveillance cameras. Cameras should be specified for low-light operation.
- Level 2: Motion detectors should automatically initiate a higher level of lighting once access is detected. The level of lighting should be high enough to clearly permit identification via security cameras. These motions sensors can also replace a manually-switched lighting control system.
- Level 3: Lighting should be a minimum of 500 lux (50 ft-candles) in the horizontal plane and 200 lux (20 ft-candles) in the vertical plane, measured 1 m (3 ft) above the finished floor in the middle of all aisles between cabinets. It is permissible to divide the space in zones and either activate level 3 lighting only in selected zones that require work on equipment or illuminate the complete facility with an override switch. When only selected zones have level 3 lighting activated, the remainder of the space should be on level 2 lighting for human safety reasons.

The motion sensor-based lighting controls would activate lighting in phases, depending on which area of the data center requires occupancy for work or passage. The lighting control system would “sweep” the area and extinguish the lighting after a preset time in order to conserve energy.

Lighting levels required to maintain Code-required egress from the space should be maintained at all times and should be coordinated with the Level 2 lighting requirement noted above.

9.8.3 Computer rooms

When occupied, the computer room should have a minimum of 500 lux (50 ft-candles) maintained in the horizontal plane and a minimum of 200 lux (20 ft-candles) maintained in the vertical plane of the data racks, both measured at 1 m (3 ft) above the finished floor. Lighting fixtures should be selected to prevent glare on equipment monitors. The lighting uniformity in the rooms should equal or exceed 90%, or the difference between the highest and lowest foot-candle levels in the room. Lighting control should be located at the room’s exits, with occupancy sensors being highly desirable. Local jurisdictions have varying energy and control codes to conform to as well.

Fluorescent lighting fixtures should be specified with low-RF ballasts. While high-intensity discharge (HID) lighting such as metal halide or mercury vapor are not specifically excluded, the restrike time of the fixtures should be as short as possible to prevent long-term lighting outages in the room.

Since the data processing rooms are typically windowless, instant-on lighting is required for the safety of personnel working in the data processing areas during the time the utility outage occurs and the generators assume the load. In this case, 50 lux (5 ft-candles) maintained over 50% of the room is suggested.

Exit signage, egress lighting and other code or AHJ required life-safety lighting systems should be provided pursuant to local codes and the requirements of the AHJ.

Portable, battery-powered lanterns are recommended to be placed in all computer rooms.

9.8.4 Support areas

All support spaces should be lit pursuant to the Illuminating Engineering Society (IES) recommendations.

For control rooms, operations center and other support spaces, fixture systems should be selected that reduce or eliminate glare on computer displays. Lighting systems for this area should be commensurate with the noncritical office areas within the facility. The lighting uniformity in the rooms should equal or exceed 90%, or the difference between the highest and lowest foot-candle levels in the room. Lighting control should be located at the room's exits, with occupancy sensors being highly desirable. Local jurisdictions have varying energy and control codes to conform to as well.

Fluorescent Lighting fixtures may be specified with standard RF ballasts. Some support spaces, such as generator rooms or large-area central plant spaces, HID lighting such as metal halide or mercury vapor may be used. Should HID sources be used, the restrike time of the fixtures should be as short as possible to prevent long-term lighting outages in the room.

9.9 Bonding and grounding

9.9.1 Introduction

The comprehensive electrical protection required for the critical facility is achieved using a system approach to integrate lightning protection, overvoltage and surge suppression, bonding and grounding and electromagnetic shielding. This section covers these different systems, which are interdependent upon each other for proper function and efficacy.

Grounding is addressed in three sections: electrical distribution, PDU, and within the computer room.

Electrical system grounding is consistently misunderstood and, for most facilities, not adequately maintained, changed or integrated to the IT loads that they serve.

Applicable electrical codes require a properly designed AC power bonding and grounding system of sufficiently low impedance at 50 to 60 Hz to substantially equalize any non-transient potential differences so that all the enclosures, raceways and all bonded metal found in the computer room are effectively at the same ground potential (substantially equalized). At higher frequencies consideration must be given to the impedance of a conductor, not just the resistance.

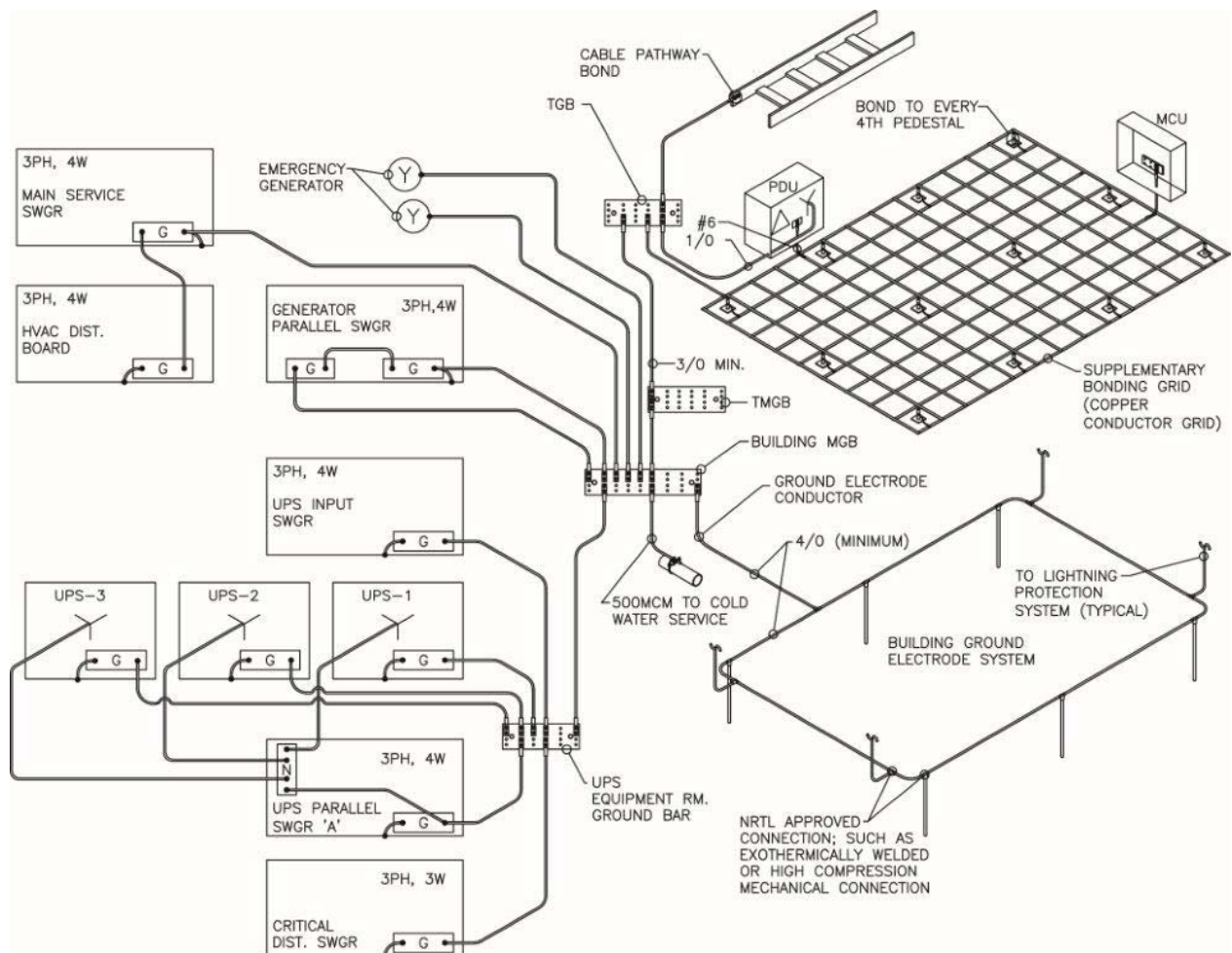
Bonding and grounding of data centers relates most specifically to maintaining the facility's common electrical bonding and grounding system along with any desired supplementary bonding and grounding for the Information Technology Equipment (ITE). Grounding also addresses such vital issues as harmonic current management and fault current mitigation. Grounding also integrates voltage transient suppression by the application of SPD systems as well as lightning protection systems. The grounding system is one of the few electrical systems completely systemic to the entire critical facility.

Bonding and grounding are essential for the safety and performance of electrical power systems, electronic equipment and surge protective devices typically utilized for a data center. Typically, systems, equipment and devices are solidly grounded. However, sometimes high-resistance/impedance grounding systems are used for both fault current mitigation as well as for the selection and avoidance of ground fault circuit tripping. These features are useful where process control requires an orderly shutdown to avoid high costs of restoration of the process. Typically, this feature is utilized as required for industrial facilities. Where used for IT installations, consideration should be given to any impact the resistance/impedance grounding systems may have on the level of electrical noise vs. earth ground at higher frequencies such as for filters. The impact may occur due to reactance of the resistance/impedance devices such as an inductor or wire-wound resistor. Inductive/reactance or resistively grounded power systems are not recommended. Check with the UPS system manufacturer if it is not connected to solidly grounded neutral sources.

Serving power systems and electronic equipment bonding and grounding primarily involves the serving power source and the power distribution to the IT and other electronic equipment. This primary level of bonding and grounding is required to be in accordance with the NRTL product safety listing of the power system and the electronic equipment (load). The entities of concern are the grounding electrode conductor (system) and equipment grounding (bonding) conductor (or green wire). These dedicated circuit conductors are required for the safe operation of the equipment, including any ground faults. In some instances, equipment may be designed as ‘double insulated’ whereby the NRTL requirements for the equipment grounding conductor may be somewhat relaxed (such as a two-prong plug or receptacle). Although data center electrical and electronic equipment may be considered ‘grounded’ according to its NRTL requirements, supplementary bonding and grounding are recommended.

If properly organized and installed, the ground system is essentially a radial system from the electrical service entrance. There are a few subtleties for critical facilities that vary from other buildings. Where generators are not treated as separately derived sources, neutrals and grounds are routed with the associated phase wiring and carried back (without being switched) to the main service and terminated on the main service’s neutral and ground buses. Where generators are treated as separately derived sources, grounds are carried back to the main service and terminated on the main services ground bus.

The data center or critical environment specifics are noted later in this section. A simplified example model for a critical facility grounding system is shown in Figure 38.



Note: not all items shown are present in every data center.

Figure 38: Critical Facility Example Grounding Diagram

Bonding and grounding for a data center involve several entities such as:

- a common grounding electrode system for the building, involving the intersystem bonding of a:
 - grounding electrode system for the electrical power;
 - grounding electrode system for the lightning protection system (LPS);
 - grounding electrode system for the telecommunications service provider cables and protectors.
- grounding electrode conductors for solidly grounding each ac power service entrance;
- grounding electrode conductors for solidly grounding each separately derived power source, such as an engine-generator for standby power;
- grounding electrode conductors for solidly grounding each telecommunications service entrance;
- intersystem bonding conductor(s) such as a ground ring;
- bonding and grounding infrastructure for telecommunications utilizing components such as the BCT, TMGB, TBB, TGB and GE as identified in ANSI-J-STD-607-A;
- equipment grounding conductor for power distribution from the service/source to the load (a grounded raceway plus an additional insulated grounding conductor);
- supplementary grounding electrodes such as building steel at a nearby column;
- grounding conductors such as the down conductors for a LPS and SPDs;
- the common bonding network (CBN) within the building that is a set of metallic components that are intentionally or incidentally interconnected to form the (earthed) bonding network (a mesh) in a building. The CBN always has a mesh topology and connects to the grounding electrode system via one or more grounding conductors;
- supplemental bonding and grounding structures for electronic equipment; such as:
 - mesh-bonding network (mesh-BN);
 - isolated bonding network (IBN);
 - supplementary bonding grid.

Data center grounding addresses all bonding and grounding work within the critical environment. These systems include:

- the separately-derived system at the PDU;
- ground path to the load;
- critical environment grounding—supplementary at the ITE;
- ITE bonding and grounding;
- personal grounding and static discharge.

9.9.2 General recommendations

The following considerations are important for understanding the complexities of bonding and grounding for a data center:

- equipotential grounding becomes increasingly difficult across an expanse such as a building or larger data center;
- distributed grounding (within a building or complex) cannot accomplish equipotential grounding;
- a dedicated and separate ground for data center equipment is NOT recommended and is entirely probable to be an electrical safety violation;
- especially where multiple services (power and communications) enter the building at separated locations, a buried ground ring is recommended to serve as an intersystem bonding conductor. Where multiple power service entrances are involved, the ground ring conductor should be sized at 120 mm² (4/0 AWG) minimum bare copper;
- where equipment is designed for double insulation, grounding that equipment may be a secondary concern (pending its product safety listing requirements and electromagnetic emissions compliance);
- any electrical grounding infrastructure (such as NEIS 331-2004) placed for the electrical power system should not replace the separate bonding and grounding infrastructure for telecommunications (ANSI-J-STD-607-A);
- generally, the infrastructure described in ANSI-J-STD-607-A is better placed in the central portions of the building and away from exterior locations where lightning current activity is more likely;
- generally, all dead metal objects within the data center should be grounded (this includes empty racks and cabinets and ladder racks);

- supplementary bonding and grounding of data center equipment is recommended (this is over and above bonding and grounding of the serving power distribution) as it:
 - provides for more locally grounded equipment;
 - maintains a level of grounding even if the serving power circuit grounding is interrupted;
 - provides dispersed path(s) for ESD currents to follow;
 - provides conductive paths among interconnected equipment where common configurations include grids and planes. The mesh-BN, pending its installation techniques, inclusion of a supplementary bonding grid, mesh density and the routing pattern of signal and power cabling may:
 - further reduce the levels of inter-unit common-mode electrical noise on signal and power cabling
 - provide a lower resistance and lower impedance inter-unit ground reference
 - reduce damage to inter-unit equipment during power fault and surge events
 - an isolated bonding network (IBN) may be utilized for certain telecommunications applications whereby the electronic equipment system is only grounded via a single point connection window. This concept has been used by the telecommunications service providers (primarily for dc powered systems, but may also be applicable for ac powered systems).
- Data circuits between data centers and different floors should be decoupled to prevent issues related to unwanted electrical transients. Fiber optic circuits and links are ideal for decoupling. Some types of circuits may utilize suitable transformer isolation for decoupling.

9.9.3 Lightning protection

9.9.3.1 Introduction

Lightning events resulting in fires, damage to buildings, and breakdowns to electrical, telephone and computer installations can cause considerable losses in operational revenues and customer dissatisfaction. Damage results from electromagnetic fields from the lightning strike, voltage differentials in ground systems, and structural damage from ohmic heating or mechanical forces. This damage can be attributed to insufficient direct strike protection, deficient grounding, bonding and shielding techniques for the susceptibility level of the installed electronic equipment systems, and deficient selection and installation of surge protection devices.

Depending on the geographical location for the data center there may be local guides available specific to the country or region such as The Risk Analysis Guide provided in NFPA 780, which takes into account geographical location and building construction among other factors to determining the suitability of a lightning protection system. If a lightning protection system is installed, it shall be bonded to the building grounding system as required by the prevailing standards and AHJ and as required for maximum equipment protection.

The key points for the lightning protection system are that it:

- is applied as a comprehensive system;
- shall be system integrated with properly sized SPDs;
- covers all systems and buildings serving the critical environment.

For some locations, lightning protection is required by AHJ (e.g., NFPA 780) for basic building safety and protection.

9.9.3.2 Recommendations

Where lightning protection from voltage fluctuations and transients is to be provided for protection of critical facilities, installation should be in accordance with industry recognized standards such as NFPA 780, IEC 62305-3, and IEC 62305-4.

9.9.4 Surge protective devices

9.9.4.1 Introduction

Surges and transient power anomalies are potentially destructive electrical disturbances, with the most damaging being overvoltage occurrences and short duration overvoltage events. High-energy transient power anomalies can arise from inductive load switching or other events within the power system or capacitive and inductive coupling from environmental events such as nearby lightning activity. Environmental and inductive power anomalies are wideband occurrences with a frequency range from close to dc to well into the RF high-frequency spectrum. It is critical that each point-of-entry (ac, telephone, LAN, signal/control and RF) into the equipment area be protected against these anomalies. This protection is essential to reduce the risk of personal injury, physical equipment damage, and loss of operations. Although lightning can cause the most visible damage, it is not the predominant cause of transient voltages.

Sources of transient voltage include, but are not limited to:

- power company switching;
- generator transfer;
- shared commercial feeders with poor line regulation;
- load switching;
- fault currents;
- HVAC units;
- heating elements;
- power tools;
- electric motors;
- fluorescent lights.

9.9.4.2 Recommendations

The installation of surge protection devices is a requirement for all data centers. A lack of surge protection devices would result in a Class F0 rating.

9.9.4.3 Recommendations

9.9.4.3.1 AC power surge protection

Surge protective devices (SPDs) offer two benefits for high-availability facilities. The first is that SPDs are an integral part of the lightning protection system for the facility. The second is the voltage transient mitigation.

SPDs shall be installed in the following locations:

- utility service entrances;
- generator buses;
- UPS inputs;
- UPS outputs;
- UPS power distribution switchboards;
- PDUs and critical power distribution panels.

SPDs should not be mounted inside the switchgear (unless specifically designed, manufactured, NRTL listed and properly installed for integral installation) and should be installed with minimum lead lengths and separation of input/output wiring in order to perform properly. For application guidance on the use of facility level SPDs for ac power systems see IEEE C62.72 and IEEE Std 1100.

9.9.4.3.2 DC power surge protection

For basic guidance, see IEEE Std 1100-2005.

9.9.5 Telecommunications surge protection

9.9.5.1 Requirements

9.9.5.1.1 Primary protection

The purpose of primary protection is to help ensure personnel safety and help protect internal cables from extremely high voltage. The installation of primary SPDs shall comply with all applicable codes. The devices shall conform to the international CE certification mark, shall be UL 497 listed, UL 1449 (latest edition) listed or recognized, or as required by AHJ. The SPD shall be installed at the entrance point into any building and within close proximity (adjacent) to the electrical service entrance and the building electrical main ground bar. Minimizing the grounding conductor lead-length between the SPD and electrical service entrance will improve the efficacy of the SPD device by reducing the self-inductance of the grounding lead. This will help reduce the voltage rise between the SPD and the electrical service entrance. In lightning prone areas, a primary SPD shall also be installed on each end of an inter-building cable run to help ensure that high energy is not allowed to penetrate the building interior. In some applications, a fused type primary SPD may be required. To reduce the need for fuse replacement, devices that incorporate resettable fuse technology are recommended.

The primary SPDs telephone circuits, data circuits, and control circuits shall be grounded in accordance with NFPA 70 Article 800.100 or other applicable codes or standards. Primary SPDs shall have the ground terminal bonded to the building MGB, TMGB, or a dedicated ground bus conductor. The conductor shall be free of sharp bends. The grounding conductor for a single line primary SPD shall be 6 mm² (10 AWG) or larger; the grounding conductor for multiple line primary SPDs shall be 16 mm² (6 AWG) or larger.

9.9.5.1.2 Secondary protection

The primary purpose of secondary SPDs is to limit the magnitude of current that can be imposed on the secondary wiring from the primary SPD to the IT. To be effective, the secondary protection must properly coordinate with the primary protection. A collateral purpose is to limit transient over voltages to within the prescribed withstand level of the protected equipment. The SPD also serves as a barrier against transient anomalies that may be induced between the cable entrance point and the equipment, and in cable runs within the building.

Secondary SPDs shall be installed as close to the equipment being protected as possible. This includes, but is not limited to, the circuits associated with the base stations, repeaters, remotes, modems, consoles, Network Interface Units (NIUs) and channel banks that extend from the room or equipment area. Secondary SPDs shall comply with safety and performance standards for their designated function. The devices shall conform to the international CE certification mark, shall be UL 497A listed, or as required by AHJ.

A separate equipment grounding conductor shall be used to bond each secondary SPD grounding conductor or ground terminal of the frame to the TMGB, TGB, or other approved ground bus conductor that serves the associated equipment. The grounding conductor for a single line secondary SPD shall be 6 mm² (10 AWG) or larger; the grounding conductor for multiple line secondary SPDs shall be 16 mm² (6 AWG) or larger. If a separate rack ground bar is installed for the SPDs, it shall be effectively bonded back to the equipment ground bus system.

This conductor shall be as short as possible, free of sharp bends, and shall be routed as directly to the equipment grounding conductor or ground bus as is possible. The operating voltage and SPD configuration is application dependent. Where the IT is already rated for internal secondary protection, the standalone secondary protector is not required.

9.9.5.2 Recommendations

The selected level of secondary surge suppression rated voltage should be chosen to ensure selective coordination with the protected equipment.

When several secondary SPDs are installed at an equipment rack or cabinet, the SPDs should be placed at a central location within the rack or cabinet so they can be effectively bonded back to the equipment rack or cabinet rack ground bar or back to a separately installed rack ground bar.

9.9.6 Building ground (electrode) ring

9.9.6.1 Requirements

A building ground electrode ring shall be installed for facilities where a lightning protection system is installed or where there are multiple power service entrance locations along the periphery of the facility.

All below grade grounding connections shall be made by NRTL approved methods such as exothermic weld or high-compression connectors.

As required by local codes and standards the ground ring shall be bonded to building steel at every other column or more often. Concrete-encased electrodes (also known as Ufer electrodes) shall be used in new construction as a method of supplementing the grounding electrode system. Concrete-encased electrodes improve the effectiveness of the grounding electrode system due to concrete having hygroscopic properties and by providing a much larger surface area in direct contact with the surrounding soil:

- concrete-encased electrodes shall be encased by at least 51 mm (2 in) of concrete, located within and near the bottom of a concrete foundation or footing that is in direct contact with the earth;
- concrete-encased electrodes shall be at least 6 m (19.7 ft) of bare copper conductor not smaller than 25 mm² (4 AWG) or at least 6 m (19.7 ft) of one or more bare or zinc galvanized or other conductive coated steel reinforcing bars or rods at least 12.7 mm (0.5 in.) in diameter;
- concrete-encased electrodes shall be bonded to any other grounding electrode system at the site.

This building grounding system shall be directly bonded to all major power distribution equipment, including all switchgear, generators, UPS systems, and transformers, as well as to the telecommunications systems and lightning protection system. The facility shall possess a building electrical main ground bus (MGB), where all the large-load feeder facility grounds terminate. This is the location, coupled with the telecommunications main grounding busbar (TMGB), where the grounding system can be validated for both continuity and impedance.

9.9.6.2 Recommendations

A building ground electrode ring should be installed for all facilities. Single or triplex ground rod fields as the only earthing vehicle are not adequate for a critical facility. Generally, the direct burial connections should meet appropriate electrical testing requirements as set out in the applicable standards and codes to ensure durability. Designs may vary according to the site parameters such as available real estate, earth resistivity, frost line level, and the depth of the water table.

The placement of ground bus bars are recommended to facilitate bonding and visual inspection.

The ground ring should be 120 mm² (4/0 AWG) minimum bare copper wire buried a minimum .8 m (30 in) deep and a minimum 1 m (3 ft) from the building wall. For larger sizes stranded conductors are recommended. Ground rings encircling buildings should be installed just beyond the roof drip line. The size of the ground ring conductor is recommended to be the same as the largest size required by AHJ for a grounding electrode conductor to promote the accomplishment of intersystem bonding. Additionally, ground rods should be connected to the ground ring. Typical ground rods are 19 mm by 3 m (3/4 in by 10 ft) copper-clad steel ground rods spaced every 6 to 12 m (20 to 40 ft) along the perimeter ground loop.

Test wells for the building ground electrode ring should be provided at the four corners of the loop.

In its entirety, the common grounding electrode system should not exceed 5 ohms to true earth ground as measured by the fall of potential method (ANSI/IEEE Std 81). This reading is typically achievable in most locales, especially where the building is served by an ac power system with a multigrounded neutral (MGN). As noted in the NEC, IEEE Std 1100-2005, and IEEE Std 142-1991, common bonding of different systems plays a crucial role along with grounding. Some portions of the system may be allowed a higher resistance rating depending on the Class or location.

9.9.7 Supplementary bonding and grounding

9.9.7.1 Introduction

Supplementary bonding and grounding methods are those provided in addition to the bonding and grounding measures typically required by the applicable electrical safety codes and product safety standards. Supplementary bonding and grounding methods are intended to improve facility and equipment performance related to bonding and grounding. Examples of supplementary bonding and grounding entities may include metallic pathways, racks and trays; under the raised floor or above the cabinet/rack metallic grid work; metal plates and metal sheets; multiple bonding conductors from equipment to a grounding/bonding structure, etc.

9.9.7.2 Supplementary bonding and grounding structures

The data center grounding system is illustrated in Figure 39. It includes not only the power system ground but also supplementary bonding and grounding.

A supplementary bonding and grounding system commonly in the form of a mesh-bonding network (mesh-BN) equipped with a supplementary bonding grid (SBG, also historically known as a signal reference structure – SRS) is typically utilized in the data center. As noted in IEEE Std. 1100-2005, the default equipment bonding topology is the common bonding network (CBN) and the supplementary bonding grid can be readily utilized for efficient direct bonding of equipment and other apparatus to the grounding system. For the typical data center, the supplementary bonding grid becomes a component of the mesh-BN. The supplementary bonding grid is an externally installed network of conductors used to effectively bond together disparate metal cabinet and rack frames, enclosures. Such an arrangement provides efficient grounding and inter/intra-unit bonding of metal cabinets, racks and miscellaneous metal objects (especially when they are not powered). Additionally, the mesh-BN ensures grounding reliability of the equipment in the event the equipment grounding conductor of the serving power circuit is compromised or disconnected during maintenance. Electrostatic charge buildup and dissipation is also greatly aided by the multiple grounding paths of the mesh-BN (see Figure 39).

9.9.7.3 Mesh BN

9.9.7.3.1 Introduction

The supplementary bonding grid (SBG) may be a recommendation from or an actual part of the equipment manufacturer's installation package. Typically, it is part of an aftermarket, field-installed wiring effort.

The mesh-BN has three primary purposes:

- 1) First, it may enhance the reliability of signal transfer between interconnected items of equipment by reducing inter-unit common-mode electrical noise over a broad band of frequency. When properly designed, installed and utilized it can be effective for noise control across low-frequency single-ended signaling links or poorly designed communication links. This function is typically limited to around 30 MHz using flat strap for a 600 mm (24 in) grid spacing.
- 2) Second, it is intended to prevent damage to inter-unit signal circuits by providing a low impedance (low inductance) path and thus an effective ground reference for all externally installed ac and dc power, telecommunications, or other signal level, line-to-ground/chassis-connected SPD equipment that may be used with the associated equipment.
- 3) Finally, the mesh-BN is intended to prevent or minimize damage to inter-unit signal-level circuits and equipment power supplies when a power system ground-fault event occurs.

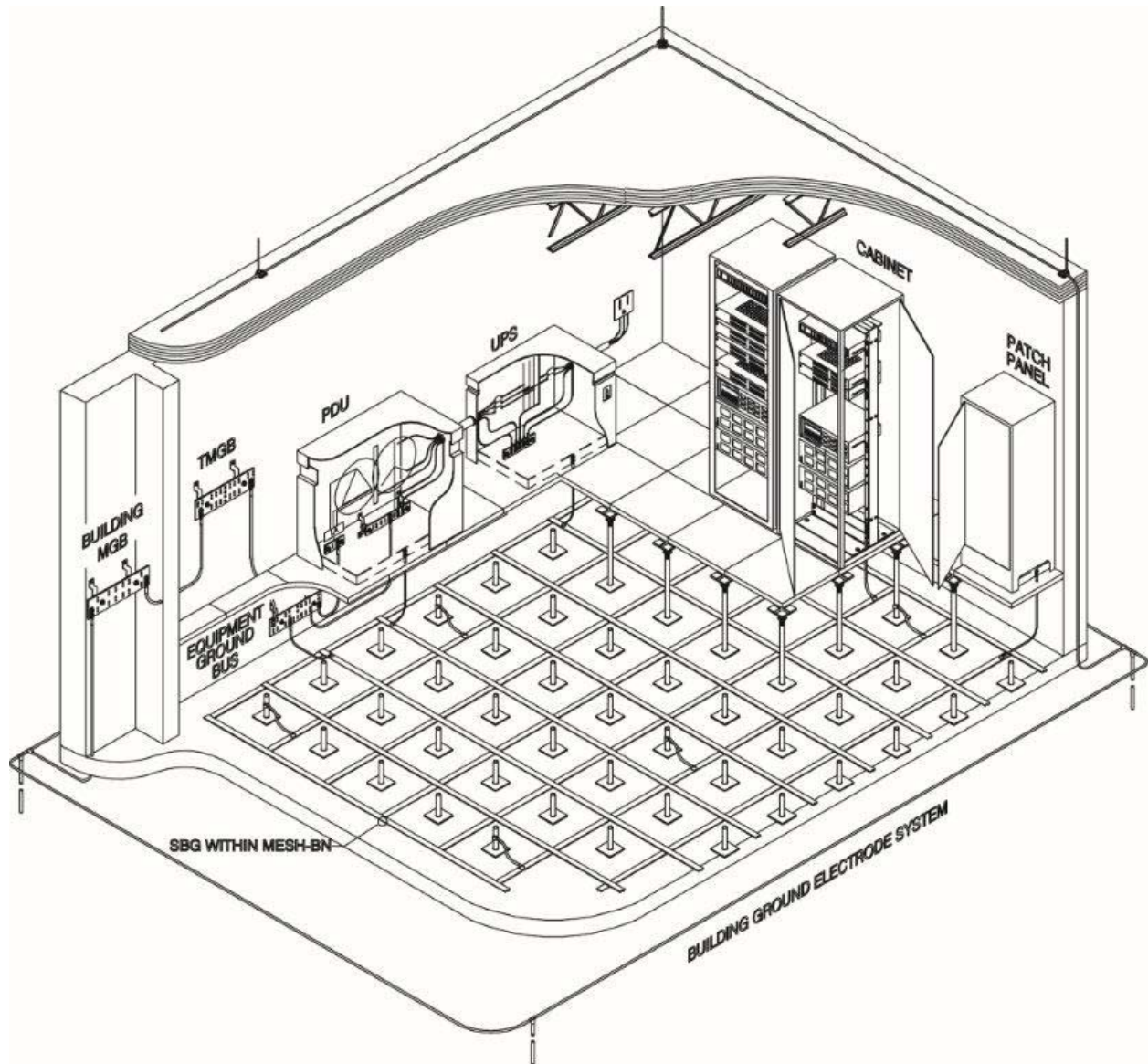


Figure 39: Data Center Grounding Schematic

The mesh-BN creates an equipotential ground reference for computer room and may reduce stray, high-frequency signals.

9.9.7.3.2 Requirements

The mesh-BN is an integral part of the CBN and it shall not be insulated or isolated from the building electrical system ground. Where utilized, the mesh-IBN (isolated bonding network) shall be insulated or isolated from the CBN except through a single point connection window. The mesh-IBN typically does not utilize an access floor or underfloor bonding grid as a supplementary bonding entity to the mesh-IBN. The reason is that the cabinet/racks are insulated/isolated from the flooring in order to accomplish the single point grounding scheme back to the single point connection window. Otherwise, the mesh-IBN intra-unit bonding is very similar to that used in a mesh-BN. The mesh-IBN is further described in IEEE 1100-2005. The mesh-IBN is not considered typical for a commercial data center installation but may be encountered in an access provider data center.

If ground clamps are used, they shall be listed for the intended application as a grounding clamp and not a wire hanger.

The mesh-BN may include a supplementary bonding grid in the form of a pre-fabricated or field assembled bare round wire or flat copper strip joined together via welding, brazing, compression or a suitable grounding clamp arrangement at each of the crossing points. The mesh-BN can also include field assembling a grid from the raised floor pedestals using standard or bare round wire.

If constructed using round conductors, the bonding grid shall be no smaller than 16 mm² (6 AWG) and up to 50 mm² (1 AWG) is typical. The conductors may be bare or insulated copper. If ground clamps are used, they shall be listed (e.g. UL 467) for the intended application as a grounding clamp and not a wire hanger or positioning device (e.g. UL 2239).

All metal surfaces, with the exception of lighting fixtures and door and window frames shall be bonded to the bonding grid, to include the building structure.

9.9.7.3.3 Recommendations

The mesh-BN should include a SBG such as a copper conductor grid on 600 mm to 3 m (24 in to 10 ft) centers that covers the entire computer room space. The ideal spacing for the grid is between 600 mm to 1.2 m (24 in to 4 ft). If the SBG is to provide enhanced reliability of signal transfer [as discussed in primary purpose 1) above see 9.9.7.3.1.1] by reducing inter-unit common-mode electrical noise over a broad band of frequency, the grid spacing must be kept at 600 mm (24 in) or less and the associated cabling must be routed in close proximity to the SBG if the declared bandwidth is to be realized.

The flat copper strip form of the supplementary bonding grid is typically installed with a prefabricated mesh. The grid should be prefabricated out of a minimum 0.40 mm (26 gauge) × 50 mm (2 in) wide copper strip with all crossing inter-connections welded, not punched (see Figure 40). The grid spacing of the mesh-BN should be 600 mm (24 in). Adjacent rolls of mesh-BN are exothermically welded in the field to form a continuous grid (see Figure 41). The copper strips are typically factory welded into a grid pattern prior to installation and then rolled out onto the floor in sections, with some minor exothermic welding performed on site prior to occupancy and IT operations commencing to complete the installation.

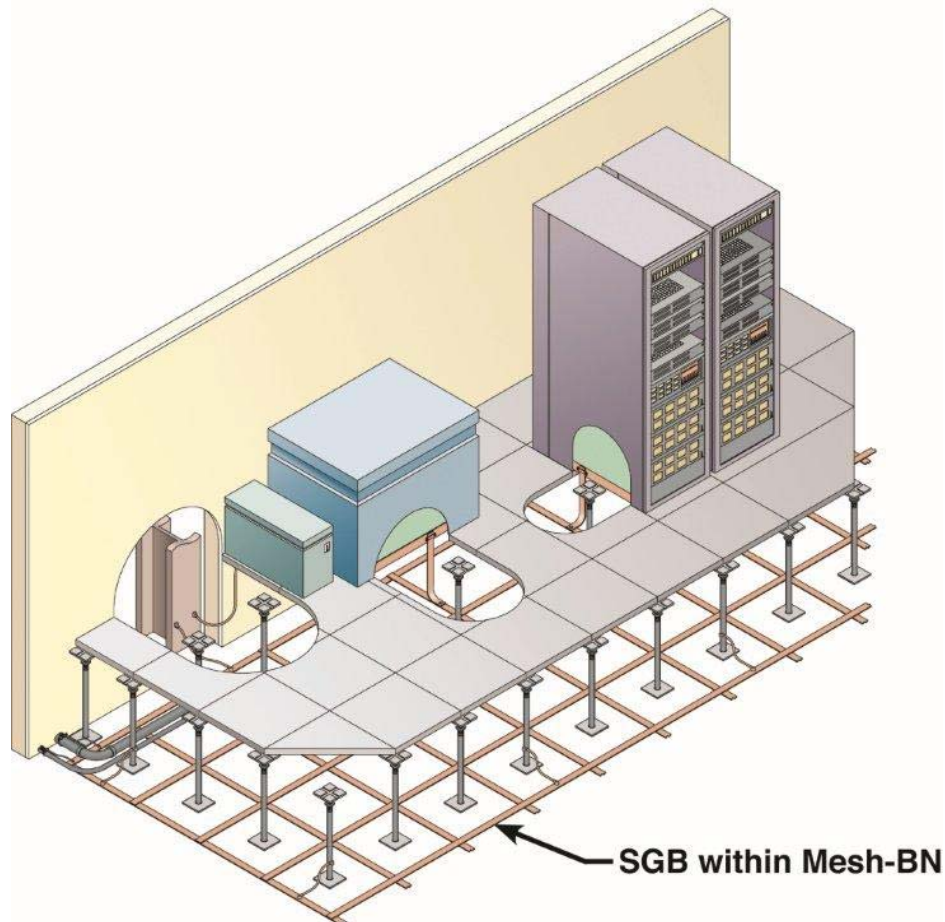


Figure 40: Typical Configuration Of Flat Strip-Type SBG Within A Mesh-BN

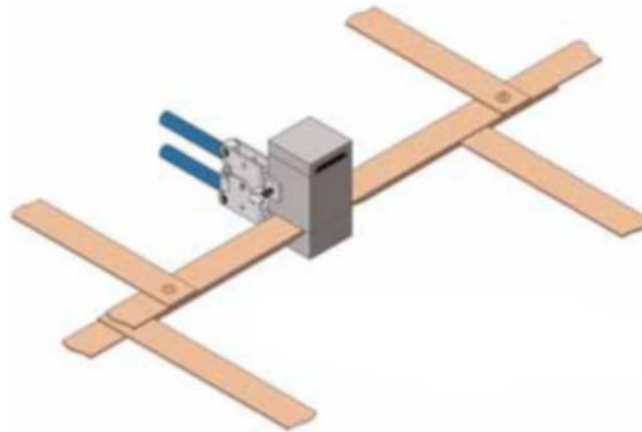


Figure 41: Adjacent Rolls Of Flat-Strip-Type SBG Being Exothermically-Welded Together

In all cases the SBG should be bonded to the pedestals of the raised floor system. If the grid is in the form of a flat strip grid (600 mm (24 in) spacing), at least every 6th pedestal should be bonded to the grid. If the grid is in the form of a fabricated bare round wire mat then at least every 3rd pedestals should be bonded to the grid. If the grid is formed from the raised floor pedestal system then at least every second pedestal should be bonded to the grid. The bonding jumper from the pedestal to the supplementary bonding grid should be no greater than 600 mm (24 in) in length. When using the access floor with bolted stringers as the supplementary bonding grid, note that it may not be as effective as a bonding grid that is built in place using copper conductors and exothermically welded joints or mechanical conductor clamps. Considerations include the removal of access floor tiles for temporary work, etc.

A SBG may be fabricated from standard, bare round wire or flat copper strip joined together via welding, brazing, compression or a suitable grounding clamp arrangement at each of the crossing points (see Figure 42). Due to the larger surface area, flat strap provides better transient protection especially at higher frequencies.

For a wire grid, bare (non-insulated) copper is preferred, because it provides greater ease of attachment of equipment to the mesh-BN. Since the immediate grid area is being rendered to the same potential, inadvertent or intermittent contact points should not be an issue if personal grounding systems are being used.

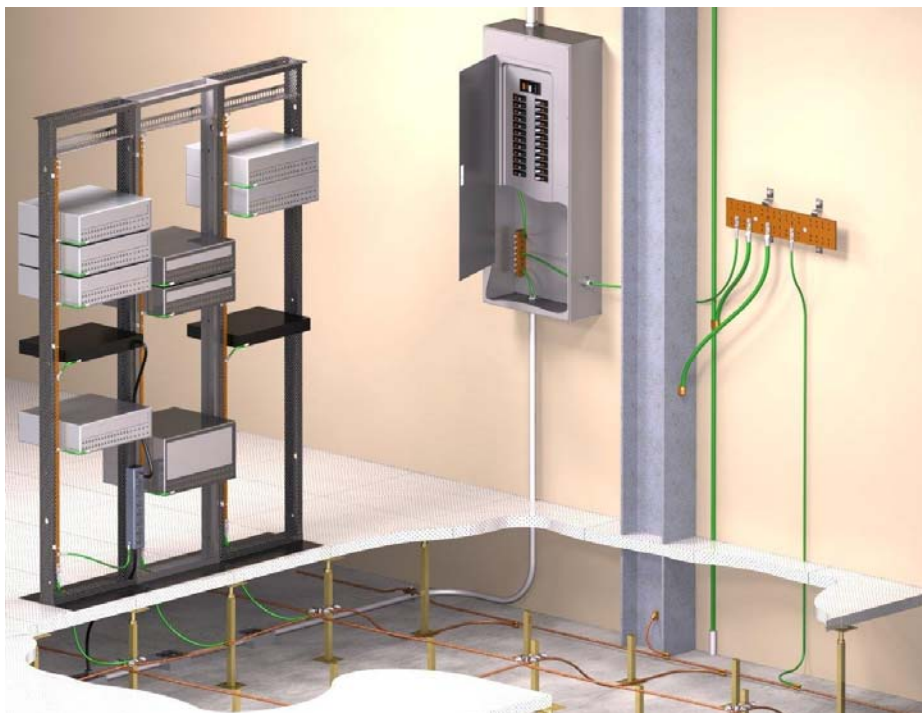


Figure 42: Data Center Grounding Infrastructure (Room Level) Example

The grounding and bonding infrastructure and ITE components should have the connections listed in Table 12.

Table 12: Grounding And Bonding Connection Schedule

<i>Connection</i>	<i>Minimum Conductor Size</i>	<i>Note No.</i>
TMGB – Building Main Ground Bus	130 mm ² (250 MCM) bare	
EGS – TMGB	130 mm ² (250 MCM) bare	
PDU – TMGB/TGB	Per applicable code (e.g., NEC 250-122)	
HVAC equipment— mesh-BN/SBG	16 mm ² (6 AWG) bare	
Steel column— mesh-BN/SBG	25 mm ² (4 AWG) bare	1 and 2
Rebar mat foundation— mesh-BN/SBG	25 mm ² (4 AWG) bare	3
Cable management—tray, conduit	16 mm ² (6 AWG) bare	4
Access floor pedestal—mesh-BN/SBG	16 mm ² (6 AWG) bare	5
Sprinkler piping— mesh-BN/SBG	16 mm ² (6 AWG) bare	
HVAC ductwork— mesh-BN/SBG	16 mm ² (6 AWG) bare	
Cabinets— mesh-BN/SBG	16 mm ² (6 AWG) bare	6
Equipment enclosures— mesh-BN/SBG	16 mm ² (6 AWG) bare	6
Frames— mesh-BN/SBG	16 mm ² (6 AWG) bare	6
Other metallic system enclosures— mesh-BN/SBG	16 mm ² (6 AWG) bare	

NOTES:

1. Size in excess of ANSI-J-STD-607 for the design of the telecommunications bonding and grounding infrastructure. Ground size should be this size or should match the ground conductor required at the electrical service entrance, whichever is larger.
2. Proper NRTL listed mechanical lugs and clamps, or exothermically welded connections to steel column.
3. Weld to rebar mat before pour.
4. Every joint should have a bonding jumper.
5. Utilize mechanical lugs, clamps, or exothermically welded connections on pedestal body and spade-type tab under stringer screw-down.
6. Cabinets, racks, frames, and equipment enclosures shall be individually bonded to the mesh-BN/SBG – not bonded serially.

9.9.7.4 Equipment bonding and grounding to the mesh-BN

9.9.7.4.1 Requirements

All non-current-carrying metallic enclosures shall be supplementary grounded and bonded, in addition to required safety grounding provided by the serving power circuit. This provides for both staff safety as well as grounding continuity, which is the logical extension of the data center grounding infrastructure to the load itself. Each equipment cabinet and equipment rack requires its own grounding connection within the mesh-BN. A minimum of a 16 mm² (6 AWG) insulated stranded copper conductor exothermically welded or mechanically terminated within the mesh-BN and mechanically terminated to the cabinet via a proper machine screw, through-bolt connection or factory-provided spot weld. Attach grounds at opposite ends of the series of racks, with the framework grounding conductor going directly to the data center grounding infrastructure.

Bare metal-to-bare metal contact is mandatory for all bonded connections, with anti-oxidant applied at the connection point of the equipment either in the field or by the factory prior to shipping the equipment.

The recommended method for all bonding is an insulated, stranded copper grounding wire, sized as recommended and with a spade terminal or compression lug being used for the wire termination. Each cabinet or rack shall have a suitable connection point (or points where multiple connections are desirable) to which the rack framework grounding conductor can be bonded.

Options for this connection point are:

- rack ground bus:
attach a dedicated copper ground bar or copper strip to the rack. A bond between the ground bar or strip and the rack shall exist. The mounting screws shall be of the thread-forming type, not self-tapping or sheet metal screws. Thread-forming screws create threads by the displacement of metal without creating chips or curls, which could damage adjacent equipment.
- direct connection to the rack:
if dedicated copper ground bars or strips and associated thread-forming/self-tapping screws are not used, then paint shall be removed from the rack at the connection point, and the surface shall be brought to a shiny gloss for proper bonding using an approved antioxidant.
- bonding to the rack:
when bonding the rack framework grounding conductor to the connection point on the cabinet or rack, it is desirable to use two-hole lugs. The use of two-hole lugs helps to insure that the ground connection does not become loose due to excessive vibration or movement of the attaching cable.

9.9.7.5 Rack connections to the mesh-BN

Racks and cabinets shall be individually bonded to the computer room grounding system.

Every structural member of the cabinet or rack shall be grounded.

9.9.8 Information technology equipment (ITE) interconnections

9.9.8.1 Introduction

An integral part of the bonding and grounding network in the access floor area or any critical environment is the grounding of the IT support equipment and static discharge management during ongoing operations. This includes the connection of a cabinet of ITE chassis to the mesh-BN, connections between various IT systems and cabinets and personal grounding checks and static charge dissipation.

9.9.8.2 Rack connections to the mesh-BN

It is common for cabinets to be physically connected for structural integrity, and they also may be logically, virtually or network connected, acting as an integral platform.

This is achieved by the manufacturer assembling the cabinet or rack in such a way that there is electrical continuity throughout its structural members. For welded racks, the welded construction serves as the method of bonding the structural members of the rack together.

All adjacent cabinets and systems should be bonded in order to form grounding continuity throughout the rack structure itself.

Electrical continuity cannot be assumed using nut and bolt connections used to build or stabilize equipment racks and cabinets. Bolts, nuts and screws used for rack assembly may not be specifically designed for grounding purposes, and unless grounding bonding jumpers are installed, do not assume electrical continuity for the cabinet lineup. Further, most racks and cabinets are painted, and since paint is nonconductive of electrical current, paint insulates. This negates any attempt to accomplish desired grounding. Therefore, paint or cabinet coating has to be removed in the bonding area for a proper bond to be formed.

Most power is routed over the top or bottom of the rack. Without a reliable bond of all four sides of the rack, a safety hazard in case of contact with live feeds exists.

9.9.8.3 Information technology equipment (ITE) bonding to the cabinet or mesh-BN

9.9.8.3.1 Requirements

The ITE chassis shall be bonded to the rack using one of the following methods:

- manufacturer-provided grounding location:
Ideally, the manufacturer will supply a separate grounding hole or stud. This hole or stud shall serve as the primary grounding site for the IT chassis, and shall be used with a conductor of proper size to handle any fault currents up to the limit of the circuit protection device feeding power to the equipment unit. Each end of this chassis grounding conductor will be bonded to the chassis hole or stud, and the other end will be properly bonded to the copper ground bar or strip. In some instances, it may be preferable to bypass the copper ground bar or strip and bond the chassis grounding conductor directly to the data center grounding infrastructure.

- grounding via the mounting system:

If the equipment manufacturer suggests grounding via the chassis mounting flanges and the mounting flanges are not painted, the use of thread-forming screws and normal washers will provide an acceptable bond to the rack.

If the equipment mounting flanges are painted, the paint can be removed, or the use of the same thread-forming screws and aggressive paint-piercing lock washers, designed for this application, will supply an acceptable bond to safety ground through the rack.

- grounding via the power cord:

Grounding through the equipment ac (alternating current) power cord does not meet the intent of this section where the power path and the equipment path offer redundant and specific ground paths for the IT loads. While the ac-powered equipment typically has a power cord that contains a ground wire, the integrity of this path to ground cannot be easily verified. Rather than relying solely on the ac power cord ground wire, it is desirable that equipment be grounded in a verifiable manner such as the methods described in this section.

9.9.8.3.2 Recommendations

Once the racks or cabinets are grounded, the equipment installed with the rack or cabinet needs to be rendered to the mesh-BN ground reference as well. Some of this has been undertaken by equipment manufacturer's for enterprise-level or factory-configured systems. For field-assembled rack-mounted systems, equipment grounding must be added to complete the ITE-to-mesh-BN grounding connection via the cabinet chassis.

Rack-mounted equipment should be bonded and grounded via the chassis, if available, in accordance with the manufacturer's instructions, if the rack is bonded and grounded properly.

9.9.8.4 Personal grounding and static discharge

Electrostatic discharge (ESD) is the spontaneous transfer of electrostatic charge. The charge flows through spark (static discharge) between two bodies at different electrostatic potentials as they approach each other.

CAUTION: Electrostatic discharge (ESD) may cause permanent damage or intermittent malfunction of networking hardware. Anyone that touches network equipment or network cabling becomes a potential source of ESD as it relates to telecommunications equipment. Network cabling that has been installed but not connected may become charged when these cables are un-spooled and slid over carpet or other surface that contributes to the buildup of ESD. The charged cabling may become a source of ESD to the telecommunications equipment to which it connects. Charged cabling should be discharged to an earth ground prior to connection to network equipment. ESD charges may remain for some time, especially in dry conditions.

Factors affecting ESD charge retention include:

- cable design;
- dielectric materials;
- humidity;
- installation practices.

Low humidity and static-generating building materials are the primary cause of ESD. There should be no significant ESD charge retention difference between categories or types of cabling. All cables have a nearly identical ability to acquire a static charge. See Section 14.5 for additional information about the categories/classes of cabling.

It is important to follow all ESD guidelines provided by the applicable network equipment manufacturer's specifications and guidelines. Mitigation techniques, such as anti-static flooring and humidity control, are important for critical installations.

The use of static discharge wrist straps when working on or installing network or computer hardware is specified in most manufacturers' installation guidelines. Wrist strap ports should be attached to the rack by a means that ensures electrical continuity to ground. Pedestrian static discharge mats and show strapping may be required for certain access floor environments or spaces with standard resistance flooring.

9.9.9 Power system bonding and grounding

9.9.9.1 Introduction

In the past, 4-wire systems were normal in critical facilities, mimicking the X-O bonding and services in traditional commercial spaces. This led to some substantial problems caused by ITE loads producing harmonics that were able to readily propagate through the power system. These harmonics caused problems such as large-scale and objectionable ground currents (often in the hundred of amps), the failure of small X-O bonds on branch circuiting, and ITE disruption and failure. Nuisance tripping of ground fault elements was also experienced.

The designer is faced with the question of what purpose the neutral serves in the 480/277 VAC and 208/120 VAC system. Only lighting and small-scale loads are served by the 480/277 VAC and 208/120 VAC neutral (when compared to the critical facilities overall load).

Without some form of isolation for these noncritical 480/277 VAC and 208/120 VAC neutrals, the incoming 480 service would be forced to generate a neutral at the highest point in the low-voltage electrical system to serve this minority of loads. This allows harmonics to propagate across several systems, because they are being connected to a 4 W switchboard or system. The balance of the loads in the facility are essentially 3 W, since there is no need for X-O bonds or separately-derived system for the 3 phase, 3 wire mechanical system or for the rectifier side of the UPS system. Some form of separately-derived system or X-O bond is required for these small 480/277 VAC and 208/120 VAC loads. However, because generating a fourth wire for those systems and their X-O bond presents an issue for most of the electrical system, an isolation transformer for the small 480/277 VAC loads is desirable.

Seeing that now isolating these loads is a positive design element and that an isolation transformer will be provided for the small 480/277 VAC loads, 3-wire feeds then become the standard for the balance of the loads in facility. This indicates that the X-O bond for the 208/120 VAC loads within the critical environments and below the inverters of the UPS systems are below the UPS on the load side of those systems.

All loads in the critical environment will be provided with dedicated and express insulated ground wires from the load to the derived ground point at the PDU.

9.9.9.2 Bonding and grounding—ac and dc powered telecommunication systems

IEEE 1100 integrates many of the traditional telecommunications recommendations and discusses how to integrate the ac and dc power systems to accomplish the important safety and performance objectives of each. The key concepts related to bonding and grounding deal with both the serving power system and the ITE. The serving power system is grounded to the building's grounding electrode system. The grounding electrode system is connected to the common bonding network within the building (see Figure 43). For ITE, IEEE 1100 refers to multipoint connections as the common bonding network and a single point of connection as an isolated (insulated) bonding network.

Much of the guidance on bonding and grounding dc power systems for telecommunications and ITE is rooted in the traditional telephone (telecommunications) utility (regulated) industry. The basis of this guidance is supported in IEEE Std. 1100-2005 for the commercial (deregulated) industry—with some modifications made to meet requirements of the commercial market segment.

A significant observation is that historically telecommunications is dc powered and historically ITE is ac powered. Therefore, the bonding and grounding standards for these different types of power systems is historically different due to the dc being predominantly utilized in a regulated environment considered “under the exclusive control of the utility” (NFPA 70).

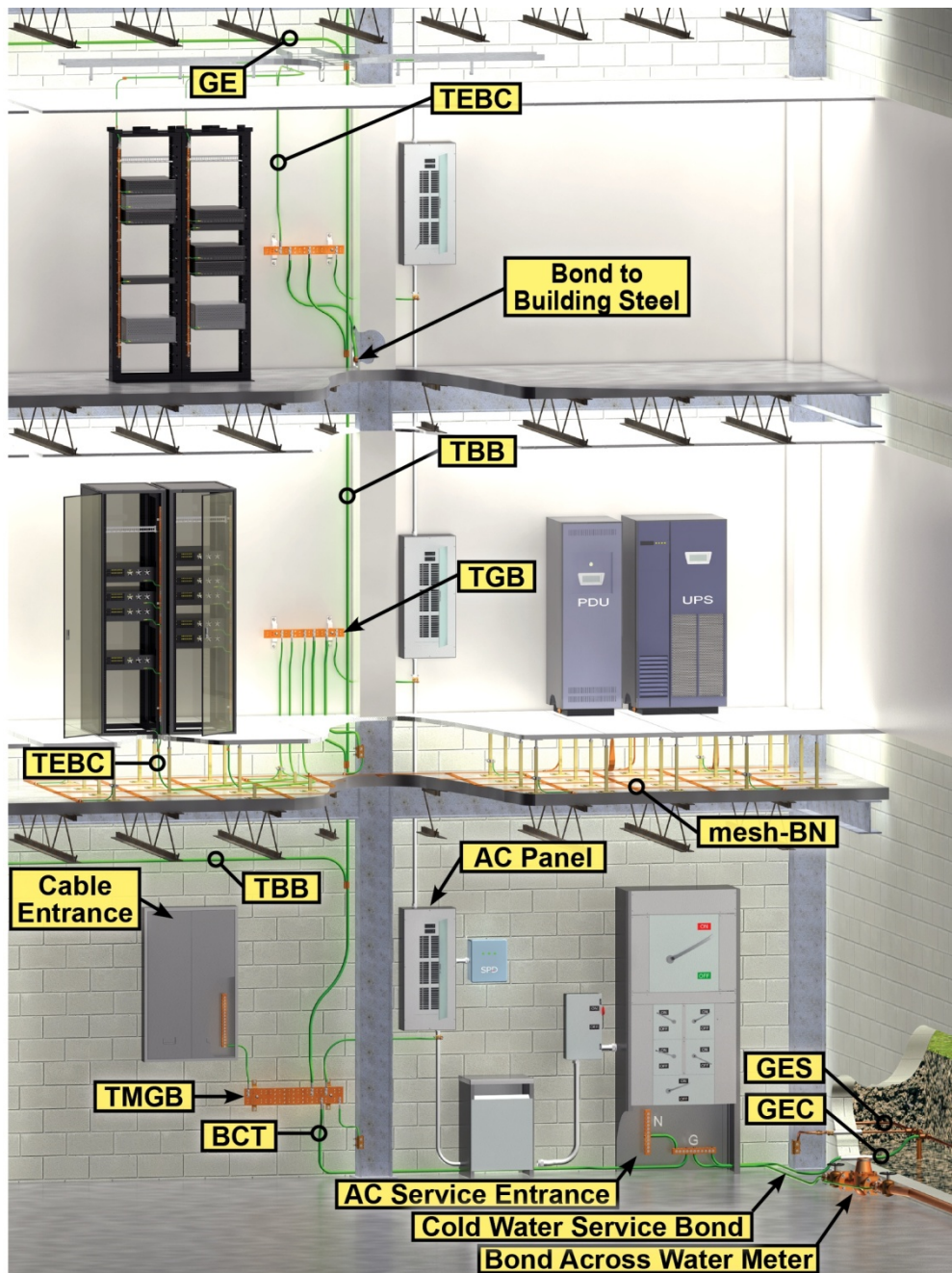
DC power system operating voltages are affected by several factors such as:

- battery technology (vented or valve-regulated);
- rectifier output regulation in maintaining constant voltage under dynamic loads;
- voltage drops in dc power conductors;
- operating voltage limits of various connected loads;
- derating for environmental conditions such as altitude.

For the data center, a telecommunications bonding and grounding infrastructure in accordance with ANSI/TIA-942, ANSI-J-STD-607-A, and IEEE Std. 1100-2005 is expected. This infrastructure is bonded to the electrical power grounding electrode system, to building steel (where accessible) and to the serving ac power panel equipment ground at each floor. Grounding needed for the data center equipment(s) is obtained from the expected ground bar on that floor (such as a telecommunications ground bar [TGB]). See Figure 43. Note that this bonding and grounding infrastructure is not the same physical structure as the grounding infrastructure that might be placed for the electrical power system.

In no situation should a totally separate grounding system be deployed because this may lead to safety and performance problems.

Noise concerns for the data center equipment do involve common mode noise generated and distributed by the power system to the electronic load equipment. Generally, the equipment ac input power supplies are quite tolerant of common mode noise. It should also be expected the server and other manufacturers will design and test equipment's (higher voltage) dc input power supplies to be similarly robust. This is already accomplished for 48 VDC telecommunications equipment meeting the requirements of Telcordia GR-1089-CORE-2006 and placed into a common bonding network (CBN).



Legend	
BCT	Bonding Conductor for Telecommunications
GE	Grounding Equalizer
GEC	Grounding Electrode Conductor
GES	Grounding Electrode System
TBB	Telecommunications Bonding Backbone
TEBC	Telecommunications Equipment Bonding Conductor
TGB	Telecommunications Grounding Busbar
TMGB	Telecommunications Main Grounding Busbar

Figure 43: Telecommunications Bonding And Grounding Infrastructure

9.9.9.3 Bonding and grounding—telecommunications dc systems

Generally, telecommunications dc power systems date back to the first telephone systems where dc was used for talk battery, signaling circuits and for operating switching and control relays. Centralized (bulk) dc power plants (systems) had primary components such as rectifiers, a powerboard, primary and secondary distribution feeders, and fuse bays. The dc power system was grounded to earth (often more than once). The grounded conductor was termed the return. The connected load equipment was called telecommunications load equipment (TLE) (hereafter referred to as ITE).

Modern dc power systems are more compact, use much smaller footprint components, and are more efficient. Today, a small centralized dc power system can be contained in a single rack. For standards compliance purposes, this equipment is generally classified as ITE. For the purposes of evaluating dc powered ITE, robustness of the system is a key consideration. Accordingly, certain questions arise regarding grounding, bonding and protection of the installation. Example questions include:

- Is the ITE suitably robust (per Telcordia GR-1089-2006) to operate in a Common Bonding Network (CBN);
- Is the ITE not suitably robust (per Telcordia GR-1089-2006) and must therefore be operated in an Isolated Bonding Network (IBN) (NOTE: The significant role of the IBN topology is to isolate the ITE from currents flowing through the CBN, especially lightning);
- Is the dc power supply dedicated to a single type of equipment bonding network (CBN or IBN) or is it to be a shared resource;
- Where is the planned location for the dc power supply relative to the location of the ITE;
- Is any of the ITE required to integrate the return and dc equipment grounding conductor (DCEG) at the dc power input?

Availability requirements for ITE in a data center may not need to be specified to all of the points required for a telecommunications service provider (TSP), such as at a telecommunications central office. The availability specification will determine if an IBN may be appropriate for the data center or a portion of the data center.

Generally, the modern centralized dc power system is designed to operate as a single-point grounded system. An equipment-grounding (bonding) conductor is installed as part of the distribution circuit to ground any metal parts of the ITE and to clear any ground faults by facilitating the timely operation of the upstream overcurrent protection device. The system grounding (electrode) conductor is termed the DCG and is connected to the Return near the dc power source. The return is only grounded once. This arrangement is extremely similar to bonding and grounding an ac power system per NFPA 70-2005 - with some possible variations allowed by UL60950. See Figures 44 to 48.

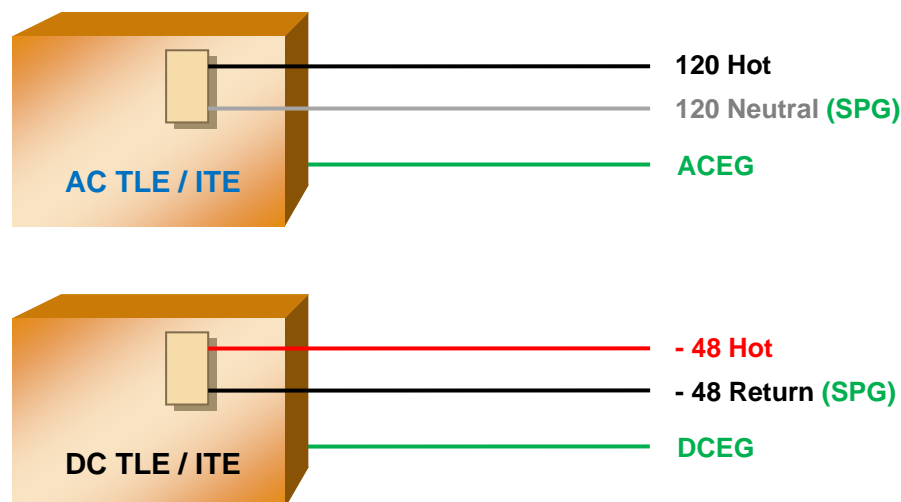


Figure 44: Similarity Of Recommended Grounding For ac And cc Power Systems And Load Equipment

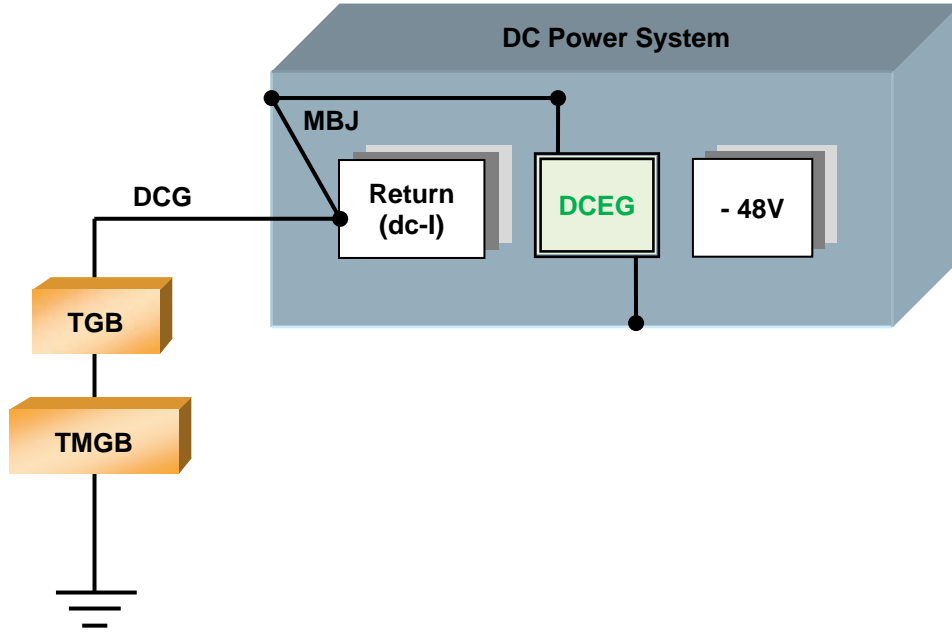


Figure 45: dc Power System Showing Single-Point Grounded Return

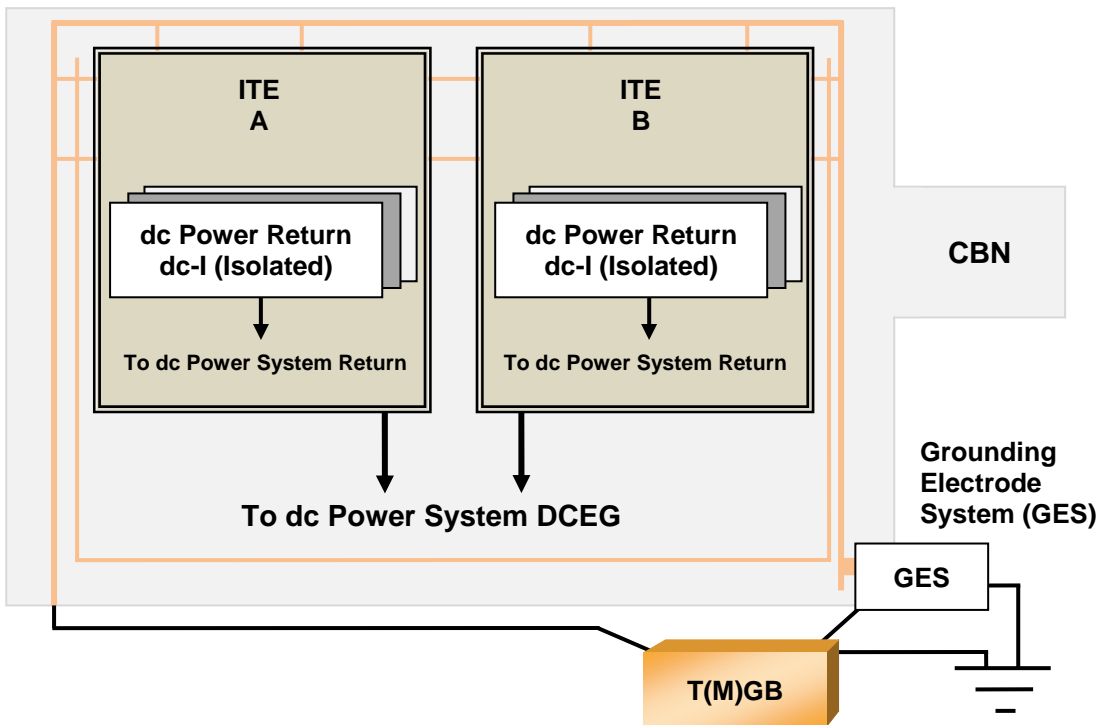


Figure 46: Information Technology Equipment Showing Grounding Of dc Power Input (Return Is Insulated)

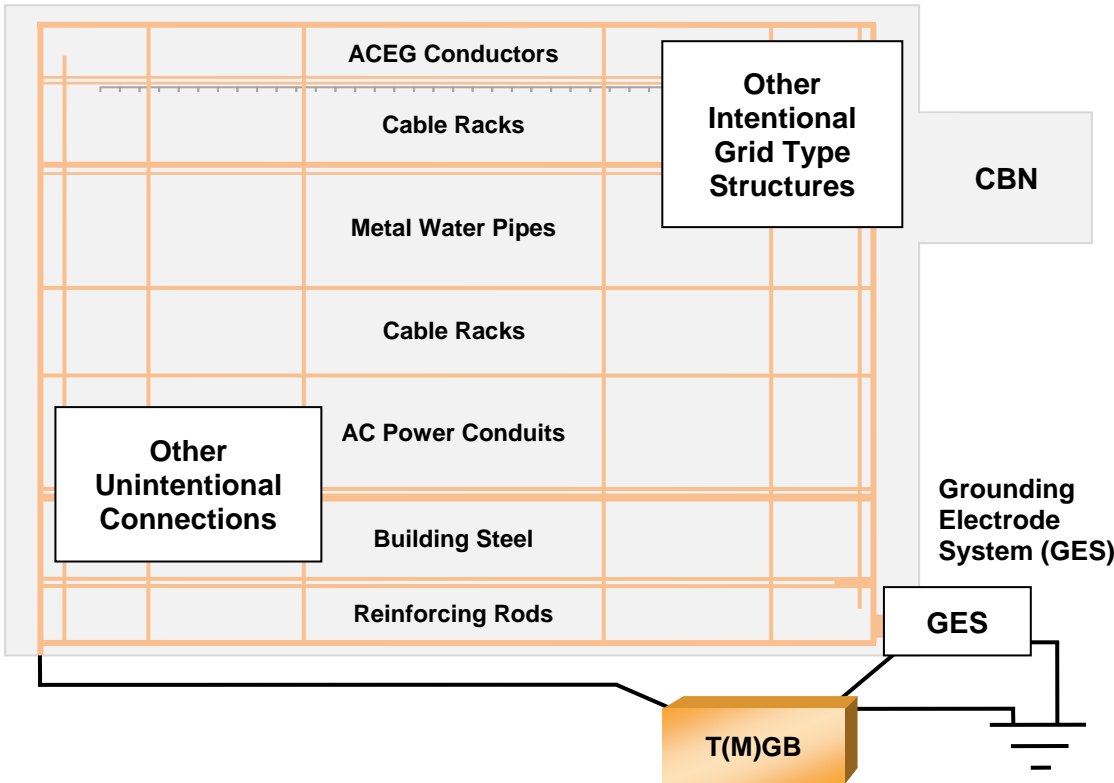


Figure 47: Common Bonding Network

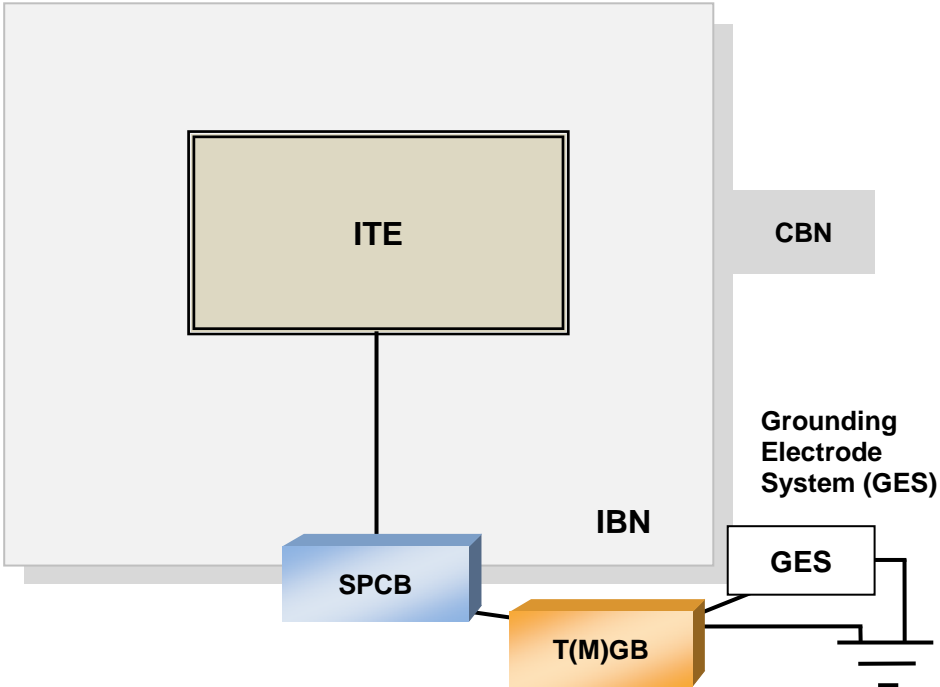


Figure 48: Isolated (Insulated) Bonding Network

Porting the dc power system telecommunications utility practices to the nonregulated environment requires additional considerations. These considerations include:

- The highest dc voltage covered by the telephone/telecommunications/ITE industry is 160 (ATIS 0600336). The utilization of higher dc voltages is essentially new territory and will require some additional safety and performance investigation. However, established principals are not expected to change.
- Overcurrent protection devices (OPD) and disconnect devices for dc power systems will need further investigation for higher voltage dc systems. ac rated devices do not automatically port over to the dc power system at the same rated voltage and current. The established 2:1 protection coordination scheme for dc fuses is not readily applicable since data centers typically utilize circuit breaker technology.
- Transients for other than 48 V dc systems are not well described, if at all.
- Battery disconnects (where batteries are used as standby resource)—are they required; which to use, 1 pole or 2 poles; what are their withstand and interrupt ratings.
- Conductor sizing is not a complete match to the specifications for ac conductors from NFPA 70-2005.
- The rectifier technology is assumed to be switched mode power supply (SMPS), which may involve noise control via power line filters (possibly connected to the return or dc equipment ground conductor) and additional audible noise from cooling fans.
- Rectifier operation modes at the higher voltages such as 380 V dc may need verification for ac input power factor correction, load sharing, paralleling, voltage sensing, and current limitation.
- The dc power distribution topology is historically bus or cabling. Further, there may also be a need for an underfloor topology. Distribution (such as rigid busbar) withstand under extreme fault current conditions [such as a direct short across the batteries (if batteries are used)] will likely vary considerably from that for a telecommunications 48 VDC system.
- What should be the design parameter for voltage drop from standby resource (such as a battery plant) to the load equipment; for telecommunications, the parameter is typically 1 V per 24 V of the supply; 48 V supply equals 2 V drop, so, does 380 V supply equal 16 V drop.
- For a 380 VDC battery plant, consider the size of the battery rack (if metallic) bonding conductor; for telecommunications, 16 mm² (6 AWG) is typically specified and should be verified with the AHJ; is this still suitable for such a much larger battery plant.
- Centralized dc power systems are restrained to use in a restricted access area (RAA) by UL 60950 (NOTE: A data center is considered a RAA.).
- The previous three bullets reflect telephone company practices accommodated by first UL 1459 and then UL 60950.
- Should the 380 VDC system be operated as a positive grounded system (similar to the 48 VDC telecommunications system) or should it be operated as a negative grounded system (similar to the 24 VDC telecommunications system).
- The location of attachment of the dc system grounding electrode conductor (DCG) to the centralized dc power system is allowed to occur forward from the source toward the telecommunications load equipment per UL60950.
- The dc power system equipment grounding conductor (DCEG) is allowed to be routed separate from the dc supply and Return circuit conductors per UL 60950.
- The DCEG is permitted to be bonded to the Return at the load equipment per UL 60950.
- Based upon these considerations, the prudent approach is to utilize IEEE Std. 1100-2005 as the base document for bonding and grounding the dc power system in a data center:
 - essentially mirrors topology for an ac power system;
 - single-point grounding of the dc power system at the source location;
 - a co-routed dc equipment grounding conductor with the circuit wiring (supply such as –48 V return);
 - bonding of dc equipment grounding conductor to the “Return” at the load equipment is prohibited;
 - fully controlled paths for direct current.

9.9.9.4 Bonding and grounding—higher voltage dc systems (above 160 VDC)

As noted previously, higher voltage dc power systems for a data center are still under research and development. This standard does not offer any further guidance.

9.10 Labeling and signage

9.10.1 Introduction

Labeling and signage falls into several categories:

- building information, such as room names and numbers;
- hazard and safety, such as chemical and shock hazard signage, exit signs, wet or open floor rope-offs, material safety data sheet locations, EPO signage and warning signs for personnel, operation or safety;
- indicating signage, such as equipment labeling and the color-coding of systems;
- informational, such as routine and exceptional informational posting on bulletin boards.

9.10.2 Requirements

Systems and labeling shall be color coded according to ANSI or IEEE standards, subject to approval by the Authority Having Jurisdiction (AHJ).

Labeling shall be integrated to the individual systems and shall offer the operator as clear a picture of system status under cursory examination. Labeling works hand in hand with the graphical user interface (GUI) and the physical organization of the equipment and systems themselves.

The GUI is typically a visual dashboard for the complete operation of the system. Information that the GUI typically includes are a color-coded power flow diagram, electrical performance, electrical characteristics, and alarm status.

Equipment itself may bear mimic busing, indicating how power flows through the system and how the individual breaks are connected. It may also be color-coded for the critical, utility, and generator power systems. For example, a critical power system with four, distinct UPS systems could be labeled UPS-A, UPS-B, UPS-C and UPS-D. Such a system could bear a unique color-coding where the A system might be red, the B system might be blue, the C system might be green, and the D system might be yellow. This color-coding would be carried all the way through the system.

All branch and data center circuits shall be marked with their individual circuit designations. Conduit systems and junction boxes shall also be color-coded by system, and power feeders may also bear their specific designation (e.g., UPS A Input). Conduit color-coding may be via a label, cladding or painting.

9.10.3 Recommendations

Circuits that are on the output of a UPS or that support critical loads should be color-coded to readily distinguish them from non-critical circuits. This color-coding may be in the form of colored self-adhesive labels or nameplates.

Equipment labeling should possess all critical information concerning the system to which it is affixed. This information should include:

- Equipment nomenclature and designation (e.g., Generator AH54).
- System capacity rating in kVA and kW (e.g., 750 kVA/675 kW).
- Input voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire).
- Output voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire).
- Power factor (e.g., 0.9 lagging).
- System or switchboard serving this piece of equipment.
- System, switchboard, or load that is being served by this equipment.

9.10.3.1 Arc flash labels

A Class F3 or Class F4 data center can be designed to allow concurrent maintenance so that work should never be required on energized equipment. However, such architecture may be prohibitively expensive or inappropriate for the application. So-called “hot work” is not a best practice and should be avoided whenever possible, but in a 24/7 data center operation scheduled down time may not be available on demand. Work on energized equipment might be authorized or required.

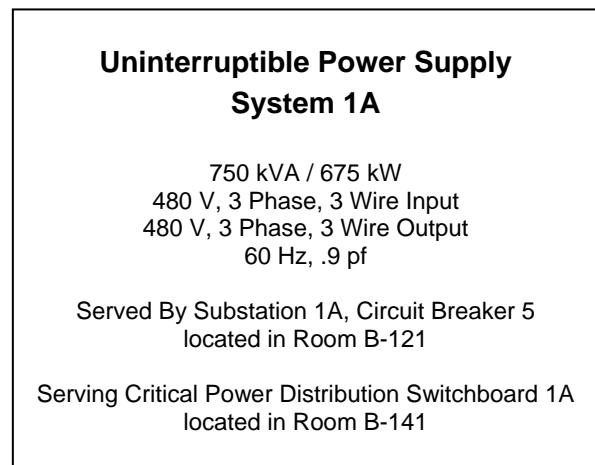


Figure 49: Sample Equipment Nameplate

Labeling should conform to requirements of local codes, but typical minimum requirements identify:

- voltage;
- fault current;
- flash and shock boundaries;
- incident energy levels;
- recommended minimum levels of personnel protective equipment (PPE).

Figure 50 shows one example of an arc flash label.

9.11 Testing and quality assurance

9.11.1 Recommendations

Testing and design/construction quality assurance are vital to validate that the design and installation will operate as intended. While this may appear to be a daunting task, by approaching this process as a sequential, reinforcing, non-redundant set of activities, it can present a logical and direct solution to systems validation needs.

For electrical systems and the sheer complexity and safety required to operate these systems, there are two fundamental camps – basic electrical construction quality control and system functional testing. The electrical quality control considerations include feeder continuity testing, basic switchgear testing, feeder landing/torque testing, labeling, over current short circuit validation, trip settings per the coordination study, and safety signage such as arc flash indication. Basic system startup, assisted by the manufacturer’s representatives, is also included in this group of activities.

The system functional testing assumes that the basic field quality controls will render a complete, safe and functional system pursuant to the design and specifications. Testing steps assume that the installation has fully met the requirements of a specific testing level prior to proceeding to the next phase of testing. All functional testing will examine normal, failure and maintenance modes of operation. Without being redundant to Section 16.4, functional testing follows this basic sequence:

- 1) Level 1 Commissioning - Equipment subject to in-factory testing and certification prior to delivery to the project location.
- 2) Level 2 Commissioning - Equipment installation has been completed and start-up activities are satisfactorily completed by the factory technicians.
- 3) Level 3 Commissioning - Component-level testing. Individual electrical system components, like a single generator or UPS power modules are tested. This commissioning step would precede the assembled parallel or complete electrical system testing.
- 4) Level 4 Commissioning – Electrical System Functional Testing. This system-level testing, where paralleled or cooperating systems like multiple generators or UPS power modules are tested together as a single unit. This commissioning step would be for electrical systems under a single control system or activity and would precede the complete electrical system testing.
- 5) Level 4 Commissioning – Electrical System Operational Testing. The completed electrical system is tested as a complete and interconnected utility. Unlike Level 4 Commissioning – Electrical System Functional Testing, this phase of testing examines the entire electrical system to verify the interaction of the varying electrical subsystems and to assure the electrical system works as a single, coordinated entity. This commissioning step would precede the complete building system testing in Level 5.
- 6) Level 5 Commissioning – Whole Building Testing. Subsequent to the successful functional and operational testing of both the individual or complete electrical and mechanical systems, the entire building’s utility infrastructure is examined as a complete system. The goal of this is to validate that the all building utility systems are operating as intended and ,to verify the proper and expected interactions of those systems, and to assure they work as a single, coordinated entity. The building is subjected to the design maximum loads for electrical supply and mechanical cooling/heating. Like previous steps, normal, failure and maintenance modes of operations are demonstrated. Load response and profiles are typically developed during this phase of the work.

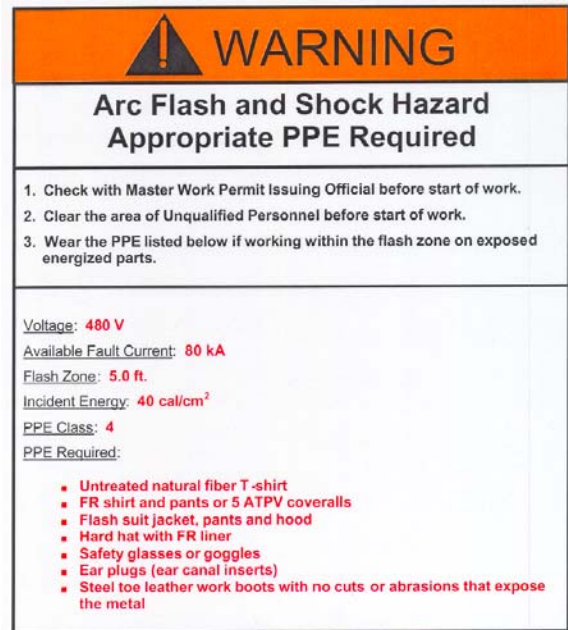


Figure 50: Arc Flash Warning Label

- 7) The interdisciplinary testing of all utility systems to examine how the mechanical system responds to a change of state in the electrical system.

Level 4 Commissioning should include training and participation of all personnel who will be responsible for any activities during any change of state in the facility power and mechanical systems. For the specific recommendations and process for facility testing and quality assurance, please see Section 16: Commissioning.

9.12 Ongoing operations

9.12.1 Recommendations

Facility and maintenance operations are an integral part of any critical facility. Human error is the leading factor in outages and errors related to MTBF, and these errors also bear upon MTTR, the crux of availability. There are recognized best practice management frameworks which cover these in detail, but the following are some high-level recommendations:

- all work should be scripted and specific to the activity being undertaken;
- IT and facility operations should work collaboratively regardless of Class or business;
- planned activities should include preventive and programmable maintenance, repair and replacement of components, addition or removal of capacity components, and testing of components and systems;
- “hot work” (on energized equipment) should be eliminated whenever possible. Where hot work is unavoidable, personnel should be trained, certified, authorized, and provided appropriate personal protective equipment.

9.13 Electrical systems matrix

Table 13 provides a summary of Section 9: Electrical Systems, with the items in the table presented in sequential order. Additional information has also been placed in the table that was not necessarily presented nor explained in the preceding text. Readers are cautioned that some of the additions are to be considered as requirements, and that Table 13 is to be used in conjunction with the text of Section 9.

Table 13: Electrical Systems Availability Classes

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
<i>9.1 (Electrical systems) Overview</i>					
Common industry description	Single path without any one of the following: alternate power source; UPS; proper IT grounding.	Single path	Redundant component/single path	Concurrently maintainable and operable	Fault tolerant
Number of power delivery paths to the critical load	One	One	One	Two, one active and one passive or non-UPS power	Two or more active
Redundant system components (e.g., UPS and generators)	No	No	Yes	Yes	Yes
Distinct UPS sources (e.g., A and B)	Optional / may not be present	Single or N	Single or N	Single or more, depending on the critical power load	At least two resulting in a minimum of $N + 2$
System allows concurrent maintenance and operations	No	No	Within some systems with paralleled components, but not consistent throughout the electrical system.	Yes	Yes
System allows fault tolerance and self-heals failures?	No	No	No	Possible, depending on system configuration	Yes
Redundancy loss during maintenance or failure?	Yes. Redundancy is zero, so load loss or systems interruption would be expected.	Yes. Redundancy is zero, so load loss or systems interruption would be expected.	Yes for the power paths. Redundancy may exist in paralleled systems and system topology may prevent load loss or interruption during routine maintenance or expected failures.	Yes, but the redundancy level reduced to N during maintenance or after a failure	No, but the redundancy level reduced to a level of $>N$ during maintenance or after a failure.
Computer and telecommunications equipment power cords	Single- or dual-cord fed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single- or dual-cord fed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single- or dual-cord fed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single-, dual- or poly-cord Feed with either 100% capacity on each cord or adequate capacity on each cord mapped to the individual IT system should a given source fail (i.e. 5 to make 6 or 2 to make 3 inputs).	Single-, dual- or poly-cord Feed with either 100% capacity on each cord or adequate capacity on each cord mapped to the individual IT system should a given source fail (i.e. 5 to make 6 or 2 to make 3 inputs).
Ability to add systems or components without interruption to existing loads	No	No	No	If planned during the initial design	Yes
Single points of failure	One or more	One or more	One or more	None	None

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
UPS redundancy	N or <N	N	A minimum of N + 1	A minimum of N + 1	Multiple N, 2N, 2N + 1 or any configuration greater than N + 1 that does not compromise redundancy during failure or maintenance modes of operation
UPS topology	Single module or parallel non-redundant system	Single module or parallel non-redundant modules	Parallel redundant modules or distributed redundant modules	Parallel redundant or distributed redundant or isolated redundant system	Parallel redundant or distributed redundant or isolated redundant system
Labeling	Recommended	Recommended	Recommended	Recommended	Recommended
<i>9.2 Utility service</i>					
Utility entrance	Single feed	Single feed	Single feed	One source with two inputs or one source with single input electrically diverse from backup generator input	Dual feed from different utility substations
Multiple services	Optional—multiple services only based upon the service size	Optional—multiple services only based upon the service size	Optional—multiple services only based upon the service size	Optional—multiple services only based upon the service size	Required. Final count based on ultimate service size
Service entrances physically separated	N/A	Optional	Optional	Optional	Required
Location	Secured or unsecured	Secured or unsecured	Secured or unsecured	Secured	Secured
Underground or overhead	Underground or overhead	Underground or overhead	Underground or overhead	Underground	Underground
Concrete-encased for underground	Optional	Optional	Optional	Recommended	Recommended
<i>9.2.2 Low voltage services (600 VAC and lower in N America and 1000 VAC and lower elsewhere)</i>					
Utility—generator transfer scheme	Typically not available	ATS or breaker	ATS or breaker	ATS or breaker	ATS or breaker
Main	80% rated	80% rated	80% rated	100% rated	100% rated
Data center loads served from	Non-dedicated switchboard	Main Switchboard	Main Switchboard	Dedicated subsystem	Dedicated subsystem
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor
Rating	Series or fully rated	Series or fully rated	fully rated	Fully rated	Fully rated
Construction	Switchboard	Switchboard	Switchboard	Switchboard or switchgear	Switchgear
Breaker types	Fixed or drawout	Static or drawout	Static or drawout	Drawout only	Drawout only
<i>9.2.3 Medium voltage services (601 V–35 kV in N America and 1001 VAC and above elsewhere)</i>					
Utility—generator transfer scheme	ATS or breaker, if generator or alternate source is available	ATS or breaker	ATS or breaker	ATS or breaker	ATS or breaker
Main	100% rated	100% rated	100% rated	100% rated	100% rated
Data center loads served from	Main switchboard or non-dedicated switchboard	Main switchboard	Main switchboard	Dedicated subsystem	Dedicated subsystem

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout, depending on system redundancy	Fixed-mount or drawout, depending on system redundancy
<i>9.2.4 Protective relaying</i>					
Type	Commercial or utility grade	Commercial or utility grade	Commercial or utility grade	Commercial or utility grade	Utility grade
<i>9.3 Distribution</i>					
Cable terminations	Mechanical or compression lug	Mechanical or compression lug	Mechanical or compression lug	Mechanical or compression lug	Compression lug
Busway terminations (where used)	Locking washer	Locking washer	Locking washer	Locking or Belleville washer	Belleville washer
Busway treatment (where used)	Tinned joints optional	Tinned joints optional	Tinned joints optional	Tinned joints optional	Tinned joints recommended
<i>9.3.7 Utility/generator transfer control and generator paralleling switchgear</i>					
Transfer system	Automatic transfer switch or interlocked circuit breakers, if generator present	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers
Critical load system transfer	Automatic or manual transfer if a generator is present. Maintenance bypass optional. UPS power system may be optional.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.
Transfer type	Open- or closed transition	Open- or closed transition	Open- or closed transition	Open- or closed transition	Open- or closed transition
Transfer and control points	One for the whole critical load.	One for whole critical load	Multiple ATSS or 2N on the utility	One for each UPS system; one for each mechanical branch and one for the non-critical load or common loads	One for each UPS system; one for each mechanical branch and one for the non-critical load or common loads
UPS	One, combined with all loads if generator present	One for whole critical load	Dedicated to UPS	Dedicated to UPS path	Dedicated to UPS path
Mechanical	One, combined with all loads if generator present	One for whole critical load	Dedicated to mechanical	Dedicated to each mechanical path	Dedicated to each mechanical path
Non-critical load	One, combined with all loads if generator present	One for whole critical load	Dedicated to non-critical load	Dedicated to non-critical load	Dedicated to non-critical load, maintain diversity of system
Generator control switchgear	If needed	If needed	If needed	If needed	If needed
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker types	Static or drawout	Static or drawout	Static or drawout	Static, with drawout preferred	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or Redundant	Redundant	Redundant
Relay type	Commercial grade	Commercial grade	Commercial or industrial grade	Commercial or industrial grade	Industrial grade
9.3.8 Unit substations					
Transformer MV primary protection	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility
Transformer specification	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount, with drawout preferred	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or Redundant	Redundant	Redundant
9.3.9 UPS					
UPS Maintenance Bypass Arrangement	Optional	UPS module, static switch and maintenance bypass from same switchboard	UPS module, static switch and maintenance bypass from same switchboard	UPS module may be fed from opposite system for redundancy. Alternatively, the downstream critical load being served may be provided from a separate and redundant UPS power system and path. This redundant path may be connected upstream at an ASTS or at the load itself via multiple power cords	UPS module may be fed from opposite system for redundancy. Alternatively, the downstream critical load being served may be provided from a separate and redundant UPS power system and path. This redundant path may be connected upstream at an ASTS or at the load itself via multiple power cords
UPS power distribution—panelboards	Panelboard incorporating standard thermal magnetic trip breakers, if UPS present.	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers
Method of distribution to computer and telecommunications equipment	PDU or individual panelboards, if UPS present.	PDU or individual panelboards	PDU or individual panelboards	PDU	PDU
Multi-system UPS power system synchronization	N/A	N/A	Optional	Optional. May be via static inputs or an external control system.	Optional. May be via static inputs or an external control system.

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
UPS power system segregated from mechanical or support loads	N/A	Optional	Recommended	Recommended	Recommended
External maintenance bypass	Optional	Recommended	Recommended	Recommended	Recommended
<i>9.3.10 Critical distribution switchboards</i>					
Location	Indoor	Indoor	Indoor	Indoor	Indoor
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Static or drawout	Static or drawout	Static or drawout	Drawout only	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or Redundant	Redundant	Redundant
<i>9.3.11 Power distribution units</i>					
Inputs	Single	Single	Single or Dual	Single or Dual	Single or Dual
Transformer K-rating	K-rated depending on load or application	K-rated depending on load or application	K-rated depending on load or application	K-rated depending on load or application	K-rated depending on load or application
Location	In computer room, service gallery (subject to AHJ approval) or electrical room	In computer room, service gallery (subject to AHJ approval) or electrical room	In computer room or service gallery (subject to AHJ approval)	In computer room or service gallery (subject to AHJ approval)	In computer room or service gallery (subject to AHJ approval)
Rating	Continuous duty	Continuous Duty	Continuous Duty	Continuous Duty	Continuous Duty
Breaker Types	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted
Controls	Standalone	Standalone	Standalone	Standalone	Standalone
<i>9.3.12 Static transfer switches</i>					
Use of STS	Critical load switching when alternate source is available	Critical load switching when alternate source is available	Critical load switching when alternate source is available	Critical load switching	Critical load switching
Configuration	Primary or secondary	Primary or secondary	Primary or secondary	Primary or secondary	Primary or secondary
Inputs	Two	Two	Two	Two or Three	Two or Three
Location	In computer room, service gallery or electrical room	In computer room or service gallery	In computer room or service gallery	In computer room or service gallery	In computer room or service gallery
Rating	Continuous duty	Continuous Duty	Continuous Duty	Continuous Duty	Continuous Duty
Short circuit tolerance	Fused or unfused short circuit protection integrated to internal circuit breakers	Fused or unfused short circuit protection integrated to internal circuit breakers	Circuit breaker protection for short circuits	Circuit breaker protection for short circuits or ability to transfer from a shorted bus	Type 3 Circuit breaker protection for short circuits or ability to transfer from a shorted bus
Breaker Types	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted
Controls	Stand-Alone	Stand-Alone	Stand-Alone	Stand-alone	Stand-alone

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
<i>9.3.14 Computer room equipment power distribution</i>					
Individual circuits in separate conduits or cables?	Optional	Optional	Recommended	Recommended	Recommended
Receptacles labeled with individual circuit?	Optional	Optional	Recommended	Recommended	Recommended
Color-coded conduit and junction boxes per upstream UPS source?	Optional	Optional	Recommended	Recommended	Recommended
Twist-lock receptacles for equipment of power strips?	Optional	Optional	Recommended	Recommended	Recommended
Circuits mapped to UPS plant capacity/redundancy	Yes, if UPS power system present	Recommended	Recommended	Recommended	Recommended
<i>9.3.15 Surge protection devices (SPDs)</i>					
Present	Optional	Recommended	Recommended	Recommended	Recommended
Utility entrance(s)	Optional	Recommended	Recommended	Recommended	Recommended
Distribution panel/below source transfer or ATS	Optional	Recommended	Recommended	Recommended	Recommended
UPS input	Optional	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer
UPS output	Optional	Optional	Optional	Recommended	Recommended
PDU/panels	Optional	Optional	Optional	Optional	Optional
<i>9.3.16 Emergency power off (EPO) systems</i>					
<i>Computer room EPO system</i>					
Single Stage system	Recommended	Recommended	Not recommended	Not recommended	Not recommended
3 stage system—off/test/armed	Optional	Optional	Recommended	Recommended	Recommended
CCTV Camera on EPO Station	Optional	Optional	Optional	Optional	Recommended
Shutdown of UPS power receptacles in computer room area pursuant to Code?	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Shutdown of ac power for cooling equipment in room?	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Compliance with local code (e.g. separate systems for UPS and HVAC)?	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Ability to safely turn off fire alarm connection for maintenance?	Recommended	Recommended	Recommended	Recommended	Recommended
Activated by emergency power off (EPO) buttons at exits with manual suppressant release per Code?	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Fire suppressant release for single zone system after emergency power off (EPO) shutdown	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Second zone fire alarm system activation. Sounds pre-release on first zone with suppressant release and EPO on the second zone	Optional	Optional	Optional	Recommended	Recommended
<i>9.4 Mechanical equipment support</i>					
<i>9.4.3.2 Chillers</i>					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	Not required	Not required	Not required	Manual or Automatic	Manual or Automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
<i>9.4.3.2 Cooling towers</i>					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or Automatic	Manual or Automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
<i>9.4.3.3 Pumps</i>					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or Automatic	Manual or Automatic

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
<i>9.4.3.4 Air handling systems</i>					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or Automatic	Manual or Automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
<i>9.4.3.5 Humidification</i>					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or Automatic	Manual or Automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
<i>9.5 UPS</i>					
Use of UPS	Optional	Required	Required	Required	Required
<i>9.5.3.2.1 Static UPS</i>					
Sizing	Either not present, or rated at <N for the connected critical load	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor
<i>9.5.3.2.2 Rotary and hybrid UPS</i>					
Sizing	Either not present, or rated at <N for the connected critical load	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor
<i>9.5.4 Paralleling and controls</i>					
Static switch duty type	Momentary, if present	Momentary	Momentary or Continuous	Continuous	Continuous
External Synch	N/A	N/A	By design	By design or active control	By design or active control
<i>9.5.5 Batteries and Stored Energy</i>					
Flywheel or battery	Either	Either	Either	Either	Either
Sizing	kW	kW	kW	kW	kW
Spill containment	By code	By code	By code	By code	By code

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Monitoring	Capacity only at UPS	Capacity only at UPS	Capacity only at UPS	Capacity only and individual cells	Capacity only and individual cells with individual cell management
Monitoring interface with BMS	Optional	Optional	Optional	Recommended	Recommended
One battery string per module	Optional	Optional	Optional	Recommended	Recommended
Minimum full load standby time	Battery run time determined to affect load transfer to generator or no less than 5 minutes or minimum safe time to transfer to generator from kinetic energy storage system.	No less than 5 minutes or minimum safe time to transfer to generator from kinetic energy storage system.	No less than 10 minutes or minimum safe time to transfer to generator from kinetic energy storage system.	Run time coordinated with UPS topology and failure recovery, but no less than 10 minutes per system, or minimum safe time to transfer to generator from kinetic energy storage system	Run time coordinated with UPS topology and failure recovery, but no less than 10 minutes per system, or minimum safe time to transfer to generator from kinetic energy storage system
Battery full load testing/inspection schedule	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer
Batteries separate from UPS/switchgear equipment rooms	Optional, depending on battery type and size of system	Optional, depending on battery type and size of system	Optional, depending on battery type and size of system	Recommended	Recommended
Battery monitoring system	UPS self monitoring, if UPS power system present	UPS self monitoring	UPS self monitoring	UPS self monitoring	Centralized automated system to check each cell for temperature, voltage, & ohmic measurement
9.6 Standby power systems					
Generator or assured alternate power source utilized	Optional	Required	Required	Required	Required
Fuel run time	No requirement	8 hours minimum	24 hours minimum	72 hours minimum	96 hours minimum
Rating	No requirement	kW load only	kW load only	kW load only	kW load only
Load Supported	No requirement	All loads	All loads	All loads	All loads
Installation	No requirement	Outdoor or indoor	Outdoor or indoor	Indoor	Indoor
Redundancy	No requirement	N	N	N+1	Greater than N+1
Bearing Sensors	No requirement	No	No	Optional	Recommended
9.6.2 Starting systems					
Start time delay (maximum for 1st generator on and load transferred)	No recommended time in excess of AHJ requirements	10 s	10 s	10 s	10 s
Load assumption time (all loads)	No recommended time in excess of AHJ requirements	3 min	2 min	1 min	1 min
Battery capacity	N	N	N	2N/independent	2N/independent
Starter count	N	N	N	2N	2N

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>	
Best battery selection system	Optional	Optional	Optional	Recommended	Recommended	
<i>9.6.3 Fuel systems</i>						
<i>Fuel filters</i>	Grade	Standard	Standard	Standard	Marine	Marine with fuel/water separator
	100 micron	Recommended	Recommended	Recommended	Recommended	Recommended
	30 micron	Optional	Optional	Optional	Recommended	Recommended
	10 micron	Optional	Optional	Optional	Optional	Recommended
	Spin-on/off while operating	Optional	Optional	Optional	Recommended	Recommended
Fuel polish	Optional	Optional	Optional	Recommended	Recommended	
Fuel additive/treatment	Optional	Optional	Optional	Recommended	Recommended	
Fuel line type	Standard	Standard	Standard	Marine/Braided Steel	Marine/Braided Steel	
<i>9.6.4 Exhaust systems</i>						
Sound rating	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	
Air quality	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	
Pollution abatement	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	
Exhaust piping	Welded	Welded	Welded	Welded	Welded	
Connections to engine	Steel and flexible	Steel and flexible	Steel and flexible	Steel and flexible	Steel and flexible	
<i>9.6.5 Cooling systems</i>						
Rating	Match engine rating for continuous, standby or prime rating	Match engine rating for continuous, standby or prime rating	Match engine rating for continuous, standby or prime rating	Match engine rating and ASHRAE (or local equivalent) extreme temperature published for the project location	Match engine rating and ASHRAE (or local equivalent) extreme temperature published for the project location	
<i>9.6.4 – 9.6.6 Monitoring and controls</i>						
Controls	Onboard generator	Onboard generator	Onboard generator or centralized if paralleled	Onboard generator or centralized if paralleled	Onboard generator or centralized if paralleled	
Pre-Alarm Conditions Reported	No	No	Yes, summary only	Yes, by point	Yes, by point	
Alarm Conditions Reported	Yes, summary only	Yes, summary only	Yes, summary only	Recommended by point	Recommended by point	
Trouble Conditions Reported	Yes, summary only	Yes, summary only	Yes, summary only	Yes, by point	Yes, by point	
<i>9.6.6 Mounting</i>						
Mounting	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements	

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
<i>9.7 Automation and control</i>					
<i>9.7.2. Monitoring</i>					
Summary alarm and trouble alerts	Optional	Optional	Recommended	Recommended	Recommended
Dynamic/real time single line	Optional	Optional	Optional	Optional	Recommended
Operations simulator	Optional	Optional	Optional	Recommended	Recommended
Utility bus/buses	Optional	Optional	Optional	Recommended	Recommended
Generator bus / buses	Recommended	Recommended	Recommended	Recommended	Recommended
Generators	Recommended	Recommended	Recommended	Recommended	Recommended
Non-critical and mechanical power systems	Optional	Optional	Optional	Recommended	Recommended
UPS output bus	Optional	Optional	Recommended	Recommended	Recommended
UPS modules	Optional	Optional	Recommended	Recommended	Recommended
Batteries/stored energy system	Optional	Optional	Recommended	Recommended	Recommended
PDU's	Optional	Optional	Recommended	Recommended	Recommended
Collector bus or static bypass cabinet	Optional	Optional	Recommended	Recommended	Recommended
Branch circuit distribution	Optional	Optional	Recommended	Recommended	Recommended
EPO system (when present)	Optional	Optional	Recommended	Recommended	Recommended
Fire alarm system	Recommended	Recommended	Recommended	Recommended	Recommended
Power quality	Optional	Optional	Recommended on the UPS output, optional on other portions of the system	Recommended only on the Utility, generators and UPS output, optional on other portions of the system	Recommended throughout
Database for alarm and trouble signals	Optional	Optional	Optional	Recommended	Recommended
Power quality monitoring	Optional	Optional	Recommended	Recommended	Recommended
Utility	Optional	Optional	Optional	Recommended	Recommended
Generator	Optional	Optional	Optional	Optional	Recommended
UPS output bus	Optional	Optional	Recommended	Recommended	Recommended
PDU	Optional	Optional	Optional	Optional	Recommended
<i>9.7.3 Power control</i>					
Controls clearly indicated and posted	Recommended, if present	Recommended, if present	Recommended	Recommended	Recommended

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
<i>9.7.4 System integration</i>					
Integrated electrical system monitoring	Optional	Optional	Optional	Recommended	Recommended
Electrical monitoring integrated to overall system	Optional	Optional	Optional	Recommended	Recommended
Electrical monitoring integrated to IT management system	Optional	Optional	Optional	Recommended	Recommended
<i>9.8 Lighting</i>					
<i>9.8.3 Computer rooms</i>					
Level	500 lux	500 lux	500 lux	500 lux	500 lux
Uniformity	>90%	>90%	>90%	>90%	>90%
Control	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors
Emergency	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles
<i>9.8.4 Support areas</i>					
Level	As required by IES	As required by IES	As required by IES	As required by IES	As required by IES
Uniformity	>90%	>90%	>90%	>90%	>90%
Control	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors
Exterior areas	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security
Emergency	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles
<i>9.9 Bonding and grounding</i>					
Grounding resistance	If 5 ohm or greater, may not conform to IEEE or BICSI	5 ohm or less, conforming to IEEE and BICSI	5 ohm or less, conforming to IEEE and BICSI. 3 ohms recommended	5 ohm or less, conforming to IEEE and BICSI. 1 ohm recommended	5 ohm or less, conforming to IEEE and BICSI. 1 ohm recommended
<i>9.9 Electrical distribution grounding</i>					
Lighting fixtures (277 V) neutral isolated from service entrance derived from lighting transformer for ground fault isolation	Optional	Optional	Optional	Recommended	Recommended
Building electrical main grounding busbar	Optional	Recommended	Required	Required	Required

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Ground wires in all feeders and branch circuits? (Grounding conductors shall be carried in all power system raceways)	Recommended	Recommended	Required	Required	Required
Grounding method	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded
<i>9.9 Critical power system grounding</i>					
mesh-BN, mesh-IBN, or combination thereof in computer room	Recommended	Recommended	Required	Required	Required
Lightning protection system	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780.	Based on risk analysis as per NFPA 780.	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780
Lightning detection system	Optional	Optional	Optional	Recommended for areas subject to lightning	Recommended for areas subject to lightning
Online weather system on site	Optional	Optional	Optional	For areas subject to lightning	Yes
Hazard signage installed	Required	Required	Required	Required	Required
Instructions posted	Required	Required	Required	Required	Required
MSDS posted or library	Required	Required	Required	Required	Required
All equipment labeled	Required	Required	Required	Required	Required
Equipment color coded	Optional	Optional	Recommended	Recommended	Recommended
Single line diagrams posted	Optional	Optional	Optional	Recommended	Recommended
All electrical systems tested prior to operation	Optional	Mandatory	Mandatory	Mandatory	Mandatory
All electrical system equipment labeled with certification from 3rd party test laboratory	Optional	Mandatory	Mandatory	Mandatory	Mandatory
<i>9.11 System start up and commissioning</i>					
Equipment subject to in- factory testing prior to project delivery – Level 1 Commissioning	Optional	Optional	Optional	Recommended	Recommended
Pre-functional start-up by manufacturer – Level 2 Commissioning	Recommended	Recommended	Recommended	Recommended	Recommended

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Equipment functional testing – Level 3 Commissioning	Optional	Optional	Recommended	Recommended	Recommended
System functional – Level 4 Commissioning	Optional	Optional	Recommended	Recommended	Recommended
Electrical system testing – Level 4 Commissioning	Optional	Optional	Optional	Recommended	Recommended
Whole building testing – Level 5 Commissioning	Optional	Optional	Optional	Optional	Recommended
<i>9.12. Critical Facility operations and maintenance</i>					
Change control/change management	Optional / likely not present	Optional / likely not present	Present / not integrated with IT	Present / coordinate with IT	Present / integrated with IT
Work rules	Not scripted	Not scripted	Scripted	Scripted	Scripted / back check
Maintenance staff	Onsite day shift only. On call at other times	Onsite day shift only. On call at other times	Onsite day shift only. On call at other times	Onsite 24 hrs M-F, on call on weekends	Onsite 24/7
Preventative maintenance	Optional	Recommended	Recommended	Limited preventative maintenance program	Comprehensive preventative maintenance program
Facility training programs	Optional	Recommended	Recommended	Comprehensive training program	Comprehensive training program including manual operation procedures if it is necessary to bypass control system

This page intentionally left blank

10 Mechanical

10.1 Code compliance and coordination

Local building codes shall be consulted in the planning and implementation of changes to the building, mechanical, electrical, and life safety systems. Code references in this standard are generally to the 2000 edition of the International Code series:

- International Building Code (IBC);
- International Mechanical Code (IMC).

The IMC establishes specific requirements for ventilation rates, in coordination with ASHRAE 62.1, and specifies battery room exhaust requirements:

- International Plumbing Code (IPC);
- International Fuel Gas Code (IFGC).

With the exception of California and Hawaii, one or more of the international codes have been adopted in every state in the US, either statewide or at the municipal level.

State and local adoption of the International or uniform codes is often done by incorporation into the state building code, with amendments to specific sections. Scope of amendments may be significant. Local amendments shall be checked before making decisions based on code requirements.

10.2 Terminology differences between codes and telecommunications standards

Terminology used in building codes and by building code officials may differ from terms commonly used in the computer and telecommunications industry. For example, codes use the term “equipment room” to describe rooms housing mechanical or electrical equipment such as air handlers, pumps, chillers, transformers, and switchgear. However, the *ASHRAE Thermal Guidelines for Data Processing Environments (ASHRAE Thermal Guidelines)* document defines equipment such as servers, storage products, and PCs.

10.3 Environmental conditions

10.3.1 Introduction

Telcordia GR-3028-CORE includes a discussion of the differences between machine and human requirements. Generally, modern data centers are not designed to provide human comfort conditions. Temperatures, air velocities, and noise levels often exceed acceptable human conditions. High processing power is moving data centers toward an industrial environment.

10.3.2 Normal operation versus loss of environmental control

Normal operating conditions exist when the HVAC system provides the necessary air conditioning to maintain the computer room within specifications. Designed properly, very high densities can be cooled adequately. Even in computer rooms with moderate densities, however, loss of the HVAC system (whether through loss of power, or cooling equipment failure) can result in steep temperature gradients and subsequently high space and equipment inlet temperatures.

10.3.3 Environmental Class definitions

10.3.3.1 ASHRAE thermal guidelines

The Environmental Class recommended in *ASHRAE Thermal Guidelines* that is the most significant for the day-to-day operation of a typical data center is Class 1: Equipment in Operation. The recommended environmental limits are:

- 18.3 to 26.7 °C (64.4 to 80.6 °F);
- 60% maximum relative humidity (RH);
- maximum dewpoint of 15 °C (59 °F);
- minimum dewpoint (lower moisture limit) of 5.5 °C (42 °F).

Dewpoint of 5.5 °C corresponds to approximately 44% RH at 18 °C (64 °F) and 25% RH at 27 °C (81 °F). The lower moisture limit is used to control electrostatic discharge (ESD).

The preceding conditions are stated at sea level. The recommended maximum dry-bulb temperature is derated by 1 °C/300 m above 1800 m.

ASHRAE recommended temperature and humidity conditions are measured at the equipment inlet and operating compliance with thermal guidelines can be demonstrated by using the Rack Cooling Index (RCI), listed in Section 10.3.4.3.

NOTE: Refer to Section 2 of the *ASHRAE Thermal Guidelines* for definitions of the other environmental classes.

10.3.3.2 NEBS GR-3028-CORE

The recommended limits for environments are 18.3 to 26.7 °C (64.4 to 80.6 °F) and maximum 55% relative humidity.

10.3.4 Air conditioning

10.3.4.1 Introduction

Control of environmental conditions within the data processing areas, as well as the supporting areas, such as UPS rooms, is critical to the functioning of computer equipment. Data processing areas have unique needs associated with heat generation, gaseous contaminants, air impurities, and variations in humidity and temperature.

10.3.4.2 Recommendations

HVAC design should consider and provide for:

- controls for temperature and humidity at the computer equipment inlet;
- adequate filtration and ventilation;
- the special needs of direct cooled equipment;
- airflow patterns for heat dissipation within the room;
- the avoidance of recirculation of hot air;
- redundant cooling systems, as determined necessary by the user;
- architectural features such as a tight vapor barrier.

Control of temperature and humidity is achieved when conditions at the equipment air inlet are maintained within the limits established by *2008 ASHRAE Environmental Guidelines for Datacom Equipment - Expanding the Recommended Environmental Envelope* or GR-3028-CORE. Limits include both high and low values of temperature, humidity, and rate of change for temperature. Because relative humidity varies with temperature without the addition or removal of moisture, it is a moving target and therefore not a good indicator of stable environmental conditions. A much more effective parameter is dewpoint. Whenever possible, space environmental controls should seek to achieve a stable dewpoint over the acceptable temperature range. This strategy will improve the stability of both temperature and humidity in the computer room.

It is recommended that consideration be given to further improve of the cooling system performance by using modular CRAC units, cold or hot aisle containment, or a combination of the two techniques. Such measures will stop hot air contaminating the expensive processed cold air and improve the environment for the remainder of the computer room space. However, a hot air return plenum may require the use of cabinet exhaust chimneys and greater cabinet depth.

10.3.4.3 Additional information

The Rack Cooling Index (RCI) is a best practice performance metric designed to gauge the compliance with the thermal guidelines of ASHRAE and NEBS for a given data center. The RCI is a measure of how effectively equipment racks are cooled and maintained within industry thermal guidelines and standards. As such, the Index can help engineers and architects to design well-functioning data centers and the Index can be used to specify the level of compliance required as part of a basis-of-design document (Herrlin, M. K. 2005. *Rack Cooling Effectiveness in Data Centers and Telecommunications Central Offices: The Rack Cooling Index (RCI)*. ASHRAE Transactions, Volume 111, Part 2, American Society of Heating, Refrigerating and Air-conditioning Engineers, Inc., Atlanta, GA).

The computer room air distribution method may be vertical, such as overhead or underfloor, or may be horizontal, such as a flooded supply or with cooling units in the rows of equipment. Overhead distribution is sometimes chosen when no access floor is used, or when central air handling equipment is used versus CRAC units. Be aware that overhead distribution may introduce more limitations than underfloor distribution, and may limit the choice of HVAC equipment. Horizontal distribution methods can also be used without an access floor. Flooded supply from an upflow or downflow cooling unit can be used, while placing cooling units among the racks is one method to close-couple the heat load to the cooling, minimizing mixing of hot and cold air. The selection of air distribution method involves many factors that are specific to a particular project. The method of air distribution should not be selected before a thorough review of the project requirements, including but not limited to physical limitations of the building, fire suppression systems, location of power and communications cabling, and budget. Refer to *ASHRAE Design Considerations for Datacom Equipment Centers (ASHRAE Design Considerations)* and *ASHRAE Datacom*

Equipment Power Trends and Cooling Applications (ASHRAE Datacom Equipment Power Trends) for additional guidelines regarding HVAC design.

10.3.5 Ventilation (outside air)

10.3.5.1 Equipment rooms

10.3.5.1.1 Introduction

Human occupancy in data centers is typically low. However, removal of internally generated pollutants and maintaining a positive pressure in the space should be considered when determining a ventilation rate. Maintaining a positive pressure relative to adjacent spaces is important as contaminants or dirt could migrate into the data center. It is especially important when the adjacent space is outdoors, as wind effects can create pressure differentials that will exceed the space pressurization, resulting in increased outdoor air infiltration.

10.3.5.1.2 Recommendations

GR-3028-CORE recommends 0.25 air changes per hour for removal of internally generated contaminants, which equals the code requirement when the total ceiling heights and access floor height is 3.7 m (12 ft) and exceeds the code requirement when this dimension is greater than 3.7 m (12 ft).

Absence or presence of vapor barriers must be considered to ensure acceptable environmental control, and to prevent mold growth.

10.3.5.1.3 Additional information

Ventilation is defined by ASHRAE as air supplied to or removed from a space for the purpose of controlling air contaminant levels, humidity, or temperature. It is typically interpreted as the portion of the supply air that is “fresh” outdoor air that has not been recirculated or transferred from any other space.

Ventilation rates prescribed by codes (*International Mechanical Code*, or other Mechanical codes adopted by the Local or State jurisdiction) and by ASHRAE 62.1 are concerned with meeting the needs of occupants. Meeting the requirements of ASHRAE 62.1 may not provide sufficient ventilation for adequate space pressurization, but code compliance must always be documented in the design process.

As ventilation rates increase, the potential for introducing contaminants into the computer room may also increase. This is because typical filter holding frames provided by the manufacturers of air handling units allow for some bypass around the filters. As the volume of outdoor air supplied to the computer room increases, the volume of unfiltered bypass air will also increase. Filter frame leakage efficiency is addressed in Section 10.3.6.

10.3.5.2 Battery rooms

NOTE: Additional information can be found in *International Mechanical Code*, Section 5: Exhaust Systems, and NFPA 70E, Article 320.

10.3.5.2.1 Requirements

When mechanical ventilation is provided, the minimum required exhaust flow is 1 cfm/ (ft² of room area), with hydrogen concentration limited to 1% of the total room volume. Conservative HVAC engineers often design the battery room exhaust system for 0.61 m³ per minute/(m² room area) (2 ft³/[ft² of room area]).

Ventilation is required for both VRLA and flooded cell batteries.

10.3.5.2.2 Recommendations

Battery rooms (or enclosures) should limit the concentration of hydrogen gas to less than 1% concentration.

In most cases, a dedicated exhaust system is provided to remove hydrogen gas that may accumulate.

Battery ventilation is a code-required safety system, and is independent of Class. Redundant exhaust fans are not required by codes, but should be provided for Class F3 and Class F4 data centers to be consistent with the reliability goals of such facilities, along with an alternate source of makeup air in the event of a makeup air system failure. Exhaust fan operation/status should be monitored.

If hydrogen detection systems are provided, they should be monitored by the central security monitoring or building automation/management system.

10.3.5.3 Computer room pressurization

10.3.5.3.1 Recommendations

ANSI/TIA-942 specifies a positive pressure differential with respect to surrounding areas. A typical range for the pressure differential between the computer room and any adjacent rooms is 3 to 12 Pa (0.012 to 0.05 in of water column).

Controlling room pressure differential with a building control system and a system of dampers or variable speed fans is often complicated, with limited effectiveness, especially if doors are frequently opened and closed. Generally, manual balancing to achieve the desired pressure differential is sufficient. Room pressure differential should be monitored.

Loose or leaky construction (such as oversized, unsealed openings created for piping, conduit, or cabling, abandoned openings, and poor construction methods) that may exist in older buildings will significantly increase the volume of makeup air required for pressurization. Care should be taken during construction to seal cracks and openings that prevent adequate pressurization.

10.3.6 Airborne contaminants (gases and particles)

10.3.6.1 Indoor limits

See ANSI/TIA-942, *ASHRAE Gaseous and Particulate Contamination Guidelines for Data Centers*, or applicable local code or standard for a list of contaminants levels.

10.3.6.2 Recommendations

Particulates in the air degrade computer operations. Good operating practices will limit or prohibit the most common sources of particulate contamination from the computer room (i.e., cardboard and storage of paper). Maintaining a controllable positive pressure in the computer room with respect to adjacent spaces will aid in reducing infiltration of particulates and humid/dry air. However, excess positive pressurization can be detrimental.

The air-handling unit supplying outdoor air should be equipped with filters to at least MERV 13 (ASHRAE 80% to 90%) to ensure a clean air supply. When this is not possible, the air supplied to the computer room for pressurization should be filtered to this level before it is supplied to the space.

Air handling units supplying outdoor air should be equipped with low-leakage filter holding frames to limit bypass to less than 1% at 0.7 kPa (3 in water column) differential pressure.

Users should not replace “standard” efficiency filters in their existing packaged computer room air conditioners with high-efficiency filters without first consulting the manufacturer of the equipment to assess the impact of this change, as reduced airflow and cooling capacity could result.

10.3.6.3 Additional information

Pressurization of the computer room with air supplied from outside the space is the most effective means of controlling infiltration of particulate that could migrate from surrounding spaces.

Particulate contamination originating from the building’s construction should be addressed, where possible, by thoroughly cleaning of the space before it is occupied. It is important to understand that increasing the filtration level at the air handlers has only a marginal benefit compared to the additional energy expended by the fan systems.

The standard filters furnished with packaged computer room air conditioning equipment have either 20% or 30% ASHRAE efficiency ratings. Higher efficiency filters at CRAC units will not provide significant improvements in air quality, and will result in higher energy costs. See the *ASHRAE Handbook* or ASHRAE 52.2 regarding minimum efficiency reporting value (MERV) ratings of filters.

Manufacturers offer optional high-efficiency filters, usually up to 85% ASHRAE efficiency (some equipment offered in Europe is available with near-HEPA filter quality filters). Selecting high-efficiency filters will require a higher static pressure blower, and correspondingly higher horsepower motors.

10.3.7 Environmental limits

10.3.7.1 Additional information

ASHRAE Thermal Guidelines specifies allowable and recommended environmental limits for four classes of environments and NEBS in both Product Operation and Power Off modes. For a typical operating computer room, the ASHRAE Class 1 recommended conditions apply, and are noted below. See Table 2.1 in *Thermal Guidelines* for all other conditions. Of note, TIA guidelines correspond to the ASHRAE Class F1 Recommended conditions.

2008 ASHRAE Environmental Guidelines for Datacom Equipment – Expanding the Recommended Environmental Envelope specifies that the recommended maximum dry-bulb temperature should be derated by 1 °C/300 m above 1800 m.

10.3.7.1.1 Recommended operational

ANSI/TIA-942: dry bulb temperature is 20 °C (68 °F) to 25 °C (77 °F)

NEBS: dry bulb temperature is 18 °C (65 °F) to 27 °C (80 °F) per GR-3028-CORE.

ASHRAE: dry bulb temperature: 18.3 C (64.4 F) to 26.7 C (80.6 F)

10.3.7.1.2 Rate of change operational

ANSI/TIA-942: maximum rate of change is 5 °C (9 °F) per hour

NEBS: maximum rate of change is 30 °C (54 °F) per hour

ASHRAE: maximum rate of change is 5 °C (9 °F) per hour

10.3.8 Humidity control**10.3.8.1 Additional information****10.3.8.1.1 Recommended operational relative humidity**

ANSI/TIA-942: 40% to 55%

NEBS: Maximum 55%, a generally accepted telecommunications practice, and no NEBS requirements exist

ASHRAE: 60% maximum relative humidity; dewpoint (absolute humidity) is between 5.5 °C (42 °F) and 15 °C (59 °F)

10.3.9 Temperature and humidity control—tape media**10.3.9.1 Additional information**

ASHRAE: *ASHRAE Thermal Guidelines* Table 2.1, footnote b notes that environments for tape products are more critical than computer equipment. This footnote sets Environmental Class F1 as the standard, and includes limits for humidity rate of change.

10.3.10 Maximum dewpoint**10.3.10.1 Recommendations**

One of the more practical considerations regarding dewpoint temperature limits in a computer room is to avoid cold surfaces in the computer room. If equipment is brought into the room when its surface temperature is below the room dewpoint, condensation on that cold surface will occur. The same is true for building components: insufficient insulation of an exterior wall or roof assembly could result in a surface temperature below the room dewpoint, with condensation resulting.

10.3.10.2 Additional information**10.3.10.2.1 Maximum Dewpoint**

ANSI/TIA-942: 21 °C (69.8 °F)

NEBS: 28 °C (82 °F)

ASHRAE: 15 °C (59 °F)

Dewpoint temperature, dry bulb temperature, and relative humidity are inter-related conditions: any two of these parameters defines the third.

10.3.11 Altitude**10.3.11.1 Additional information****10.3.11.1.1 Maximum altitude**

NEBS: 4000 m (13,000 ft)

ASHRAE: 3050 m (10,000 ft)

Maximum altitude is specified to account for the limitations of HVAC equipment.

10.3.12 Noise levels**10.3.12.1 Recommendations**

Room air distribution noise level should follow ASHRAE guidelines and be at or below the maximum level of NC-45 using the Beranek Noise Criteria (NC) Method.

10.3.13 Leak detection**10.3.13.1 Recommendations**

Leak detection should be provided at any location where water can exist, or at the very least where water is most likely to exist. The most common sources of water are leakage from piping or valves, and condensation on cooling coils in HVAC equipment. Whenever possible, install leak detection in drip pans below the areas that have the highest leak potential. Drip pans can minimize the amount of leak detection equipment required, and provide some degree of containment.

In piping systems, leakage will most likely occur at screwed or flanged connections, at valve stems, or at unions. Welded or soldered joints in piping have a much lower leak potential. However, especially in insulated piping systems, water can “travel” along a sloped pipe, and drip off many feet from the source of the leak. A continuous drip pan below piping, with either spot or continuous detection, is desirable.

If drip pans are not feasible, the piping should be equipped with leak detection cables installed directly within the thermal insulation, to provide for early leak detection. Additional leak detection cables should be installed below the piping on the floor in areas with screwed or flanged connections or valves.

Air handling units should be provided with drip pans below, with spot detection in the drip pan. If drip pans are not feasible, a loop of leak detection cable around the unit will detect, but not contain a leak. The most common failure modes in air handlers that result in leaks are:

- failed condensate pump. Gravity drainage is always preferable to a pump;
- overflow of condensate drain pan. This happens either due to plugging of the outlet with biological material growing in the pan, or due to an improperly configured drain trap;
- leaking coil connection.

10.4 Thermal management

10.4.1 Introduction

Effective heat removal from computer equipment requires attention to the direction of airflow. An important part of thermal management of air-cooled electronic equipment is air management. Selection of the appropriate HVAC system and equipment are made based on many factors. There is no single HVAC solution that is appropriate for all data centers, and some systems may be inappropriate for a particular combination of factors. Each of the factors noted below, either individually or in combination can have a significant impact on the selection of the appropriate system and cooling equipment:

- room size;
- overall cooling density (watts per square meter or watts per square foot), which is established by the maximum kW load for the computer equipment used in the electrical design. Cooling load should match actual operating load, as opposed to nameplate load;
- kW per cabinet or module;
- number and capacity of HVAC units required to meet load and redundancy criteria, and their location in the space relative to computer equipment layout.
- room location relative to mechanical support spaces;
- room location in the building relative to outdoors;
- ceiling height;
- absence or presence of access floor;
- access floor height;
- future expansion needs;
- reliability requirements;
- available maintenance personnel;
- local climate.

As the cooling load and power density increase, selection of the appropriate HVAC system becomes more and more critical. Refer to GR-3028-CORE for a definition of Room Cooling (RC) and Supplemental Cooling (SC) Classes for equipment environments.

ASHRAE Datacom Equipment Power Trends and *ASHRAE Design Considerations* provide in-depth descriptions of data center HVAC systems and equipment.

10.4.2 Use of operating rather than nameplate load

ITE manufacturers now provide heat release data to allow more effective planning of cooling system capacity. Using this data will result in significantly more accurate estimates of the heat release than by applying a derating factor to nameplate electrical ratings. *ASHRAE Thermal Guidelines* provides a template for ITE manufacturers to use in reporting heat release and airflow (volumetric flow rate and configuration). Data is provided for Minimum, Full, and Typical configurations, and some manufacturers also have configuration tools available to allow for more accurate estimation of specific hardware configurations.

10.4.3 Current equipment heat release and trends

10.4.3.1 Additional information

Section 3 of *ASHRAE Datacom Equipment Power Trends and Cooling Applications* provides estimates of power and cooling trends through the year 2014 for various hardware platforms. In all cases, these densities are well in excess of the cooling ability of most existing data center HVAC systems.

10.4.4 Equipment heat release specifications

10.4.4.1 Recommendations

Whenever possible, power and cooling requirements for electronic equipment should be determined based on the manufacturer's actual published data for the specific configuration in question. GR-3028-CORE and *ASHRAE Thermal Guidelines* propose a standardized template for equipment manufactured to report power and cooling requirements for use by both end users and the designers of power and cooling infrastructure.

In the absence of the data noted above, refer to Sections 2 and 3 of *ASHRAE Datacom Equipment Power* to estimate power and cooling requirements. Section 2 provides a method for planning a data center based on equipment, applications, and space. Section 3 provides both historical data and future trends for equipment power and cooling requirements for the typical data center platforms.

10.4.4.2 Additional information

ASHRAE Thermal Guidelines includes an example of a Thermal Report in Section 5. In this example, the Nominal Airflow column is where the manufacturer will report the air volume moved through the electronics by the internal server fans. For any particular row of racks, the total of all server airflows in that row represents the total airflow through the racks from the cold aisle to the hot aisle. This is not the same as the volume of air that must be supplied to the cold aisle by the HVAC system. The HVAC system must supply more air, since the temperature difference produced by the HVAC equipment will generally be lower than the temperature rise through the electronics equipment, due to bypass air waste and related mixing of supply air and return air.

10.4.5 Electronic equipment cooling

10.4.5.1 Recommendations

ANSI/TIA-942: Equipment that utilize front-to-rear cooling schemes should be used in conformance to ANSI/TIA-942 and *ASHRAE Thermal Guidelines*, so as not to disrupt the functioning of hot and cold aisles.

Also refer to NEBS GR-3028-CORE: Airflow Protocol Syntax (EC-Class).

Equipment cabinet air inlet temperature measurement points should be selected in accordance with *ASHRAE Thermal Guidelines*.

10.4.6 Humidification and dehumidification equipment

10.4.6.1 Additional information

A study of local environmental conditions in conjunction with building construction will determine requirements for humidification/dehumidification. If ultrasonic humidifiers are used, deionized water should be provided to prevent formation of dust from dissolved solids in the water. If availability of deionized water over the life of the data center is uncertain, ultrasonic type humidifiers should be avoided.

The integrity and construction of the building envelope, use of vapor barriers, pressurization of the computer room relative to adjacent spaces, and the conditioning of outdoor air supplied to the space must be considered in the context of local environmental conditions when selecting a humidity control scheme. If a central steam boiler used for building heating is also used for direct steam humidification, the type of boiler water chemicals should be considered. Generally, steam generating humidifiers (using electricity, natural gas, or steam as the energy source) have a lower life cycle cost than ultrasonic humidifiers which need deionized water in the ultrasonics. Evaporative humidifiers can be very effective and save energy when air from the hot aisle is used to evaporate water. Refer to the *ASHRAE Handbook* for design considerations.

Humidifiers and reheat coils can be included in individual CRAC units. However, when two or more CRAC units are in a space, care should be taken to ensure that the controls and sensors are calibrated so that individual units do not fight each other (e.g., some humidifying while others are dehumidifying). It may be beneficial to use a centralized humidification system to avoid this issue, as well as for ease of maintenance. Refer to *ASHRAE Design Considerations* for information on different types of humidification systems.

10.4.6.2 Location of humidification and dehumidification

Humidification and dehumidification may be located at either the CRAC units or the central air handlers.

10.4.7 Computer room cooling

10.4.7.1 General considerations

HVAC systems and cooling equipment must always be selected using a holistic approach. The choice of air distribution method should never be considered without evaluating other significant factors, such as whether or not an access floor is used, the return air path, location of CRAC units or air handling equipment relative to server racks, orientation of hot/cold aisles, ceiling height, methods for humidity control, and provisions for future expansion, to name just a few. Each choice affects the others, and the overall performance of the data center cooling system will be dictated by the entire package of decisions. ASHRAE *Datacom Equipment Power Trends* and *ASHRAE Design Considerations* provide general descriptions of the various air delivery methods, and some of the cooling system technologies available, but they do not provide hard and fast rules for selection, since there are so many combinations of the factors noted above. A knowledgeable and experienced data center HVAC engineer/consultant is essential to achieve a successful outcome.

10.4.7.2 Access floor versus no access floor

The necessity or use of an access floor for any particular data center depends on a number of factors. As with the selection of an HVAC system, access floor decisions should be made as part of a larger consideration of needs and requirements, many of which are unrelated to the mechanical system.

Advantages of access floor with underfloor air distribution:

- allows great flexibility in location of load to CRAC unit;
- imposes fewer limits on locating CRAC units in the space;
- piping services may be concealed below the access floor;
- more compatible with gravity condensate drainage from cooling coils and humidifiers;
- no overhead supply ductwork to obstruct the return air path, or to interfere with lighting, sprinkler heads, or overhead power/cable distribution systems;
- permits the use of nearly any cooling technology, regardless of air supply/return configuration.

Disadvantages of access floor for HVAC:

- the underfloor space is an air distribution plenum—all cable must be installed in conduit, or be listed for data processing, or plenum rated for flame spread and smoke developed characteristics (refer to 14.4.8.1 for considerations of overhead versus under-floor cable routing);
- poor planning of underfloor utilities can result in blocked airflow and poor cooling performance;
- poor management of cable openings can result in reduced airflow at perforated tiles, supply air grilles, or other supply air openings;
- recent research suggests that overhead cooling delivery may be capable of producing more favorable rack cooling efficiency than underfloor cooling. (Herrlin, M. K. and Belady, C. 2006. *Gravity-Assisted Air Mixing in Data Centers and How it Affects the Rack Cooling Effectiveness*. ITherm 2006, San Diego, CA, May 30–June 2, 2006.)

Access floors have traditionally been the first choice for medium to large rooms with higher power/cooling densities. A factor in this has been the commercial availability of specialized data center HVAC equipment.

Several HVAC equipment manufacturers now offer equipment capable of cooling very high-density loads with localized overhead or horizontal air distribution. This equipment is sometimes suited to specific heat rejection technologies, and may not be appropriate for all buildings.

Access floors offer fewer air distribution advantages for small data centers. Smaller HVAC equipment can perform very well in small spaces, where the electronic equipment is in close proximity to the HVAC unit.

10.4.7.3 The hot aisle/cold aisle concept

10.4.7.3.1 Recommendations

The hot aisle/cold aisle concept for arrangement of computer equipment in the computer room should be used, regardless of whether air distribution is overhead or supplied from an access floor plenum.

10.4.7.3.2 Additional information

Conventional wisdom regarding data center supply air considers recirculation of return air from hot aisles to cold aisles as a condition to avoid. The following example illustrates this and also why controlling environmental conditions based on relative humidity is difficult.

With the ASHRAE Class 1 recommended equipment inlet conditions of 18 to 27 °C (64.4 to 80.6 °F) (dry bulb temperature) and a relative humidity range of 40 to 55%, server exit conditions are very often close to 38 °C (100 °F) and 20% RH. The typical CRAC unit supplies air between 13 °C

and 16 °C (55 °F and 60 °F) and close to 90% RH: clearly conditions that are outside the range required by the typical server manufacturer. To achieve 18 to 27 °C (64.4 to 80.6 °F) at the server inlet, mixing between hot and cold airstreams must occur in the proper proportion, and the resultant air should be uniformly distributed along the entire server rack, top to bottom, unless supply air and return air can be completely isolated from each other and the supply air can then be delivered within the required use parameters. Since server fans generally vary the airflow to maintain a balance between temperature and power consumption, the airflow through the server cabinets is not constant.

The temperature and relative humidity displayed on the CRAC unit control panel is measured at the inlet to the CRAC unit. This temperature represents the mixed condition of all the air that makes it back to the CRAC unit. In most data centers, the CRAC unit temperature set point is set between 20 to 25 °C (68 to 77 °F), and the CRAC unit operates to maintain this temperature. This tells the data center manager/operator that enough hot aisle air has mixed with enough cold aisle air in the space between the CRAC unit and server racks to ensure that the right conditions exist at the CRAC unit inlet, but it tells nothing of the conditions that are most important - the actual temperature at the server inlets. For the condition described above to exist, the air temperature at the server inlets will be well below the temperature range recommended by ASHRAE, with a corresponding elevation of relative humidity.

Airflow in the typical data center consists of two flow loops:

- CRAC units (a few big fans) circulate air within the entire room;
- servers (many little fans) circulate air between cold and hot aisles.

These loops are “decoupled”: they do not depend on each other, and one will continue to operate if the other is shut off, or if the flow rates do not balance. Hot air is buoyant and will tend to rise, and all air will take the path of least resistance relative to the room pressure gradients. Air will tend to flow back toward the CRAC unit inlets, but the greater the distance from the CRAC unit, the less momentum the air mass has to overcome turbulence.

Each of the two airflow loops described above operates with a different temperature difference between inlet and supply. However, the energy must balance between the two: all of the heat rejected from the servers must be further rejected in the CRAC unit. Therefore, the relative airflow rates of the two loops will be proportional to the temperature difference of each loop. The air temperature rise through servers is not constant, since most servers use variable speed fans to balance CPU temperature, power consumption, and noise, but 11 °C to 17 °C (20 °F to 30 °F) is common. CRAC units typically will operate at a constant volume, and varying temperature rise based on load, depending on the type of cooling technology employed. A typical CRAC unit temperature difference is 8 °C to 11 °C (15 °F to 20 °F) (depending on whether the CRAC’s are chilled water units or are air/glycol cooled). The CRAC unit loop can circulate 50% more air than the sum of all the server fans.

The “ideal” data center HVAC design would supply air at the server inlet at the desired inlet temperature, and at a volume, that matches the server fans. All hot aisle air would be returned to the air-handling units with no mixing or recirculation between hot and cold aisles. When such isolation cannot be achieved, careful attention must be paid to monitoring server in-take supply air to be sure the proper calibration is maintained of the mix of source air and return air.

10.4.7.4 Access floor

10.4.7.4.1 Recommendations

The type of air delivery method through an access flooring system should be consistent. Do not mix perforated tiles with supply air grilles, as the differences in flow/pressure drop characteristics will result in inconsistent and unpredictable performance. Similarly, large, relatively unobstructed openings in the access floor can have significant adverse effects on the underfloor pressurization and should be avoided, as the larger the opening, the smaller the pressure drop corresponding to a particular cubic meters or feet per minute. Since air takes the path of least resistance, large openings will starve the perforated floor tiles. *Large* means any opening that is large relative to a single perforation in an access floor tile. Many (relatively) small openings can begin to look to the HVAC system like a few very large openings.

Cable penetrations into the bottom of server cabinets should be filled to minimize the flow of air directly into the cabinet from below. The area of the unobstructed portion of a cable opening looks to the HVAC system like a large opening. It is not uncommon for unprotected cable cutouts to allow up to half of the total CRAC unit airflow capacity to bypass the perforated tiles.

An access floor system provides a flexible method of delivering cooling to data centers, allowing for numerous configurations. Perforated panels can readily be moved to accommodate high heat load areas. Floor height should be

selected based on the combined needs for airflow, power distribution, network/communications cabling, and chilled water distribution, if used. Access floor heights greater than 900 mm (36 in) introduce additional cost to the flooring system, may require special considerations for access and safety, and do not significantly enhance the uniformity of air distribution below power densities of 1350 W/m² (125 W/f²). For data centers with power densities in the 1610 to 2150 W/m² (150 to 200 W/f²) range, a 1000 mm (42 in) access floor depth should be considered.

Chilled air should always be delivered into the cold aisle in front of the cabinets, not be delivered directly into the bottom of the cabinet. There are three main reasons for this:

- 1) openings provided below the racks for this purpose will generally be large compared to the tile perforations;
- 2) some of the air will bypass out through the back of the rack into the hot aisle;
- 3) air supplied directly into the bottom of a cabinet may be significantly below the minimum temperature prescribed in *ASHRAE Thermal Guidelines* or GR-3028-CORE. CRAC unit discharge air temperatures are typically in the 13 to 16 °C (55 to 60 °F) range, and 80% to 90% RH at that temperature. With underfloor distribution, the air coming out of the perforated tiles will usually be below 20 °C (68 °F).

Room temperature measurement points should be selected in conformance to *ASHRAE Thermal Guidelines*:

- temperature measurement sensors should be regularly calibrated.
- a significant difficulty with temperature and humidity measurement point locations is the physical installation in meaningful locations. Sensors typically must be mounted on a fixed surface, making the mid-aisle 1.5 m (4.9 ft) above floor locations impractical for permanently installed devices. Temperature and humidity sensors furnished with CRAC units are factory installed in the units at their inlet and do not indicate the conditions of the air at the computer equipment inlets.
- temperature-measuring points should ideally mimic the equipment inlet conditions since these conditions define the equipment comfort.

Floor plenums should be as airtight as possible relative to adjacent spaces and cleaned prior to being put into use.

10.4.7.5 Overhead air distribution

Overhead air distribution can be used effectively, although it will generally not be as flexible for future equipment placement as underfloor supply. Fixed diffusers locations limit reconfiguration.

Overhead ductwork must be closely coordinated with lighting, sprinklers, and power or network cabling in data centers where these utilities are not located below an access floor. Overhead ducts wider than 1.2 m (48 in) will require sprinkler heads to be located below the ductwork.

Supply air should be placed in the cold aisles only.

Outlet airflow should be 0.38 to 0.47 m³/sec (800-1000 CFM) per GR-3028-CORE, based on cited *ASHRAE Handbook – Fundamentals* on system specifications for vertical overhead delivery.

10.4.7.6 Row-integrated cooling

For ITE that takes cool air in the front and discharges hot exhaust air out the back, cooling units can be applied within the rows of equipment racks. The cooling units should be designed for row integration, with an airflow pattern from back to front. These types of units, which can be refrigerant or chilled water based, are designed to capture the hot air being exhausted out the back of the equipment into the hot aisle and to discharge cool supply air into the cold aisle in front of the racks. By placing the cooling units very close to the heat source (ITE), the path that the hot air must take to return to an air conditioner can be greatly reduced, thereby minimizing the potential for mixing of hot and cold air streams. Fan power can be lower, and capacity and efficiency can be higher due to the higher return air temperatures to the cooling units. The high return air temperatures also lead to a very high sensible heat ratio, minimizing the amount of unnecessary dehumidification (and a subsequent need for rehumidification to maintain constant humidity levels).

This type of configuration can work well for low- to medium-density loads. For higher densities, it is possible to install a containment barrier around the entire hot aisle to ensure that all of the hot exhaust air is directed into a cooling unit, thereby eliminating any mixing of hot exhaust air with the cool supply air.

10.4.7.7 Other

10.4.7.7.1 Recommendations

Displacement ventilation can be an effective method of cooling data center equipment as long as the equipment configuration is taken into account. Vertical displacement should be considered in rooms with multiple rows of racks, allowing the heat plume to rise in the same direction as the ventilation.

Horizontal displacement system design should avoid return air path crossing through cold aisles.

10.4.7.7.2 Additional information

Horizontal displacement systems will be limited by the maximum cooling density, physical configuration of the room, and by the size range of commercially available CRAC units that are designed for displacement applications.

10.4.8 Supplemental cooling

Supplemental cooling systems are any method of heat management that is added to an existing data center to supplement the primary or original cooling system, either by mitigating local hot spots or by adding cooling capacity. Section 5 of *ASHRAE's Design Considerations* lists five common approaches to supplemental cooling. Each of these approaches is aimed at increasing the local cooling effect by one of the following means:

- improving or regulating air circulation either at the inlet or discharge of the ITE cabinet or rack;
- more closely coupling cooling equipment with the ITE;
- isolating hot and cool airstreams from one another to reduce recirculation or mixing;
- directing cool air from the cooling equipment discharge into the ITE inlets;
- directing hot air from the ITE discharge into the return air path to the cooling equipment.

Well-designed airflow management brings significant performance and efficiency benefits every opportunity to improve air circulation and isolate the hot and cold airstream should be considered in the design of primary cooling systems for new data centers. These techniques can also be applied to correct hot spots or when expansion of the primary system is too costly or disruptive to correct the problem at hand.

The choice of supplemental cooling systems depends partially on whether the problem is a shortfall of cooling capacity, or lack of cooling effectiveness. A capacity shortfall can only be addressed by systems that provide heat rejection to the outdoors or to an existing system such as chilled water. System effectiveness problems are most likely due to airflow deficiencies, which may be improved by airflow solutions.

10.4.8.1 In-room

Supplemental chilled water room cooling units may be used to cool room hot spots when floor space and chilled water are available in accordance with the system descriptions of GR-3028-CORE.

10.4.8.2 In-frame

Supplemental in-frame chilled water-cooling may be used where water can be introduced into the computer room and where a solution does not exceed the standard cabinet floor utilization specifications to deliver the cooling benefits described in GR-3028-CORE.

10.4.8.3 Direct return

Direct return air systems may increase the cooling capacity of the supply duct system when equipment is located per GR-3028-CORE and has an acceptable interface between the equipment exhaust and the ductwork:

One method of direct return is to install rack-mounted fan air-removal units to capture 100% of the exhaust air from each rack and direct the hot air to an overhead return air plenum. This solution works well as a solution for isolated hot spots or for new installations. Because it requires unique ducting on every rack, some of the benefits can be offset by the cost and reduced flexibility.

Another method of direct return is to install barriers that will channel 100% of the hot exhaust air from a rack into an adjacent row-integrated cooling unit. This solution is very effective for extreme high-density applications.

A third method of direct return is to use row-integrated air conditioning units and a totally enclosed hot aisle. The hot aisle becomes the return duct to all cooling units installed on either side of the hot aisle. This method is effective when there are many high-density racks in close proximity, thereby creating a high-density zone within the computer room. Provisions must be provided to comply with local codes for smoke detection and fire suppression within the enclosed aisle.

A weakness of direct ducting is that the delta temperature (ΔT) will typically exceed the range of the cooling unit, with one possible result being a resultant increase in the supply air temperature. This can be addressed by specifying special cooling units that operate efficiently at wider ΔT s.

Loosely coupled direct ducting in the ceiling plenum space provides opportunities for "conditioning" the return air with ceiling grates that would allow for some mixing with bypass make-up air. In addition, in environments where there might be reason for mixing ducted exhaust cabinets with standard cabinets, the ceiling grills would be required to move the free-space return air from the room and introduce it into the return air path in the plenum. This could occur where there were high-density cabinets mixed in a room with low- or moderate-density.

A fully deployed ducted exhaust system also greatly reduces the detail management of air delivery to just setting the overall room temperature and assuring it is pressurized just above the consumption rate of the room's cumulative

load. This eliminates the negative effects of low-pressure vortices formed under the floor by cycling between air handlers for service and maintenance

10.4.9 Hot and cold equipment aisles

See *ASHRAE Thermal Guidelines* for a more in-depth discussion of hot and cold aisles.

10.4.10 Equipment layout

Printers and other potential contamination sources should not be located in the computer room.

Cabinets and racks shall be arranged in rows with fronts of cabinets/racks facing each other in a row to create hot and cold aisles. Equipment should be placed in cabinets and racks with cold air intake at the front of the cabinet or rack, and hot air exhaust out the back and/or top. However, reversing the equipment in the rack will disrupt the proper functioning of hot and cold aisles. Blank panels should be installed in unused rack and cabinet spaces to improve the functioning of hot and cold aisles.

When placed on an access floor, cabinets and racks shall be arranged to permit tiles in the front and rear of the cabinets and racks to be lifted. Cabinets should be aligned with either the front or rear edge along the edge of the floor tile, per ANSI/TIA-942.

Cabinet size, location for air entry, location for cable entries, and access to front and rear should be planned for consistency according to ETSI EN 300-019.

CRAC units should be located in the hot aisle path when the return air path is the free space in the room (e.g., not ducted to the CRAC unit inlet).

10.4.11 Supply air layout

When underfloor cooling is used, perforated access floor tiles should be located in the cold aisles only to support the functioning of the hot and cold aisles. For an overhead air distribution system, the supply diffusers should be placed above the cold aisles only.

10.4.12 Return air layout

Return air should be positioned to capture the highest heat concentration, such as return air intakes directly over the hot aisles or directly over equipment producing the highest heat. Capturing the heat with return grilles, and not entraining it in the supply air should be the goal of return and supply layouts. When using a return air system to reduce recirculation, supply air temperature must be controlled to very near the lowest acceptable equipment inlet temperature.

A ceiling height of at least 3 m (10 ft) above the access floor will allow for an effective hot air area above racks and cabinets and optimize the return air path. Rooms with high-density cooling loads should consider ceilings higher than 3 m (10 ft).

10.4.13 Cable management

The cold aisle plenum space should remain unobstructed by raceways in conformance to ANSI/TIA-942.

Floor tile cutouts for cable egress to cabinets and damping around cables should conform to ANSI/TIA-942.

When overhead cable systems are used in lieu of or in addition to underfloor cabling, placement and grouping of cable should be planned to minimize the effects on return air. Obstructions in the return air path could contribute to higher levels of hot air recirculation to the cold aisles, depending on the configuration of the cable system relative to the rack layout (refer to 14.4.8.1 for additional considerations of overhead versus under-floor cable routing).

Telecommunications cabling under the access floor should run parallel to CRAC air delivery path, in accordance with applicable standards (e.g., BSRIA BG 5/2003). Where the cable pathways cross the front of the air delivery system then care should be taken to reduce the impact on the air flow.

Cables shall not be left abandoned under access floor, in overhead raceways, or above suspended ceilings. Inactive cables shall be removed or terminated on at least one end and marked “for future use”.

10.5 Mechanical equipment (design and operation)

10.5.1 General recommendations

Most of the following recommendations and topics are also addressed in more detail in the *ASHRAE Design Considerations for Data and Communications Equipment Centers*.

HVAC availability and redundant power access should conform to the requirements of the Class that best satisfies the reliability goals of the enterprise. The Class chosen will then drive selection and configuration of the HVAC systems and equipment selected. For example, providing CRAC units and other mechanical cooling equipment with dual power sources to ensure continuous operation if one source of power is lost is to be considered for Class F3 and

Class F4, but is not mandatory under the requirements of this standard, and is not required for Class F2 or lower facilities. Mechanical equipment, including specialized mission-critical equipment such as CRAC's, is not offered by manufacturers with provisions for dual power sources as a "standard option". Specifying this feature for mechanical systems should be done only after careful consideration of the costs and complexities involved compared to alternative approaches to achieve the same or similar result.

Use mechanical equipment that is designed for mission-critical installations.

Air ducts, water pipes, and drain pipes not associated with the data center equipment should not be routed through or within the data center spaces.

Electrical power for mechanical systems should be on generator backup.

There should be two independent sources of water for the HVAC systems or one source and on-site storage.

Air filters in air conditioning equipment should have a Class F1 rating. Class F1 filters are less able to support combustion than Class F2 filters.

Duct coverings and insulation should have flame spread ratings less than 25 and smoke developed ratings less than 50.

In areas where there is no equipment to cool, replace perforated tiles with solid tiles and close air ducts.

Mechanical equipment should be anchored to the elements that support them. Equipment that vibrates should be mounted on vibration isolators. The vibration characteristics of the floor should be carefully reviewed.

10.5.2 Computer room air conditioning (CRAC) units

10.5.2.1 Recommendations

At minimum, each computer room should have one redundant CRAC/CRAH, though analysis-using tools such as computational fluid dynamics modeling may determine that more than one redundant CRAC/CRAH may be required to maintain adequate airflow to all areas of the room.

Set points for CRAC and CRAH units should not be set lower than necessary to keep temperature at the equipment air intakes (in the cold aisles) in the 18 to 27 °C (64.4 to 80.6 °F). The temperature in the hot aisles is not a concern if the temperature at equipment air intakes is within these temperature ranges and does not exceed the safe operating limit for wiring and equipment in the hot aisle.

Set points for CRAC and CRAH units should not be any higher (or lower) than required to keep relative humidity below 60% and dewpoint between 5.5 °C (42 °F) and 15 °C (59 °F). Do not unnecessarily humidify or dehumidify air. Additionally, to prevent CRACs/CRAHs from working against each other to control humidity, set all CRACs/CRAHs to the same humidity settings and use a 5% dead-band on humidity set points.

Arrange CRACs/CRAHs and air ducts to enhance the proper functioning of hot and cold aisles. If CRACs/CRAHs are not fully ducted for both air intake and discharge, they should be arranged perpendicular to rows of equipment. Any air intake ducts should be placed in hot aisles. Perforated tiles and tiles with supply grilles should be placed in cold aisles. Overhead supply should be designed to direct air downward into the cold aisle, not laterally, or into hot aisles.

Return ducts for CRACs/CRAHs placed on the room perimeter should be placed as high up in the ceiling as possible and be aligned with hot aisles.

In computer rooms with an access floor, CRAC units located in the room should be supported independently such that they do not transmit vibration to the access floor system.

10.5.3 Central air handlers

Central air handlers are preferred over CRAC units when a ducted supply or return air system is used. CRAC units are packaged systems that do not offer the designer the flexibility to tailor the fan selection to match the duct system performance.

Central air handlers can allow the use of air-side economizers for improved energy efficiency, when the physical configuration of the building and geographical location (e.g., local climatic conditions) are favorable.

10.5.4 Supplemental cooling systems

Supplemental cooling methods include:

- spot cooling;
- cooled cabinets;
- rear door heat exchangers;
- in-row cooling.

Redundancy for supplemental cooling may be required in addition to redundancy for power to support them.

- backup supplemental systems;
- generator feed for supplemental cooling systems;
- dual power feeds for supplemental cooling systems.

10.5.5 Chilled water systems

Systems using chillers as the primary cooling source (with either chilled water CRAC units or built-up air handling systems) can be more energy efficient than systems using air-cooled packaged CRAC units. Packaged air-cooled machines can be less efficient than straight air-cooled CRACS, but offer benefits other than efficiency. Chilled water systems overcome distance limitations on air-cooled CRAC refrigerant piping, allow free-cooling in many climates, and enable thermal storage. Chillers are not as cost effective for smaller systems. There is no strict load that defines smaller, but in general, critical loads below 300 – 400 kW may be too small to provide economic justification for installation of a chilled water system, unless the load is expected to grow significantly over the life of the facility. Each project must be evaluated to determine the suitability of chilled water compared to other cooling solutions.

The entire chilled water system consists of chillers, pumps, cooling towers, controls systems, water treatment, and chilled water distribution piping. Many configurations are possible to achieve alignment with the reliability goals established for the data center.

If dual power paths are provided to the individual components in a chilled water system, the use of transfer switches, either manual or automatic, must be provided at each system component.

10.5.6 Chillers

The chiller technology chosen can depend on the size of the load served, and the availability of space indoors in a dedicated equipment room. Chillers located outdoors will be packaged, air-cooled units, with capacity limited to approximately 500 tons each. If larger chillers are desired, indoor units must be used. Equipment located indoors is better protected from physical and environmental hazards, and may receive better service from maintenance personnel.

10.5.7 Cooling towers

10.5.7.1 Recommendations

For Class F3 and Class F4 facilities, a reliable backup source of water, or water storage must be provided.

10.5.7.2 Additional information

Evaporative cooling towers are generally the most maintenance intensive part of the chilled water system. When evaporative towers are used, installation and maintenance of a condenser water treatment system is essential. Evaporative towers are dependent on a steady source of makeup water (typically domestic, potable water) to provide heat rejection of the building load. Interruption of this water supply will result in a complete cooling system shutdown.

10.5.8 Thermal Storage

10.5.8.1 Recommendations

The thermal storage system should be designed for the simplest operation, with the minimum number of components that must operate and start.

10.5.8.2 Additional information

Goals for thermal storage as a concept must be clearly defined and understood by all parties, and coordinated with the electrical system design. Thermal storage system purpose and function will define the scope and design. Site considerations are important, as some sites do not have adequate space for thermal storage.

Thermal storage systems for data centers are used to provide short term cooling at times such as during a chiller short-cycle lockout. In this case, the energy stored in the thermal storage tank may be required to be available at the point of use in less than two minutes.

10.5.9 Piping and pumps

10.5.9.1 Recommendations

The most effective way (e.g., practical, cost effective) to accomplish “dual path” supply in a chilled water system is to provide a looped piping system, allowing both ends of the loop to be supplied from the chiller plant. Dual piping systems are not practical for most data centers as they introduce significant cost and complexity.

A piping loop may be installed below the access floor on its perimeter, or preferably, outside the room. Sectionalizing valves installed at intervals in the loop will permit isolation of one or more CRAC units or air handlers, for servicing a leaking isolation valve at the unit inlet. If a sectionalizing valve is installed between each CRAC unit branch pipe, then two adjacent CRAC units would need to be shut down to isolate a single leaking sectionalizing valve. An alternative method for valve servicing is to freeze the pipe.

10.5.9.2 Additional information

Circulating pumps, dry coolers, and close-circuit fluid coolers (where used) are subject to the same restrictions regarding dual power as chillers – automatic or manual transfer switches must be installed as part of the electrical design.

Piping itself is very reliable, especially when care is taken in the design and water quality is maintained. Catastrophic failure of piping is rare when compared to other failure modes, such as slow leaks from threaded joints or valve stems and end connections. These concepts should be kept in mind when evaluating designs to achieve high reliability.

Thoughtful design and layout coordinated with the reliability goals of the data center are essential. For example, adding more valves for isolation is not a solution by itself, as installing more valves may only increase the likelihood of failures. Instead, the use of very high quality valves (industrial quality versus commercial quality) can be a cost effective way to achieve higher reliability levels. In the vast majority of data centers of all Classes, commercial quality valves are or will be installed.

10.5.10 Fuel oil tank and piping

10.5.10.1 Recommendations

All fuel oil systems with bulk fuel storage should incorporate the following basic features:

- leak detection and annunciation for both the tank and piping;
- remote monitoring of fuel level;
- physical protection for piping from main tank to building;
- fuel filtration or polishing;
- security at tank fill points (e.g., locking covers);
- training of operators to understand fill equipment operation to prevent accidental entry of water in tanks (underground tanks only).

10.5.10.2 Additional information

Fuel tanks may serve a single generator, or be part of a multiple generator system. Installing multiple bulk storage tanks versus a single larger tank may not increase the reliability of a system, as multiple tanks may add complexity due to the configuration. Site issues can significantly affect the number of tanks that can be installed, as some sites may only have room for a single tank, where others may not be suitable for underground tanks due to ground water or flooding issues.

10.5.11 Plumbing

10.5.11.1 Additional information

The following additional items should be considered when planning plumbing for data centers:

- domestic water;
- tempered water—safety shower/eyewash equipment;
- sanitary sewer;
- storm drainage system.

10.5.12 Generator

The following additional items should be considered when planning generators for data centers:

- exhaust muffler;
- muffler drain;
- louvers and dampers.

10.6 Materials and finishes

10.6.1 Introduction

Problems can arise if improper size, strength, or spacing of materials are used. Finishes must be suitable and not cause danger to persons or equipment.

10.6.2 Materials in air plenums

10.6.2.1 Recommendations

Materials such as wire and cable jacketing, plastic piping, and insulation jacketing must meet UL, NFPA, and fire code requirements for flame spread and smoke developed characteristics.

Plenum-rated or LSZH cable is the minimum required for telecommunications cabling under access floors in many jurisdictions.

PVC piping is not acceptable for use in air plenums. CPVC piping with an appropriate rating is available.

10.7 Referenced standards and documents

This section provides information regarding some of the references used within Section 10 for planning mechanical systems for data centers.

ASHRAE and ASHRAE Technical Committee 9.9-Mission Critical Facilities, Technology Spaces, and Electronic Equipment:

- *Thermal Guidelines for Data Processing Environments* (2004):
This document provides guidance on four topics and adopted several of the concepts that were introduced in Telcordia GR-3028-CORE:
 - defines operating specifications for equipment in four environmental classifications, plus NEBS environments;
 - measurement of temperature and humidity for evaluating data center environmental performance;
 - equipment arrangement based on maintaining proper environmental conditions at the air inlet;
 - recommendations to manufacturers for standardized documentation and reporting of equipment heat generation, power consumption, and airflow performance.
- *Datacom Equipment Power Trends and Cooling Applications* (2005):
This document provides guidance in three areas:
 - concentration and distribution of the various types of network and telecommunications equipment in a typical data center for the purpose of planning and estimating physical space requirements, cooling loads, and power consumption;
 - power consumption and heat generation trends for various classifications of network and telecommunications equipment, with projections through 2014 of watts per rack and watts per square meter (or square foot) for each classification;
 - a general discussion of the predominant cooling technologies and air distribution methods used in data centers. New strategies being introduced by computer room cooling manufacturers are addressed, along with a discussion of water and refrigerant cooling at the rack level.
- *Design Considerations for Datacom Equipment Centers* (2009):
This document incorporates the key concepts of *Thermal Guidelines* and *Datacom Equipment Power Trends* with a comprehensive and in-depth discussion of the critical system design topics for data centers, including reliability, power distribution, structural, acoustics, contamination, and commissioning. Mechanical systems are covered in more depth than nonmechanical topics.
- *Liquid Cooling Guidelines for Datacom Equipment Centers* (2006):
This document provides equipment manufacturers and facility operations personnel with a common set of guidelines for liquid cooling. It covers an overview of liquid cooling, various liquid cooling configurations, and guidelines for liquid cooling infrastructure requirements.
- *2008 ASHRAE Environmental Guidelines for Datacom Equipment—Expanding the Recommended Environmental Envelope* (2008):
This document expands the recommended environmental envelope published in the 2004 ASHRAE TC 9.9 thermal guidelines document to provide greater flexibility in facility operations, particularly with the goal of reduced energy consumption in data centers.
- ASHRAE Standard 62.1, Ventilation for Acceptable Indoor Air Quality:
This standard is the basis for the ventilation rates required by most building codes. The current version is 62.1-2007. The mechanical code in force in a particular state or municipality must be used for the purpose of code compliance. The HVAC designers should use the version of 62.1 that is referenced by the code to establish the appropriate methods to achieve compliance. Some jurisdictions use earlier versions of 62.1, such as 62.1-1989.

National Fire Protection Association (NFPA)

- NFPA 70, National Electric Code:
NFPA 70 and 75 have specific requirements regarding HVAC configuration and operation, depending upon which fire protection strategy is selected. It is important to coordinate the mechanical design and operation with the fire safety design chosen.
- NFPA 70E, Electrical Safety in the Workplace:
Article 320 – Safety Requirements Related to Batteries and Battery Rooms, sets general requirements for ventilation and safety equipment installed in battery rooms, but does not set specific limits on hydrogen level, ventilation volumes, or air changes per hour.

Telcordia

- Telcordia GR-3028-CORE (2001), Thermal Management in Telecommunications Central Offices: Thermal GR-3028-CORE:
 - This is a requirements document for thermal management in telecommunications access provider central offices. It provides thermal management information, guidelines, targets, objectives, and requirements for equipment manufacturers and service providers for ensuring network integrity while leaving room for innovative equipment designs and environmental solutions;
 - The document also classifies and reports relevant attributes of both the electronic equipment and the equipment room so that manufacturers understand the various environments in which the equipment will be deployed, and so that the service providers understand the equipment attributes for successful deployment of new telecommunications systems.
- Telcordia GR-63-CORE (2006), NEBS Requirements: Physical Protection:
These criteria are requirements and objectives for personnel safety, property protection, and operational continuity. NEBS compliance is a critical issue to service providers in evaluating the suitability of products

This page intentionally left blank

11 Fire Protection

11.1 Introduction

Fire protection regulations differ between countries and the designer must use the appropriate local codes and standards. The following section describes the best practices in the United States and can be used for guidance in other locations as, whilst the codes and standards may differ, the safety philosophy and best practices employed will be similar.

11.2 Basic design elements

The basic design elements of fire protection are:

- Fire suppression—extinguishing systems to protect the data processing equipment;
- Fire detection—smoke, heat, and early warning detectors connected to an alarm and monitoring panel;
- Fire alarm system—a system, including the fire detection systems, with a means to automatically send alarm, supervisory and trouble signals to a central station, security center, fire department, or other approved, constantly attended location, and warn occupants of the presence of smoke, heat, or fire through the use of audible or visual alarms.

11.3 General requirements and recommendations

11.3.1 Requirements

The computer room shall be separated from other areas or occupancies within the building by fire-resistance-rated construction. Refer to Table 4 (Section 7) for minimum fire rating of spaces.

The computer room shall have a fire protection system. If the computer room is located in a sprinklered building, the computer room shall be likewise protected with a sprinkler system. If the data center is a standalone facility (not part of a larger building) or is located in a nonsprinklered building, the computer room shall be protected with either a sprinkler system or a gaseous clean agent system or both a sprinkler system and a gaseous clean agent system.

The basic fire suppression system in a computer room shall be a fire sprinkler preaction system. The sprinkler system for a computer room shall be valved separately from other sprinkler systems. Valves controlling water to the computer room sprinkler system shall be labeled and easily identified as separate from those controlling sprinkler water to the rest of the building.

Sprinkler heads shall be flush-mount pendant type if there is a suspended ceiling. The sprinklers shall be installed per applicable local codes, standards, and regulations.

Halocarbon clean agent systems, including Halon 1301, shall not be used to protect under an access floor unless the space above the access floor is likewise protected by the same halocarbon gaseous fire suppression system.

Any furniture in the computer room shall be constructed of metal or nonflammable materials. However, chairs may have seat cushions made of flame retardant material.

Tapes and records shall be in a separate room with a fire suppression system and with fire rated construction separating these rooms from the rest of the computer room and from any adjacent occupancies that are not part of the computer room. See Section 7 for further information regarding fire resistant construction.

Automated tape libraries or other types of automated information storage system (AISS) units shall have a gaseous agent fire suppression systems installed within each unit if there are more than 0.76 m³ (27 ft³) of tapes or other combustible media.

Combustible materials shall not be stored in the computer room.

11.3.2 Recommendations

The fire detection system should include an early warning smoke detection system and a water leak protection system.

When practical, the sprinkler system should have an alternate water source to prevent a single point of failure and to allow maintenance.

Where it is critical to protect electronic equipment in the computer room, a gaseous, clean agent system dedicated exclusively to the computer room should be considered in addition to any required fire sprinkler system and, when used, it should be configured as the system that is activated first. While overhead water sprinklers provide excellent protection for the building structure, water from sprinklers will not reach fire located within ITE cabinets. Gaseous agent extinguishing systems provide “three dimensional” protection of spaces within equipment enclosures and are capable of suppressing fire in circuit boards and internal components.

If the entire facility is not protected with a gaseous clean agent system, it is a best practice to protect space under access floors with a dedicated inert gas clean agent system or a carbon dioxide total flooding system. Carbon dioxide should normally not be used above the access floor in computer rooms.

Computer rooms should not have any trash receptacles. All unpacking should occur outside the computer room and any trash in the computer room should be promptly removed.

Data center personnel should be trained on the use and function of the fire detection and extinguishing systems of the computer room.

Paper should be stored outside the computer room with a fire suppression system separate from the one used by the computer room.

11.4 Enclosures - walls, floors, and ceilings

11.4.1 Requirements

NFPA 75 gives minimum requirements for the construction of the walls, floors and ceilings of the computer room.

Penetrations through the walls and floor of the room shall be sealed with a fire resistant material that provides a fire rating at least equal to the rating of the wall and floor. Air ducts shall be provided with automatic fire and smoke dampers where the ducts pass through fire rated structure. If pass-throughs or windows are provided in the fire rated walls of a computer room, such openings shall be provided with a fire rated shutter or fire rated window of rating equal to the wall.

Some clean agents such as the inert gas agents will require vents in the enclosure that open during the discharge of clean agent to prevent excessive pressure build up due to the influx of gas in the room. Consult NFPA 2001 and the system manufacturer for guidance.

11.5 Handheld fire extinguishers

11.5.1 Requirements

Hand-held, clean agent fire extinguishers shall be provided as described by AHJ (e.g., NFPA 75, NFPA 10). The fire extinguishers shall be clearly visible. Each fire extinguisher shall be labeled to describe clearly the type of fire on which it should be used.

Extinguishers that use dry chemical agents shall not be used because they will damage electronic equipment.

11.5.2 Recommendations

Switchgear rooms should have clean agent handheld fire extinguishers similar to those used in the computer room.

11.6 Fire protection

11.6.1 Water sprinkler system

11.6.1.1 Wet system

11.6.1.1.1 Introduction

The wet sprinkler system is a method of fixed fire protection using piping filled with pressurized water, supplied from a dependable source. Closed heat sensitive automatic sprinklers spaced and located in accordance with recognized installation standards are used to detect a fire. Upon operation, the sprinklers distribute the water over a specific area to control or extinguish the fire. Wet systems are applied to the noncritical areas of the data center (see Table 14). This system is usually required as a minimum to protect people and property.

As with preaction sprinkler systems, the wet system may require additional water supplies and/or fire pumps if there is not enough water pressure available from utility serving the site (e.g., from the city).

11.6.1.2 Preaction sprinkler system

11.6.1.2.1 Recommendations

The best practice for critical areas is to install a preaction sprinkler system. This type of sprinkler system provides some safeguard against water damage to the data processing equipment due to an accidental discharge.

11.6.1.2.2 Additional information

The sprinkler piping system is similar to the wet system except the piping in the critical areas does not contain water until there is a fire event.

Two events are required before the deluge valve will open and allow water to flow into the sprinkler piping. A single interlock system requires a detection system to operate a valve to flood the fire sprinkler system piping with water. A double interlock system admits water (by opening the deluge valve) in the sprinkler piping upon operation of both

detection and a loss of pressure in the sprinkler piping. Both systems have sprinkler heads requiring a heat rise open the sprinkler head allowing the water to flow. The interlock systems designs are intended to prevent accidental water flow in sensitive areas caused by events such as the accidental operation of a sprinkler head or leaks that may develop in the sprinkler piping. Applicable codes and standards require review prior to the application of either of the interlock systems. The detection systems are smoke, heat and/or other automatic fire detectors such as air sampling detectors or flame detectors.

It is important to note that pendant systems will typically have a column of water in the sprinkler pipe drop from the branch main. The sprinklers should be removed and the pipes drained after system trip testing.

Table 14: Recommended Sprinkler Systems For Data Center Spaces

<i>Area</i>	<i>Sprinkler system</i>
Computer room	Preaction sprinkler system
Network operations center	Preaction sprinkler system
POP	Preaction sprinkler system
Office	Wet sprinkler system
Electrical switchgear	Preaction sprinkler system
Battery and UPS rooms	Preaction sprinkler system
Generator rooms	Dry sprinkler system
Chiller room	Wet sprinkler system
Back of house	Wet sprinkler system

NOTE: AHJ requirements may supersede these recommendations

11.6.1.3 Fire protection interfaces

11.6.1.3.1 Additional information

Interfaces to the fire protection system include:

- fire detection/control/alarm;
- building automation system (BAS);
- security/guard station;
- electrical power control and monitor system;
- EPO (emergency power off) system.

11.6.2 Gaseous fire suppression

11.6.2.1 Clean agent gaseous system

11.6.2.1.1 Introduction

Because of the expense involved with replacing the data center equipment and the difficulty of water from overhead sprinklers to reach fire within ITE cabinets, building owners may consider a gaseous fire suppression system. Typically, chemicals referred to as “Clean Agents” are utilized with the design requirements discussed in NFPA 2001, “Standard on Clean Agent Fire Extinguishing Systems.” These chemicals are stored in pressurized cylinders in or near the computer room to keep pipe lengths short. The system is usually designed to fully discharge within 10 to 60 seconds from initiation.

Fire suppression is achieved by developing an extinguishing concentration of the clean agent in the fire zone.

11.6.2.1.2 Requirements

Where clean agent gaseous fire suppression systems are used, the extinguishing concentration shall be maintained long enough for the materials that have been heated by the fire to cool sufficiently so that the fire will not reignite. NFPA 2001 requires that 85% of the design concentration be maintained at the highest level of combustibles in the protected space for at least 10 minutes or for a time period long enough to allow for response by trained personnel.

Protection shall extend to all areas of the computer room within the fire rated envelope. If a separate gaseous agent system is provided for protection of the space under an access floor, it shall be arranged to discharge simultaneously with the gaseous agent system protecting above the access floor.

Subject to the approval of the AHJ, gaseous agent systems may be provided to discharge gas within specific ITE enclosures. Such protection is typically used for automated information storage systems such as automated tape libraries.

11.6.2.1.3 Additional Information

The air sampling pipe network is a system of pipes installed above or below the access floor with strategically placed air sampling ports. Sample piping material must be approved for use in air plenums when installed in return air ceilings or under raised floors in accordance with the requirements of the AHJ.

Due to restrictions imposed by the Montreal Protocol (1987), the production of halons has stopped in the industrialized world. Existing Halon 1301 systems may continue in usage unless prohibited by local laws. The installation of new Halon 1301 systems is no longer recommended.

11.6.2.2 System controls

11.6.2.2.1 Introduction

In a gaseous fire suppression system, an automatic fire detection system activates the release of the gas. Two-detector actuations are used to minimize false discharges.

11.6.2.2.2 Requirements

Upon initiation of a stage 2 alarm, system controls shall activate an adjustable time delay prior to activation of the actual release of the suppression gas. During this time delay, manual operation of an abort control station can halt the release of the gas, if necessary. The abort station shall be located inside the computer room and be a “dead man” type switch.

Manual release control stations and abort control stations shall be located at the exit doors.

11.6.2.2.3 Recommendations

Actuation of one detector should initiate a stage 1 alarm consisting of audible alarms and automatic notification to the central station or fire/security monitoring system.

Actuation of a second detector should initiate a stage 2 alarm consisting of an audible alarm that is distinct from the first stage alarm. Discharge commences after a time delay of no greater than 30 seconds, subject to approval by the AHJ.

The abort station should not restart the discharge delay sequence.

A land line telephone and fire extinguisher should also be located at each exit and emergency station. A land line is an analog line served directly by the service provider and that bypasses owner’s PBX.

11.7 Fire detection

11.7.1 Area requirements

Table 15: Recommended Detection Systems For Data Center Spaces

<i>Area</i>	<i>Detection system</i>
Computer room	Incipient or early warning intelligent
Network operations center	Incipient or early warning intelligent
Entrance room	Incipient or early warning intelligent
Office	Ionization/photoelectric
Electrical switchgear	Ionization/photoelectric
Battery and UPS rooms	Ionization/photoelectric
Generator rooms	Thermal or flame detectors
Chiller room	Ionization/photoelectric
Back of house	Ionization/photoelectric

NOTE: AHJ requirements may supersede these recommendations

11.7.2 Detector technology

11.7.2.1 Addressable systems

11.7.2.1.1 Recommendations

Provide an addressable, multiplexed, microprocessor-based, electrically supervised fire alarm system for the facility. Design the system to AHJ requirements.

11.7.2.2 Design considerations

11.7.2.2.1 Requirements

The smoke detection system shall be designed to automatically control air supply and exhaust systems and shall be interfaced with the building automation system. Where required, duct-type smoke detectors shall be provided in all ventilation systems.

Smoke detector spacing shall conform to NFPA 72. The air velocity of the HVAC system needs to be considered and may cause this spacing to be reduced.

11.7.2.2.2 Additional information

Ionization type detectors are designed to be installed in areas of low air velocity and are not recommended for computer rooms.

Photoelectric type detectors are designed to be installed in areas of higher air velocity. Smoke detectors located in ducts and air plenums should be rated and clearly labeled for use in high air velocity applications.

Incipient air sampling systems are not normally affected by the air velocities found in a typical computer room. Incipient stage fire detection located at the CRAC return air grills provides the most reliable detection. Sample points can be provided in the exhaust air stream from critical pieces of equipment to provide very early warning of equipment overheat.

In many cases, the CRAC can be provided with supplemental built-in smoke detectors intended strictly for internal CRAC system controls. When such devices are intended to comply with fire alarm code requirements for the building, the detectors will need to be interfaced with the BAS and/or the fire alarm system.

11.7.2.3 Addressable system – non-data floor conditions

11.7.2.3.1 Requirements

The system shall provide:

- smoke detectors in all unoccupied spaces;
- audiovisual notification appliances to meet local code requirements;
- manual pull stations at all exit doors;
- connections from flow/tamper switches to the fire alarm system;
- the required interface(s) with security system. Upon activation, the fire alarm system shall release all security doors;
- monitoring of fire pump and generators, if provided.

Fixed temperature heat detectors or flame detectors shall be provided in generator rooms. Coordinate the temperature set point with the sprinkler system operation parameters so that the heat detectors will actuate first.

Smoke detectors shall be provided in conjunction with magnetic door holders, where applicable.

Firefighters' control panel, graphic smoke control panel (if required), printer and annunciator shall be located at the main security office.

11.7.2.4 Addressable system—data floor conditions

11.7.2.4.1 Requirements

Photoelectric and ionization-type smoke detectors shall be provided in computer rooms and in UPS equipment and battery rooms. Cross-zoned smoke detectors are to work in conjunction with the preaction sprinkler system and the clean-agent fire suppression system.

11.7.2.4.2 Additional information

When an access floor is present in the computer room, photoelectric type detectors may be installed below the floor and may be required by the AHJ.

11.7.3 Early warning detection systems

11.7.3.1 Incipient (air sampling) systems

11.7.3.1.1 Recommendations

In areas where maximum fire protection is required, early warning or incipient type systems should be installed at selected computer room and entrance room locations.

11.7.3.1.2 Additional information

Early warning or incipient type systems can be up to 2000 times more sensitive than conventional spot type detectors.

Consideration needs to be given regarding the level at which incipient systems are used with these systems, as premature activation should be avoided.

Incipient control panels may be installed at several locations and connected to the fire alarm control panel.

The air sampling pipe network is a system of copper or PVC pipes installed above or below the access floor with strategically placed air sampling ports. When mounted under an access floor the pipes are mounted to floor support pedestals with nonconductive supports midway between data and power raceways.

If added protection is desired, sampling pipes may be run above the ceiling or surface mounted to structures where no ceiling is provided.

11.7.3.2 Early warning intelligent detectors (alternative to incipient)

11.7.3.2.1 Additional information

A class of (spot) detectors provided by several manufacturers is able to detect conditions at the early stages of a fire. The early warning detectors utilize a combination of laser, infrared or thermal technology.

The detectors are addressable, which allows for multiple detector protection for preaction sprinkler and gaseous suppression systems.

The detectors utilize a processing capability to both learn and automatically compensate for actual conditions.

The detectors should be installed according to codes and manufacturer's recommendations for air velocity and other conditions.

11.8 Labeling and signage

11.8.1 Requirements

All devices shall be labeled with the fire alarm circuit, zone or address.

Junction boxes shall be painted red or as required by AHJ.

11.8.2 Recommendations

Labeling and signage requirements for the fire protection system include the following:

- Emergency procedures should be posted on all fire alarm control panels and annunciator panels.
- Fire alarm manual stations should be clearly labeled to avoid any confusion. Where permitted, install a cover over these manual stations to avoid accidental triggering.

11.9 Testing and quality assurance

11.9.1 Requirements

Startup and commissioning for the fire protection system shall follow those required by applicable standards, regulations, and the AHJ (e.g., NFPA 72, NFPA 2001).

11.9.2 Recommendations

Preaction sprinkler systems should be trip tested at least once every three years.

11.10 Ongoing operations

11.10.1 Requirements

Site operations and maintenance for the fire protection system shall follow as a minimum those required by applicable standards, regulations, and the AHJ (e.g., NFPA 72).

11.10.2 Recommendations

Clean agent systems should be maintained in accordance with NFPA 2001.

11.11 Reference

References used in this section and their uses are:

- NFPA 12, *Carbon Dioxide Fire Extinguishing Systems*, provides criteria for purchasing, designing, installing, testing, inspecting, approving, listing, operating, maintaining carbon dioxide systems;
- NFPA 12A, *Halon 1301 Fire Extinguishing Systems*, provides criteria for purchasing, designing, installing, testing, inspecting, approving, listing, operating, and maintaining, halogenated agent extinguishing systems (Halon 1301);
- NFPA 13, *Sprinkler Systems*, provides for the protection of life and property from fire through standardization of design, installation and testing requirements for sprinkler systems;
- NFPA 20, *Installation of Stationary Pumps for Fire Protection*, provides for the protection of life and property from fire through standardization of design, installation and testing requirements for stationary fire pumps;
- NFPA 72, *National Fire Alarm Code*, defines the means of signal initiation, transmission, notification and annunciation; the levels of performance; and the reliability of various types of fire alarm systems;
- NFPA 75, *Standard for the Protection of Information Technology Equipment*, sets forth the minimum requirements criteria for purchasing, designing, installing, testing, inspecting, approving, listing, operating, and maintaining engineered or pre-engineered clean agent gaseous fire extinguishing systems developed to replace Halon 1301;
- NFPA 2001, *Standard on Clean Agent Fire Extinguishing Systems*, provides for the application of certain classes of clean agents because of the restrictions established by the 1987 Montreal Protocol;
- *Fire Protection Handbook*, 2003 Edition (NFPA,)
- *Fire Protection System for Special Hazards* (NFPA 2004), provides information on fire detection and suppression systems for specialized occupancies;

This page intentionally left blank

12 Security

12.1 General

12.1.1 Introduction

The purpose of this section is to define the physical security practices and countermeasures necessary to protect the confidentiality, integrity and availability of the data center. Many companies are now creating dedicated data center structures and/or areas, permitting them to become private or semiprivate space, and allowing the operator much more control over the physical security of the structure, the equipment and the people who work in it.

12.1.2 Requirements

The requirements in this standard shall apply to all existing data centers; all new construction, renovation, alterations, remodeling or expansion of any site, building shell, data center or computer room.

12.2 Physical security plan

The physical security plan provides security for data center staff, contractors and visitors along with the ITE, network technology, telecommunications assets, and the sites and buildings that house them. A physical security plan shall be created and followed for the data center and the entire building and/or campus where it is located.

12.2.1 Recommendations

During construction on any existing data center, temporary security measures should be put in place.

12.2.2 Additional information

There is no guarantee of security implied, however compliance with the requirements listed in this section should provide the most acceptable level of security.

No single countermeasure provides effective security. All architectural, operational, and physical security measures (see Figure 51) are intended to do one or more of the following individually and collectively:

- Delay
- Deter
- Detect
- Decide
- Act

12.2.2.1 Physical security in data center

Modern data centers are composed of layers of technical, administrative support and end user space supporting a large computer room with vast amounts of processing and storage capability. Depending on the number and types of potential threats, providing physical security for the data center can encompass the full range of security needs for the site, zones, buildings, rooms, and areas, including;

- Access control devices.
- Architectural design.
- Barriers.
- Detection and alarms.
- Guard services.
- Surveillance.

12.2.2.2 Physical and IT security

Historically the policies, design, practices, technology and personnel utilized to protect physical assets have been separate from those used to protect IT and its data. The increasing use and importance of devices that create data when combined with the increasing sophistication of the attacks and frequency of attempts to capture or compromise that data requires a move toward a more holistic type of security, will require the data center operator to consider both physical and IT countermeasures.

12.2.2.3 Cyber/IT security plan

The cyber security plan provides security for data at rest and data in motion, and protects it from attempts to defeat its confidentiality, integrity or availability through electronic means. Cyber security plans are beyond the scope of this section.

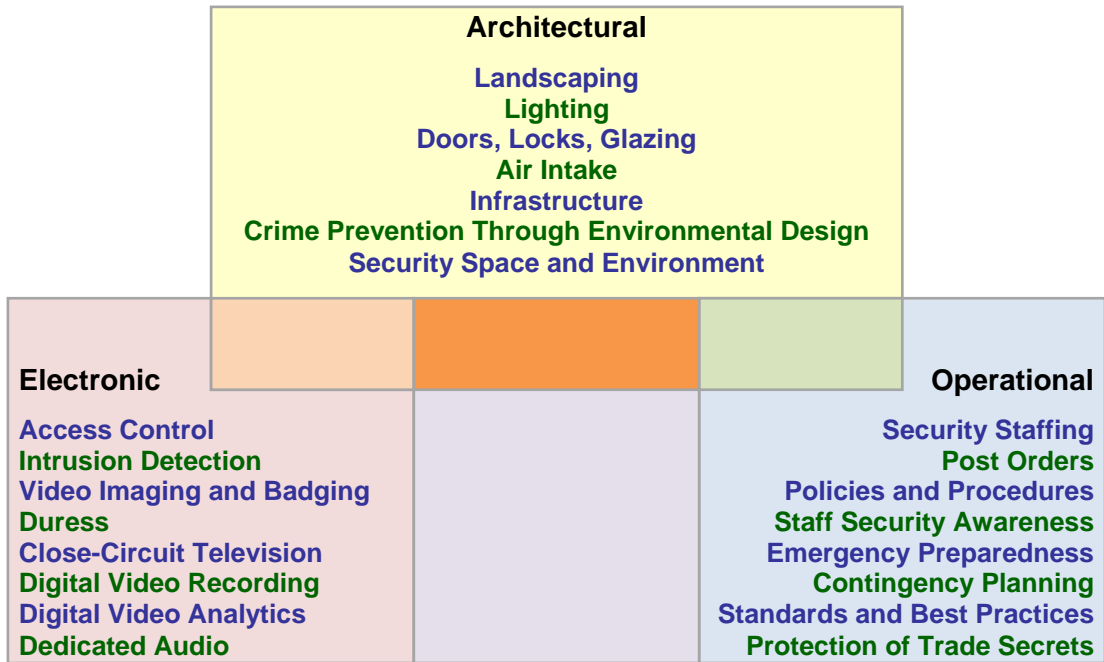


Figure 51: Security Measures

12.3 Risk and threat assessment

12.3.1 Definitions

Definitions that apply specifically to risk and threat assessment follow. These definitions only apply to the security section of this standard.

- Asset: an employee, contractor, or any physical, technological or intellectual possession.
- Countermeasures: the procedures, technologies, devices or organisms (dogs, humans) put into place to deter, delay or detect damage from a threat.
- Risk: the likelihood that a threat agent will exploit a vulnerability creating physical or technological damage.
- Threats: the agents by which damage, injury, loss or death can occur; threats are commonly classified as originating from temperature extremes, liquids, gases, projectiles, organisms, movement or energy anomalies.
- Vulnerability: a physical, procedural or technical weakness that creates and opportunity for injury, death or loss of an asset.

12.3.2 Recommendations

12.3.2.1 Security survey/analysis

Every data center should have a complete security survey or analysis during the preplanning and planning stages of construction, then annually upon occupancy. The security consultant, architect or engineer should assess the following metrics and provide written recommendations.

- the identification of assets;
- the identification of natural, technological and human threats;
- the probability of risk;
- the past and future losses of the complex or building;
- the potential impact of losses and risk;
- possible countermeasures;
- cost/benefit analysis of proposed countermeasures.

12.4 Regulatory requirements and legislation

12.4.1 Recommendations

Security training should include topics regarding industry-specific regulatory and best practices leading to compliance with them.

The physical and cyber security plans should contain requirements that support regulatory compliance.

12.4.2 Additional information

The law requires the protection of sensitive data and the computer equipment in which is stored or by which it is processed or transported. Depending on the size of company and IT dependence, compliance with government regulations should have a positive impact on document management, storage management and the establishment of record retention schedules.

12.4.2.1 Regulation or laws affecting security

The regulatory and legal requirements affecting the operation of a data center will vary widely between countries, regions and localities. The data center owner and operator should be familiar with all legal and regulatory requirements concerning privacy, purposeful or accidental disclosure of financial, medical or personal data, and national security. Some examples of regulatory and legal documents affecting the operation of the data center include:

- Sarbanes-Oxley;
- industry-specific standards;
- US Patriot Act;
- Federal Information Processing Standards (FIPS);
- Health Insurance Portability and Accountability Act (HIPAA);
- Gramm-Leach-Bliley (GLB);
- National Assoc. of Security Dealers Conduct Rules 3010, 3013 and 3110;
- European Privacy Standards.

The primary purpose of these rules and regulations are to protect investors, shareholders, employees and the public from a variety of violations ranging from accidental disclosure of personal information through the pending collapse of the corporation.

Data center operators and security architects and designers should avoid viewing these laws and regulations mechanistically, or as a checklist. They should be viewed and approached as a top-down risk assessment.

12.5 Data center security plan

12.5.1 Recommendations

12.5.1.1 General

The data center security plan should be comprehensive, but easy to read and understand.

The data center security plan should be reviewed and updated as follows:

- once annually;
- following any major construction or remodeling project of the data center and related spaces;
- following any major construction or remodeling when the data center is located in a multitenant building or campus;
- following any major breach of security or disaster;
- when a change in local, regional or national security events warrant.

Prior to creation of a data center security plan, the data center operator, security architect or designer should conduct a thorough risk assessment of the existing or future site, buildings and demographics of the data center.

The data center security plan should address all areas of potential risk identified during security survey.

The data center security plan should address departmental responsibility for each plan element, including:

- administration;
- cyber security;
- facilities;
- finance;
- human resources;
- information technology;
- physical/plant security;
- purchasing;
- operations.

The data center security plan should detail the roles and responsibilities that IT/network security can play in supporting the physical security procedures.

The data center plan should detail policy providing that countermeasures should be selected and deployed from the following sections, utilizing the following criteria:

- protection of the life and safety of occupants;
- protection of physical assets;
- protection of electronic assets.

The data center security plan should address departmental responsibility for implementing the plan, including:

- administration;
- cyber security;
- facilities;
- finance;
- human resources;
- information technology;
- physical/plant security;
- purchasing;
- operations.

All employees should receive training on all relevant aspects of the security plan. This training should be done during orientation and periodically refreshed during their employment. Training should include penalties for failure to follow the security plan.

12.5.1.2 Access control policy and procedures

The control of access to the data center should be addressed by the security plan. Questions answered by the security plan should include:

- who has access to the data center, and during what hours;
- if the data center occupies the entire building, how is the security for public areas, loading docks, utility areas, offices, and meeting areas addressed;
- if the data center occupies only a part of the building, how is security to be addressed for common areas with other tenants, elevators, storage areas, risers and common telecommunications areas;
- how is access granted;
- how are visitors and contractors managed;
- how are breaches in security policy dealt with;
- is there a space programming standard that specifies recommendations or a template for each type of space;
- do some areas, such as the computer room, prohibit sole occupancy by an employee or contractor;
- how are service providers monitored when working in the facility;
- do access control procedures change during nonbusiness hours;
- what types of doors and locks are used for each type of area:
 - public;
 - semipublic;
 - semiprivate;
 - private.
- how are keys managed.

12.5.1.3 Badging policy and procedures

The security plan should require the use and display of badges for all employees.

The security plan should require the use of temporary identification badges for all visitors, contractors and delivery personnel.

All temporary identification badges should have some visible method by which employees, security, and law enforcement personnel can easily determine whether the badge has expired. Possible methods for ensuring that expired badges are not reused include:

- a rotating color scheme;
- the expiration date printed on the badge;
- the day of the week printed on the badge;
- use of self-adhesive tokens that gradually expire over a predetermined period, typically one day;
- use of badges that gradually expire over a given period, gradually displaying bars some other visually distinctive method.

The security plan should specify how the visitor, contractor or delivery person should wear or display the identification badge.

If employees are required to wear identification badges, the visitor, contractor or delivery person badges should be different from those of employees.

The security plan should address how identification badges will identify those visitors, contractors and delivery personnel who must be escorted.

12.5.1.4 Signage and display policy and procedures

The security plan should identify the wording, readability and location of signage and displays intended to control pedestrian and vehicular traffic from straying into unauthorized areas.

12.5.1.5 Fire prevention, detection and suppression

The security plan should contain policy on the type and location of fire suppression equipment.

The security plan should contain policy on what type of protective containers should be used for sensitive material. This may include the reference to or specification of fire-resistance standards.

The security plan should contain policy on the storage of combustible chemicals and materials.

The security plan should contain policy and procedure for the fire rating of any containers found in sensitive areas, such as trash receptacles.

12.5.1.6 Monitoring and alarm, policy, and procedures

The data center should have written guidelines for evaluating emergency responses to all alarms.

The security plan should specify what types of alarms or monitoring systems are used for controlling access to certain areas or devices. Areas of particular concern should be:

- common cross-connect spaces;
- common riser closets;
- computer room;
- elevators and stairwells;
- entrance facilities;
- administrative, HR, and finance departments;
- offices;
- plenum and ceiling spaces;
- telecommunications spaces;
- utility rooms and closets;
- vehicular and pedestrian gates.

The security plan should address who has access to alarm codes to turn off or bypass systems.

The security plan should state the policy on when codes are changed due to terminated employees, contractors or contract personnel, such as janitorial.

The security plan should address the issuance of unique codes, or groups of codes to employees, contractors or contract personnel.

The security plan should coordinate with the cyber/IT plan how live data and telephone jacks in public or semipublic areas are monitored and secured against unauthorized access. This would include common building areas such as riser closets, common cross-connect areas, entrance facilities and service provider areas.

When applicable, the security plan should coordinate with the cyber/IT security plan, the policy for alarming and monitoring of computers cases, server cases, and cabinets against the unauthorized access to or removal of discreet components or equipment.

Alarm company and security service providers should be monitored when working on surveillance and alarm systems. The security plan should detail policy and procedure to ensure that only authorized service is performed on alarm and surveillance equipment by requiring 24 hour advance notice of the employee's name and other identification information, or similar.

12.5.1.7 Material control and loss prevention

The security plan should address:

- all aspects of material control and loss prevention both in and out of the data center site, campus, buildings, parking garages, and office areas;
- which materials, including ITE, employees are authorized to bring into and take out of the data center and inspection procedures;
- which materials, including ITE, visitors, and contractors are authorized to bring into and take out of the data center and inspection procedures;
- the inspection and receiving procedures for all deliveries, including authorized points of unloading and authorized personnel authorized to receive deliveries;
- approved methods for disposal of printed materials and magnetic or other media.

The security plan should state the policy, inspection procedures and penalties for unauthorized transport or use of removable media, such as thumb drives, tapes, optical disks, or removable hard drives. This should be complimentary to any existing cyber/IT security policy.

The security plan should specify when property tags, electronic tags and other identification systems should be affixed to data center equipment and assets.

12.5.1.8 Surveillance policy and procedure

The data center should have written guidelines for evaluating emergency responses to all CCTV alarms or incidents.

The security plan should detail:

- policy for the location and placement of surveillance equipment, including special circumstances noted during the risk/threat assessment process;
- the policy and procedure for the protection and secure placement of surveillance devices within offices, work areas, elevators, loading docks, lobbies, parking garages, and exterior areas of the data center;
- who can authorize special surveillance, covert surveillance or placement of new CCTV equipment;
- the secure placement, storage and disposal of surveillance tapes and recorded media (servers, storage, and DVR).

12.5.1.9 Disaster recovery

Definitions as defined by NFPA 1600, the Standard on Disaster/Emergency Management and Business Continuity Programs:

- natural events, including drought, fire, avalanche, snow/ice/hail, tsunami, windstorm/tropical storm, hurricane/typhoon/cyclone, biological, extreme heat/cold, flood/wind-driven water, earthquake/land shift, volcanic eruption, tornado, landslide/mudslide, dust/sand storm, and lightning storm;
- technological events, including hazardous material release, explosion/fire, transportation accident, building/structural collapse, power/utility failure, extreme air pollution, radiological accident, dam/levee failure, fuel/resource shortage, strike, business interruption, financial collapse, and communication failure;
- human events, including economic, general strike, terrorism (ecological, cyber, nuclear, biological, chemical), sabotage, hostage situation, civil unrest, enemy attack, arson, mass hysteria, and special events.

The security plan should include the development of detailed plans for the notification, response and emergency operation of the data center following a natural, technological or human disaster.

The data center operator, security architect and designer should work with other departments and plans to identify asses and mitigate any foreseeable natural or other disasters. The security plan should whenever possible focus on prevention and mitigation to threats.

The security plan should put into place systems, process and procedures prior to a disaster that will enable the data center to:

- prepare for natural, technological or man-made events;
- respond to disasters;
- recover from disasters;
- work with civilian or military authorities during a disaster.

The security plan should protect detail measures to protect the following:

- health and safety of data center or campus occupants at the time of the disaster;
- health and safety of emergency services and disaster aid personnel responding to the incident;
- ability for the data center to continue operations;
- condition and usability of the site, campus, building(s), critical and telecommunications infrastructure;
- utilities and telecommunications services;
- the environment;
- economic and financial condition of the company;
- regulatory and contractual obligations;
- company's reputation.

The security plan should identify the approved and/or contractual civilian and governmental resources for mutual aid in the event of a disaster.

The disaster recovery section of the security plan should be reviewed and updated at least once per year or following any of the following events:

- identification of new hazards;
- regulatory changes;
- reorganizations or down-sizing;
- disasters;
- disaster preparedness drills;
- major changes on the site, campus, or building;
- changes in the venue of the data center (e.g., annexation into a city)

12.5.1.10 Personnel

The security plan should detail all hiring and termination procedures, which may affect the safety and security of the data center, its occupants, facilities, ITE, and other assets.

In cooperation with Human Resources policy and procedure, the security plan should detail mandatory information needed from each applicant, including:

- name and variations (verified);
- correct address;
- citizenship;
- military record;
- references;
- any security clearances;
- previous education;
- employment history;
- background information regarding spouse and relatives;
- criminal convictions;
- organizational affiliations;
- previous residences.

The security plan should detail policies and procedures ensuring that essential information needed from an applicant and/or employee is obtained from a legally binding application, including the appropriate authorization for investigation and release of information forms.

The security plan should include details on applicant screening procedures, background investigation standards, employee conduct and termination procedures.

The security plan should include recommendations for additional preemployment screening for certain positions, which might include psychological, skills and aptitudes or integrity tests.

The security plan should require that all data center employees have an exit interview. Exit interviews can enhance security by:

- reducing the loss of confidential information and trade secrets through discussion of nondisclosure agreements and potential penalties;
- discovering problems that existing employees can't or won't reveal;
- reducing loss of data center property through the use of checklists;
- gives the employee a chance to express grievances, reducing the possibility of vandalism, sabotage or violence.

12.6 Crime prevention through environment design

12.6.1 Recommendations

The crime reducing concepts and strategies of Crime Prevention through Environmental Design (CPTED) should be followed during the planning process of the design or retrofit of a data center. There are three underlying principles of CPTED. They are 1) Natural Access Control, 2) Natural Surveillance and 3) Territorial Enforcement.

12.6.1.1 Natural access control

The data center security architect or designer should utilize natural access control (e.g., placement of doors, fences, lighting, landscaping, other natural or architectural features) to guide pedestrian traffic as it enters and leaves the site, campus, building, or a room or space inside the building.

Each data center room and area should be classified by the level of protection required based upon the sensitivity of the equipment or activity in occurring there. Each area of a data center, including all support areas, closets, utility and service provider areas, loading docks, lobbies, and offices, should be classified into one of the four basic CPTED space types:

- public, used to designate areas that are available for all pedestrian traffic. public areas would include lobbies, dining areas of restaurants or cafeterias, parking garages and hallways or sidewalks.
- semipublic, which is a term describing areas that are usually accessed from public areas, but not available to everyone. these areas might include conference rooms, restrooms or break areas.
- semiprivate, a term used to classify space where natural, physical or electronic access control is used to control pedestrian traffic. Semiprivate areas would include general office space, walled offices not used for sensitive work, private floors in a multitenant building, utility rooms, and TRs.
- private spaces, those that are restricted from most pedestrians, including unauthorized employees. Typical private areas might include the computer room of a data center, a bank vault, a surgery suite, and the executive floor of an office tower.

The concept of natural access control can be found in the following practices, which should be considered during any data center design:

- place lights and attractive landscaping along the main sidewalk leading to the front door of the business.
- place vegetation so that there is a clear line of sight only to the desired entrance of a building.
- use lakes, rocks, hills and vegetation to reduce the number of potential entrances onto a data center site, campus or building.

12.6.1.2 Natural surveillance

The concept of natural surveillance relies on the use and placement of physical environmental features, walkways, open spaces, pedestrian traffic patterns and work areas to maximize visibility of the activity within an area by those outside of it, and outside the area by those inside it.

Data center security designers should design the rooms, areas, spaces, walkways, and site so that there are many ways for observers to see unauthorized traffic, activity or criminal behavior. As much as possible, all areas of the data center buildings and site should make the occupants feel safe and comfortable.

12.6.1.3 Territorial reinforcement

The concept of territorial reinforcement is to create a sense of community or belonging so that if an unauthorized person strays or intentionally enters the area, they both feel out of place and is easily identified as being such.

The data center security designer should ensure that the atmosphere contributes to a sense of territoriality. The secure space should produce the feeling or sense of proprietorship or territorial influence, so that potential offenders perceive this and are discouraged from entering or offending. One way to accomplish territorial reinforcement is to create clear borders between controlled and public spaces, so that potential offenders must cross into an unauthorized area in full view of authorized occupants.

12.7 Access control

12.7.1 Requirements

All access control systems must allow emergency egress of the facility in compliance with applicable building codes. The facility designer shall review the applicable life safety code requirements with the AHJ and comply with all AHJ requirements, which can vary from one location to another.

12.7.2 Recommendations

12.7.2.1 General

Access to the data center should be restricted to authorized employees, contractors, or visitors using one of the following methods:

- security guards, receptionist, or other personnel;
- card reader systems;
- biometric devices.

Access control designs should support one or more of the following objectives:

- permit or deny entry;
- alter the rate of movement within certain areas;
- protect occupants, materials, and information against accidental or malicious disclosure;
- prevent injury;
- prevent damage.

All building access points, including maintenance entrances, equipment doors, and emergency exits, shall use some form of access control.

Methods of authentication should include one or more of the following:

- Type 1: What a person has (e.g., keys, cards)
- Type 2: What a person knows (e.g., passwords, codes)
- Type 3: What a person is (e.g., guard recognition, biometric data)

When possible, the computer room and other high-value or sensitive areas of the data center should require multifactor authentication, with biometric data utilized as one of the factors. An example would be a two-factor authentication scheme for the computer room where both fingerprint scan and proximity card are required to enter.

A list should be maintained of the employees and contractors that have been issued keys, magnetic cards, codes, tokens and badges so that the devices can be confiscated upon termination, confiscated upon change of responsibilities, or to permit the access control codes to be changed. It is important that HR or the department for which an employee or contractor worked, immediately notify the “owner” of all access control systems (IT, facilities or security) when an employee or contractor is terminated, or no longer requires access to all areas for which they were/are authorized.

Access control should be coordinated with emergency services personnel with each local agency, including police, fire, and EMS. Access during emergencies should be immediately granted regardless of the day or time, utilizing any one of the following:

- rapid entry key systems (such as Knox-box);
- preissued cards, badges, tokens or codes;
- combination locks, vaults, cabinets;
- electronic key retention units;
- other locally approved methods and devices.

When possible, alarms from access control events should transmit to a local or remote location where timely responses or other actions can be initiated. Typical locations include the following:

- remote contract monitoring company;
- main guard station off-site;
- guard station in another building;
- guard station in the same building.

Where union labor is utilized in the building by the data center corporate enterprise or by another company located in the same building or campus, planning for a labor strike should be included in the security plan, disaster recovery plan and access control systems.

In the event of a strike, the existing hardware or software authentication should be backed up, and the hardware or software authentication (e.g., locks, access control programming) for striking workers should be temporarily disabled or changed.

12.7.2.2 Locking Mechanisms

12.7.2.2.1 General

Locking mechanisms are grouped into two general categories, with a variety of available types and security levels with each one:

Mechanical:

- warded
- lever
- pin tumbler
- wafer tumbler
- dial type combination
- electronic dial type combination
- mechanical block out devices for equipment ports and cords

Hybrid – electrical and mechanical operation:

- electric deadbolt
- electric latch
- electric strike
- stair tower
- electric lockset
- exit device
- electromagnetic lock
- shear lock

The data center security design should include input from the risk, threat and vulnerability assessment before selecting the appropriate locks for each area.

Significantly, planning and analysis should occur during the determination of the types of locking systems to be utilized in the data center. Planning criteria include:

- total number of locks;
- classification of space;
- employee and contractor demographics and turnover;
- type of facility;
- local crime statistics;
- risk/benefit analysis;
- availability and use of other countermeasures.

Both the level of skill needed to attack a locking mechanism as well as the psychological deterrence should be considered when selecting a locking mechanism. Among the vulnerabilities of mechanical locks that must be considered when selecting a locking device are:

- force;
- separation of the door jamb from the door—door jamb and surround wall materials should be strong enough to meet the delay requirements needed;
- length of the bolt – a 25 mm (0.98 in) minimum should be used for all secure areas where risk of attack by force exists;
- inclusion of an astragal or metal plate covering the gap over the location where the latch enters the keeper;
- requiring a hardened plate to cover the exposed lock housing and cylinder;
- high-quality pins in pin tumbler cylinders to prevent snapping of the pins and manual rotation of the plug;
- picking;
- taking impressions of keys;
- Stealing or inheriting keys.

12.7.2.2.2 Mechanical locks

All lock tumblers should be periodically rotated to maintain security as employee and contractor terminations occur. This can be accomplished through rotation of just the tumbler or core, or can involve the removal and rotation of the entire lockset.

Locks and keys should never be used as a primary method of access control for computer room doors or other high-value or sensitive areas.

Key control using a single great grand master process is not recommended. This is especially true with larger facilities.

All keys should be included in a comprehensive key control procedure.

All keys should have the following words molded or engraved into the key body, "DO NOT DUPLICATE".

All keys should be coded.

When possible, keys should be made on special blanks that are not available to others.

All new installations of door locks should comply with regulatory requirements for disabled occupants. One example of this type of requirements is the ADA, which requires the use lever handles instead of doorknobs.

The security designer for the data center facility should consider the function of the lockset as part of the security, ingress, and egress traffic patterns. Functions of locksets are classified as follows:

- Office, where the handle on either side will operate the latchbolt; locking is accomplished using the thumbturn inside the room, or a key on the outside of the room.
- Classroom, where the latchbolt is only operated by the handle inside, or a key outside.
- Institutional, where only a key will operate the latchbolt from either side.
- Corridor, where the same functionality exists as in the office scenario, but the key and thumbturn throw a deadbolt; for safe egress, the inside lever also opens both the deadbolt and the latchbolt.

12.7.2.2.3 Electrified locksets

Electrified locksets should be a key central design element of any data center security plan. These locksets are locked and unlocked remotely and are commonly layered and integrated with other systems in the electronic access control system.

It is important for the data center security designer to consider the operation of the facility during normal and emergency conditions. The ability to utilize either a "fail safe" or "fail secure" condition for each door must take into consideration the location and emergency egress routes for all occupants, as well as the location and risk to high-value equipment and other assets. Failure to design the appropriate lock can create a significant risk of injury or death to occupants due to entrapment, or unauthorized entry due to inadvertent opening of doors to storage areas.

A fail-safe lock is one in which the locking mechanism unlocks under any failure condition.

A fail secure condition is where the locking mechanism remains locked under any failure condition.

It is important that fire codes be consulted for requirements for door locking mechanisms and functions. One example of this is the stair tower lock, which releases a dead-locking mechanism if power is removed, allowing the door handles to be used.

The electromagnetic lock is an important locking mechanism and secures the door by means of a power electromagnet, which is rated by the force required to open the door when it is energized – typically 2200 N (500 lbf) to 8900 N (2000 lbf).

Combinations of more than one lock type are an important design strategy and should be utilized when attempting to maintain security during normal operation, loss of power and emergency conditions.

12.7.2.2.4 Cipher and combination locks

Cipher locks do not have the ability for multiple codes. The use of cipher locks for computer rooms doors and other high-value or sensitive areas is not recommended due to the high probability of compromise due to "shoulder surfing" and the lack of ability to track entry/exit data.

If cipher locks are used on any door, security or other data center personnel should verify that the default setting has been changed.

Cipher lock combinations should be changed at least every 30 days; however 90 days is the maximum time recommended without changing the combination.

12.7.2.3 Doors

In general, the following provisions will apply, except as modified by the AHJ:

All pedestrian doors located within the data center and computer room areas, should comply with the required provisions for egress as follows:

- a sensor on the egress side must unlock the door upon detection of an occupant approaching the door;
- the locking system is fail-safe;
- all doors must utilize listed panic or fire exit hardware that, when operated, unlock the door;
- a request-to-exit (REX) manual release device is provided adjacent to the door unlocks the door that meets the following requirements:
 - has appropriate signage (“PUSH TO EXIT”);
 - directly interrupts of power to the door lock (e.g., is hardwired into the door lock control circuit);
 - when activated, unlocks the door for at least 30 seconds.
- initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset.

When enhanced security is required in the data center or computer room exit doors should be equipped with delayed egress locking systems that do not allow egress for a typical period of 15 to 30 seconds after pressing of the exit device for no more than 3 seconds, with the following provisions:

- initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset;
- initiation of the release process activates an audible alarm and/or visual signal in the vicinity of the door;
- after release, locking shall be by manual means only;
- signage on egress side of door is provided (“PUSH UNTIL ALARM SOUNDS. DOOR CAN BE OPENED IN 15 SECONDS”).

Emergency Exits should be monitored and alarmed if the door is opened for any reason without release from the access control system. The delay period should be determined by the amount of time needed for guard response, surveillance activation or other method activated to monitor the location and reason for the emergency exit alarm.

An interface with the video surveillance (CCTV) system should be provided to permanently archive the buffered video for the period before, during, and after a door alarm condition, to allow security personnel to respond to the incident and investigate the incident.

12.7.2.4 Electronic access control (EAC)**12.7.2.4.1 General**

All electronic access control (EAC) systems should be able to track the movement through access points independently. Each employee should have a unique pin or identification code, card or other physical or electronic method of authentication.

Automated EAC systems should record all of the following:

- entry and exit time;
- identification of the entrant;
- authorization mechanism.

12.7.2.4.2 Touchpads

When keypads are used, they should utilize a high-security approach where each numeral is randomly scrambled to a new position each time the start button is pressed. This way, a bystander cannot see the code, learn the pattern, nor identify telltale wear marks on certain keys to access where the ID code or PIN number cannot be accidentally shared with, or stolen by, onlookers.

When possible, the touchpad should be a hybrid device and contain a card reader or other electronic access control authentication method.

12.7.2.4.3 Card Systems

Card systems for access control provide a unique access/identification card for every individual with access authorization. Card readers are provided at all designated access entrances to the facility, which interface with the security system and door controls to unlock or open doors when a valid card is presented to the reader.

There are a variety of access card technologies and options available today, including:

- barium ferrite;
- embossing readers;
- hollerith readers;
- magnetic stripe;
- optical character;
- proximity;
- RFID;
- smart cards;
- watermark magnetic;
- wiegand wire.

Card access technology should be integrated into the ID badge when possible.

12.7.2.4.4 Biometrics

Biometric authentication refers to technologies that measure and analyze human physical characteristics for authentication purposes. Biometrics is usually used in conjunction with identification card access to decrease database search times and improve reliability. Examples of physical characteristics used by biometric systems include:

- fingerprints;
- eye retinas;
- eye irises;
- facial patterns;
- hand measurements.

12.7.2.5 Special access control applications

All electronic card access systems for the data center should incorporate and have active the ability to detect more than one individual going through a controlled doorway with only one card or biometric authentication. Ultrasonic scanning of the mantrap compartment can verify that there is only one individual entering the facility, and eliminates the ability of unauthorized individuals to piggyback behind an authorized employee, contractor or visitor.

All electronic card access systems for the data center should incorporate and have active the anti-passback feature. This feature should only permit one entry without an accompanying exit. When activated, this feature should not interfere with normal and authorized movement within the data center or computer room, but limit the ability of more than one employee, contractor or visitor to use the card for the same ingress or egress.

In high-value or sensitive areas with restricted access, security designers should consider the use of the “two man rule”. This feature of electronic access control systems requires that at least two authorized persons be in any specified area at the same time. When a restricted room or area is empty, two authorized persons must use their access cards within a specific period, typically 45 seconds, or entry is denied and a log entry or some sort of notification is made.

Mantraps should be designed to provide secure access control with or without the presence of security personnel, and using a combination of two interlocked doors on both sides of a controlled access compartment. Mantraps can utilize card readers, biometric scanners, and ultrasonic scanning of the mantrap compartment to limit the area to a designated number of authorized personnel able to pass into the secured area. Mantraps can be utilized for both entry and exit.

In addition to the access control and intrusion sensors, each mantrap should also have the ability to sense chemical, biological, radiological and nuclear threats within the controlled access compartment.

Sally ports consist of a controlled pedestrian or vehicular interior or exterior space secured with two controlled and interlocked doors or gates. Sally ports operate by allowing personnel or vehicles entering the facility enter the sally port space, and then close the first door before authentication occurs, and the second door is opened to proceed. Security options that should be considered when designing sally ports for the data center include:

- designed to facilitate identity verification and authentication while the vehicle and/or pedestrian is still secured in the sally port space;
- when installed inside a building, sally ports should be able to withstand predetermined levels of explosions;
- provide a safe and isolated location for identification, authentication and inspection
- should have fixed and mobile surveillance to facilitate inspection of vehicles;
- should have normal and emergency communication equipment installed;

- should have a secure room with access to the sally port for interviews without the need to leave the sally port area;
- sally ports can be constructed of a variety of materials, ranging from barriers, like chain link fence for outdoor applications, to explosion resistant glazed material for the in-building designs.

Sally ports should also be used to restrict traffic flow to one at a time to prevent unauthorized entry into the secured space via piggybacking or tailgating.

12.7.2.6 Turnstiles

If turnstiles are utilized to control pedestrian access to secure data centers, the turnstile should be full height and either integrated with the electronic access control system, or monitored and controlled by guards. Half height turnstiles are easily overcome and provide little security if not augmented by guards or other countermeasures.

12.7.2.7 Gatehouses

Considerations when designing and building gatehouses/guardhouses should include:

- must provide unobstructed observation in all directions;
- located in the center of the roadway providing the ability to stop and inspect vehicles entering and exiting;
- sufficient access for the volume of vehicles during shift changes and other busy times;
- traffic arms, pop-up bollards or other mechanisms to effectively control vehicular traffic;
- access control for after hours ingress and egress;
- a turnstile for pedestrian traffic, if no inadequate pedestrian traffic control or sidewalks exist or can't be sufficiently controlled by security staff;
- buffer areas for those without prior authorization, or for handling of employees, contractors or others who have lost or problematic identification badges;
- CCTV surveillance using multiple cameras to monitor and record images of the driver/passengers, front and rear license plate locations, and a general view of the gatehouse and/or gate area;
- at least one concrete-filled bollard at each corner of the guardhouse, at least 1 m (3.5 ft) high. Metal highway barriers are an acceptable alternate;
- bullet resistance in high crime areas.

Remote gatehouse/checkpoint can reduce the number of guards or employees needed to secure a perimeter. If a remote gatehouse/checkpoint is used it should have the following features;

- CCTV surveillance providing images of approaching vehicles, drivers and optionally the gate;
- lighting for after dark operation;
- intercom system;
- a motor operated gate;
- one or more access control systems (cards, biometrics, keypads);
- loop detectors.

12.7.2.8 Badging and identification

Identification badges should be issued by the employer and contain sufficient data to properly identify and authenticate the bearer. Information contained on the badge should include some or all of the following:

- name of the bearer;
- department or division;
- a photograph of the employee, contractor or visitor;
- a physical description of the employee, contractor or visitor;
- special access privileges (computer room access);
- date of issue or expiration.

ID badges should be distinctive and difficult to forge or alter. In addition to the basic information, each ID badge should contain distinctive color symbols.

ID badges should be designed for the foreseeable circumstances for which they may be used in the operation of the data center, including:

- access control;
- meal purchase;
- inventory control;
- time and attendance;
- parking.

All employees should be issued and required to display identification badges.

The data center should charge for replacements for lost badges where no acceptable explanation is provided, or at some multiple of lost badges.

Lost badges that later are found to be used or attempted to be used by the employee, another employee, contractor, or visitor should trigger an immediate investigation.

Badges should be laminated in order to provide the highest level of tamper resistance.

Temporary identification badges should be issued for all visitors, contractors and delivery personnel.

All temporary identification badges should have some visible method by which employees, security, and law enforcement personnel can easily determine whether the badge has expired. Possible methods for ensuring that expired badges are not reused include:

- a rotating color scheme;
- the expiration date printed on the badge;
- the day of the week printed on the badge;
- use of self-adhesive tokens that gradually expire over a predetermined period, typically one day;
- use of badges that gradually expire over a given period, gradually displaying bars some other visually distinctive method (see Figure 52).

Visitor, contractor or delivery person badges should be visually distinctive from those worn by employees.

Identification badges should prominently display which visitors, contractors, and delivery personnel must be escorted.

Digital photos taken at the time of ID badge issuance should be stored securely for later comparison with individual ID badge.

12.8 Alarms

12.8.1 Introduction

Alarms utilize one or more sensor technologies to detect a variety of conditions relevant to the security of the data center. Sensor technology includes:

- audio;
- capacitance;
- electro-mechanical;
- glass break sensors;
- passive infrared (PIR), which detects thermal or infrared images;
- photoelectric;
- ultrasonic and microwave;
- vibration.

12.8.2 Recommendations

12.8.2.1 General

Audio sensors should be used in the data center perimeter to detect and record any sound in a protected area or filter sounds traveling along fencing, or telecommunications conduit to eliminate sounds from traffic or weather and trigger an alarm if impact, cutting, or digging is detected.

Capacitance sensors should be used in the data center to detect changes in electronic fields and are primarily limited to monitoring the electronic field around protected objects.

Electro-mechanical sensors include things like foil, wire and screen detectors, pressure mats, mechanical and magnetic contacts. When used as sensors in the data center they should be installed so that the activity of the intruder causes some movement or pressure triggering an alarm, and can be mounted on or in a wide variety of locations.

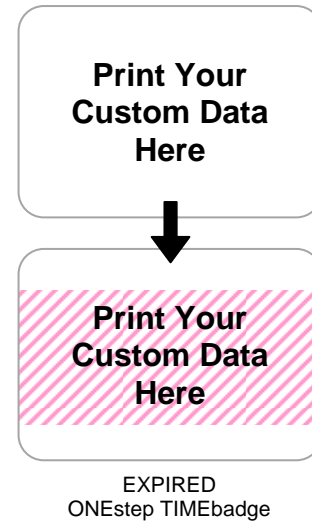


Figure 52: Expiring Badge

Glass break sensors can be installed on a wall or ceiling surface, but to directly receive the sound waves needed to trigger the sensor, they should be mounted directly across from the window being monitored. Some glass break sensors are subject to false alarms from RFI. Glass break sensors used in data center applications should contain technology immune from RFI induced false alarms.

Passive infrared (PIR) sensors in the data center should be installed so that an intruder must pass across its field of view. PIR devices can be used to protect perimeters, areas or objects. This includes areas where barriers or mechanical detectors were historically the only countermeasure available, including skylights and maintenance holes.

Known conditions that create false alarms are:

- rapid changes in temperature;
- bright windows or direct sunlight;
- insects;
- drafts;
- RFI.

Photoelectric sensors installed in the data center or campus should be used indoors or outdoors, in any location where an invisible beam of light is monitored at the receiving end for interruption. False alarms can be triggered by some atmospheric conditions like snow and heavy rain, or in an outdoor environment by animals.

Ultrasonic and microwave sensors operate much like PIR sensors, but substitute sound waves for infrared detection as a trigger. These sensors should be used indoors where the types of movement are limited to protected area such as offices, storage areas, TRs, loading docks and areas of the data center.

Vibration sensors should be placed in locations where there is a possibility of an attempt to penetrate a wall or floor of a safe, vault, storage area or other secure area of the data center.

Other sensors that should be considered for use in and around the secure areas of a data center include the following, which are commonly referred to as CBRNE sensors:

- chemical;
- biological;
- radiological;
- nuclear;
- explosive.

12.8.2.2 Intrusion

Intrusion alarms should be used to detect the presence and/or movement of unauthorized persons at a point of entry, room or general area or in the proximity of an object.

Intrusion alarms should utilize one or more of the basic alarm triggers as follows:

- break in an electrical circuit;
- interrupt a light beam;
- detect a sound;
- detect a vibration;
- detect a change in capacitance.

12.8.2.3 Other alarm systems

Fire detection and prevention is covered in detail in Section 11.

Water detection is covered under leak detection in Section 10.

12.8.2.4 Integration requirements

All alarm outputs should be terminated in one of four methods/locations:

- local;
- central station;
- direct connection to EMS, fire, or law enforcement;
- proprietary connection (security command center).

Local alarms should not be used as the only termination in a data center facility as there is no guarantee that the alarm will be detected and acted upon. Local alarms do have advantages when layered with other termination methods. Those advantages include:

- psychological deterrent;
- low cost;
- may interrupt criminal or unauthorized activity.

If central station termination is utilized, the data center operator should periodically test and evaluate the training and response of the monitoring company. If the monitoring service also includes first responder alarm investigation, the background and training of the central station alarm investigators should be periodically evaluated.

Alarm and access control systems must be integrated to allow coordination of programming of desired security operational parameters, and a coordinated response to alarm conditions. For example, in many facilities, initiation of a fire alarm signal will be programmed to automatically unlock emergency egress doors in the facility to allow quick evacuation of the facility by personnel. Initiation of a security alarm by motion detectors can be programmed to initiate automatic display of video of the location on the security system computers.

12.9 Surveillance

12.9.1 Introduction

Security employs two types of surveillance: physical and technical. Physical surveillance techniques are primarily done by humans and are outside the scope of this standard. Technical surveillance is accomplished by electronic equipment, typically CCTV.

Closed Circuit Television or CCTV cameras serve several purposes in the security of the data center:

- enable security and monitoring personnel to centrally view many locations simultaneously;
- provide a visual record of monitored area during alarms and access control events;
- record crimes, civil and operational offenses for use as evidence in prosecution and human resources processes;
- record monitored areas and employee activity for use as a defense in civil and criminal prosecution against the data center.

12.9.2 Recommendations

Placement of cameras, frames per second, resolution, lighting, and other criteria should all be determined as a result of a risk/threat and vulnerability assessment. A qualified security consultant should identify the vulnerable areas and evaluate the operational, technical and environmental parameters before the CCTV design is approved.

CCTV placement should be coordinated with lighting designers to provide adequate image to recognize faces, vehicles, discern activity and other significant facts. This is especially important in outdoor situations where the type of image sensing technology, lens characteristics and lighting can affect the usability of view or recorded video.

CCTV cameras should be protected against theft, vandalism or neutralization. Protection for cameras should include:

- mounting the camera out of reach of pedestrian and vehicular traffic;
- protecting the camera in a secure enclosure or dome;
- environmental protection in extreme heat or cold conditions, or when the camera manufacture requires a controlled environment;
- securely mounted and fastened to a stationary object;
- in high-risk situations the camera may have an alarm sensor or switch attached;
- IP cameras can utilize simple network management protocol (SNMP) and trigger an alarm if the camera drops off the network.

When selecting a camera for any overt or covert monitoring scenario, the designer should consider the following performance criteria before selecting any CCTV camera/system:

- video analytics;
- backlight compensation;
- environmental operating limits;
- image sensing device;
- Internet Protocol (IP) capabilities;
- light compensation;
- method of synchronization;
- power over Ethernet capabilities;
- resolution;
- sensitivity;
- signal-to-noise ratio;
- size—dimensions and weight;
- telemetry;
- video output level.

Fixed cameras are designed to monitor a defined area, and come with adjustable aiming provisions and lenses to allow field setting of the coverage zone and focal length. Once set in the field for the focal length and coverage area, they remain fixed.

Pan-tilt-zoom (PTZ) cameras have an integral motorized mechanism that allow remote control from a special joystick/keyboard controller to move the field of coverage and change image magnification within the limits of the camera. PTZ cameras can be programmed to automatically sweep designated areas within their field of view and can be manually controlled to cover areas or zoom in to an area where suspicious activity is detected.

CCTV cameras mounted outdoors should be environmentally resistant and to have integral heaters and blowers to maintain the housing interior temperature within the camera's operating limits.

When low-light conditions are anticipated, the CCTV design requires the use of cameras designed for this application, as follows:

- day/night cameras are often used to provide color video during daytime conditions, which switch to monochrome video during nighttime conditions with lower lighting levels;
- infrared (IR) illuminators generate infrared light that is nearly invisible to the human eye, but will enable IR-sensitive CCTV cameras to produce high-quality images under nighttime conditions without requiring visible light illumination;
- cameras should be installed to maximize the amount of lighting coming from behind the camera or directed in the same direction as the camera; avoid light sources that provide direct illumination on the camera lens. Current camera technology utilizes charge coupled device (CCD) chips, which are more sensitive to low light and the IR spectrum;
- lighting sources for areas having video surveillance should have good color rendition, such as fluorescent or HID metal halide. Avoid use of low-pressure sodium, high-pressure sodium, and mercury vapor lamp sources, which have poor color rendition and do not adequately support video surveillance equipment performance.

Some video surveillance systems have “video analytics” (AI) capability that allows distinguishing of movements detected by the cameras and triggering programmed response such as alarms, recording or log entries. Cameras utilizing video analytics should be used to monitor high-value or sensitive equipment or areas of the data center, where a specific asset is at risk, or where it does not make sense to record the surveillance, 24/7 such as very sporadic offenses.

Dummy cameras should not be used for data centers. The use these empty camera housings are frequently discovered in the office environment and can lead to additional liability for the management of the data center facility.

IP cameras should be considered when selecting the CCTV system for the data center. They have the following performance advantages described below, but require coordinating with network engineers to operate properly without degrading network performance.

- cameras can use power over Ethernet (PoE), eliminating the need for separate power supplies, reducing labor and cable costs;
- surveillance distribution is available to authorized users directly off the network;

- existing structured cabling system (SCS) infrastructure is used, in an open architecture;
- camera system is scalable and easily expanded;
- in addition, routine permanent archiving of video to capture authorized occupant entries and exits from the facility or controlled spaces is often employed to maintain a record in case an incident occurs that requires an investigation.

If the CCTV surveillance system is monitored locally by guards or other personnel, the method(s) by which the cameras are monitored should be determined by the threat/risk and vulnerability of person(s) or assets in the area being monitored. The four methods of monitoring surveillance cameras include:

- dedicated monitors;
- split screens;
- sequential switching;
- alarm switching.

Integration of the CCTV surveillance system with alarms or access control applications should be part of the data center security plan. Examples of this would include automatic switching to a fixed camera when the two-man rule is violated for the computer room, or in the same scenario, having a PTZ camera automatically move to the data center access control point when the same alarm occurs.

The use of SNMP also should be used for events and alarms triggered by unauthorized access to or removal of physical layer infrastructure in the data center. An example of this would include the integration of fixed CCTV cameras, intelligent patching and integrated alarms in a remote telecommunications closet, where the attempted insertion into a data switch activates the surveillance system and notifies the network operations center of the possible unauthorized access.

12.10 Barriers

12.10.1 Introduction

12.10.1.1 Definitions

Definitions used in this section are as follows:

barrier: a fabricated or natural obstacle used to control access to something, or the movement of people, animals, vehicles, or any material in motion.

clear zone: an area separating an outdoor barrier from buildings or any form of natural or manufactured concealment.

compartmentalization: the isolation or segregation of assets from threats using architectural design or countermeasures, including physical barriers.

layering: the use of many layers of barriers, other countermeasures, or a mixture of both, used to provide the maximum level of deterrence and delay (see Figure 53).

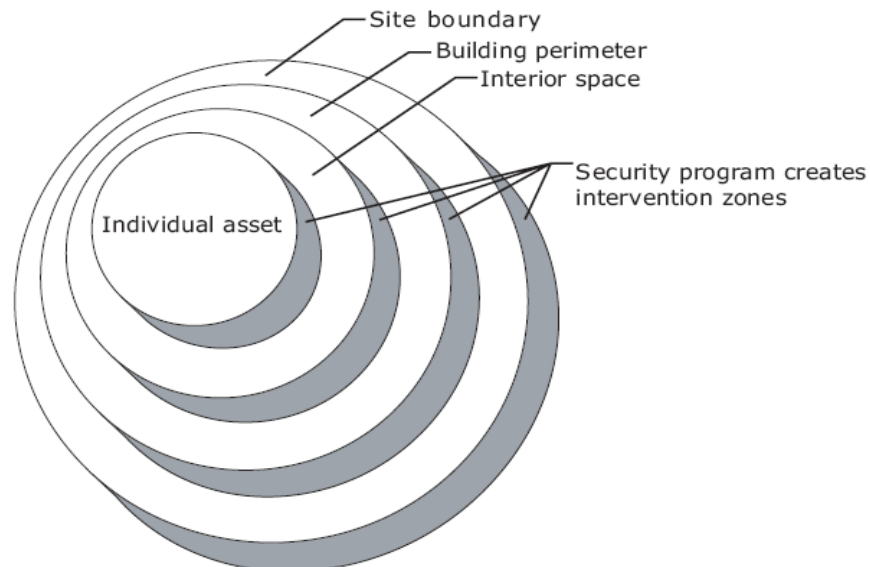


Figure 53: Security Layers

natural barrier: any object of nature that impedes or prevents access, including mountains, bodies of water, deserts, and swamps.

psychological barrier: a device, obstacle or lack of obstacle that by its presence alone discourages unauthorized access or penetration.

structural barrier: something that physically deters or prevents unauthorized access, movement, destruction or removal of data center assets.

12.10.1.2 General

Barriers can be classified into three major groups:

- building exteriors;
- fences;
- masonry structures.

Structural barriers are not impenetrable, but are primarily used to delay entry so that another system(s) can detect and notify employees, guards, monitoring stations, or law enforcement. At a minimum, good use of barriers will force the intruder to leave evidence of their penetration and simultaneously triggering an electronic or human countermeasure.

12.10.2 Recommendations

Structural barriers should be put in place to protect against accidental and intentional explosions. The architect and security designer for the data center should consider the relative resistance to explosion that the various barriers offer. The following list of barriers is organized from the most blast resistance to the least:

- thick reinforced concrete walls;
- thick brick or concrete walls without reinforcement;
- reinforced concrete walls;
- thick earthen barricades;
- building walls with steel frames;
- sturdy wooden frame walls;
- common brick walls;
- wire-reinforced glass;
- common glass.

Table 16 demonstrates the thickness of a concrete wall needed to protect from the secondary damage cause by projectiles launched by an explosion at varying distances:

Table 16: Thickness Of Concrete Wall For Projectile Protection

<i>Distance from explosion m (ft)</i>	<i>Projective velocity m/s (ft/s)</i>	<i>Concrete wall thickness mm (in)</i>
30.5 m (100 ft)	610 m/s (2,000 f/s)	305 mm (12 in)
69 m (225 ft)	610 m/s (2,000 f/s)	254 mm (10 in)
152 m (500 ft)	457 m/s (1,500 f/s)	178 mm (7 in)
274 m (900 ft)	305 m/s (1,000 f/s)	127 mm (5 in)
716 m (2,350 ft)	152 m/s (500 f/s)	64 mm (2.5 in)

Source: *Protection of Assets Manual*, ASIS International

Barriers should be designed in layers so that the asset(s) that need to be protected lie behind or inside of multiple levels, with the objective of each barrier to create as much delay as possible.

Barriers should also be used to prevent or delay the unauthorized movement or removal of objects by employees, visitors, contractors or other occupants.

Barriers should be used to delay or prevent access to or damage to the site, buildings or areas of the data center.

A barrier can also be utilized to prevent visual access to a building or asset. Preventing visual access will prevent the potential offender from knowing the location of the asset, or that it even exists. An example of a visual barrier, would be locating a data center inside an old warehouse or inside of a dense forest, with no visual clues of its existence.

Barriers should be utilized to delay or prevent three types of penetration:

- by force;
- by deception or stealth;
- by accident.

When barriers are used outdoors, a clear zone free of anything that could offer concealment, such as trees, weeds, rubbish, small buildings or vehicles should be maintained.

Guidelines for clear zones around barriers used at data center site perimeters include:

- clear zones should be maintained on both sides;
- the outside of the barrier should be at least 6 m (20 ft) away from all potential visual obstructions, including buildings, roads, parking lots, and natural objects like trees, rocks, and hills;
- the inside of barriers used for a perimeter, should maintain a clear zone that is at least 15 m (50 ft) away from any building or other asset.

12.10.2.1 Vehicle barriers

The data center architect and security designer should take into consideration the escalating use of vehicles to both inflict primary damage to buildings and persons (intentional and accidental), but also as a delivery mechanism for explosive devices.

Barriers that should be considered when designing protective barriers for the entrances and other vulnerable areas of the data center site and buildings include the following:

- Fences;
- Metal highway guard rails;
- Concrete vehicle bollards and barriers;
- Concrete Jersey barriers;
- Metal beams or posts;
- Combinations of material such as tires, railroad ties, and earth.

Table 17 illustrates the vulnerability of various barriers to penetration by vehicles.

Table 17: Vehicle Barrier Comparison

<i>Barrier tested</i>	<i>Vehicle</i>	<i>Barrier damage</i>	<i>Vehicle damage</i>	<i>Occupant injury</i>
Chain link fence	3/4 ton pickup truck	Full penetration	Paint scratched	No injury
Double swing gate	3/4 ton pickup truck	Full penetration	Slight dents	No injury
Chain link fence w/ 19 mm (0.75 in) cable	3/4 ton pickup truck	Full penetration, vehicle stopped, cable held	Extensive front end damage	Risk of injury
Concrete media barrier	3/4 ton pickup truck	No penetration	Major damage	Risk of injury
Tires	3/4 ton pickup truck	No penetration	Major damage	Risk of injury

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.10.2.2 Building exteriors

Building exteriors should be evaluated for their ability to delay potential attacks on the data center.

During data center planning, the ability of all building surfaces should be evaluated for their performance as security barriers. Existing structures being retrofitted as a data center should include both a physical survey of the structure and a review of available architectural drawings created during initial design and construction.

Evaluation of the architectural drawings and physical inspection of an existing building for the effectiveness of any wall, ceiling, or floor should consider the following metrics at a minimum:

- amount of space existing between walls, ceiling and floors;
- risk introduced by the existing or updated HVAC air handling spaces;
- modification of the original walls, ceiling or floors;
- weaknesses revealed during the physical inspection;
- rooftop accessibility from adjacent structures;
- underfloor accessibility through tunneling;
- underfloor accessibility through drainage tunnels, subways and other subterranean passageways

The six walls (floor, ceiling and vertical walls) of any structure housing a data center should be composed of reinforced concrete or other masonry components due to the increase in penetration time over other commonly used materials.

12.10.2.3 Concrete walls

Concrete walls make excellent barriers and offer excellent psychological deterrence and physical delay. Success in using concrete walls as barriers will depend on the thickness of the concrete and materials used for reinforcement. General guidelines for concrete walls can be found in the following sections.

Concrete or block walls that are used to support structural loads are not necessarily designed to provide enough delay to be an effective barrier. Unreinforced concrete walls offer little protection from penetration. For the security of a data center, all concrete walls should include steel reinforcing bars or rebar. Table 18 demonstrates the speed at which a 300 mm (12 in) thick reinforced concrete wall can be penetrated.

Concrete block walls that do not include a reinforcing material offer almost no resistance to penetration using small hand tools. When used for data center construction, concrete block walls should include some type of reinforcing methodology, typically filling the hollow core with concrete or mortar, installation of rebar, or both:

- 100 mm (4 in) thick reinforced concrete walls are typically used for curtain walls and provide little resistance to penetration with hand tools.
- 150 mm (6 in) thick reinforced concrete walls offer more delay, but are still vulnerable to hand tools and small explosions.
- 200 mm (8 in) thick reinforced concrete walls are common as load bearing structural support walls and can also be penetrated using hand tools.
- Concrete walls of greater than 200 mm (8 in) are usually found only in the construction of vaults or blast resistant bunkers.

NOTE: Studies have shown that it can take under a minute to create a person-sized hole in a 200 mm (8 in), mortar-filled block wall with a common sledgehammer, and only a few more seconds if 13 mm (0.50 in) steel rebar is added.

Table 18: Speed Of Concrete Wall Penetration

300 mm (12 in) thick concrete with #5 rebar on 150 mm (6 in) centers

<i>People needed</i>	<i>Equipment needed</i>	<i>Equipment weight kg (lb)</i>	<i>Minimum time min</i>	<i>Maximum time min</i>
2	Explosives, tamper plate, hand hydraulic	22 kg (48 lb)	2.8	8.4
2	Explosives, hand hydraulic bolt cutters	18 kg (39 lb)	2.8	8.4
1	Explosives, platter	102 kg (225 lb)	1.95	5.85
2	Roto hammer, sledge, punch, handheld power hydraulic bolt cutters, generator	73 kg (161 lb)	15.0	45.0
2	Explosives, tamper plate, handheld hydraulic bolt cutters	69 kg (153 lb)	1.4	4.2

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.10.2.4 Building openings

Building openings generally are utilized for one of the following purposes:

- entrance (pedestrians and vehicles);
- exit (pedestrians and vehicles);
- natural illumination;
- ventilation;
- material movement (loading docks);
- utility access;
- drainage.

Any building opening less than 5.5 m (18 ft) above ground and larger than 62,000 mm² (96 in²) should be or be protected by a barrier, alarmed and/or monitored for use as an unauthorized access point.

Building openings should be at least as difficult to penetrate as the walls, ceilings or floor of a data center. Table 19 illustrates the amount of time needed to penetrate the standard industrial pedestrian door.

Doors are typically built from one or more of the following materials or a combination of them:

- wood;
- glass;
- metal.

The following should be considered when considering the design and construction of doors for the data center:

- if wooden doors are used, ensure that no gap exists between the doorstop and the doorjamb, which would allow shims or levers to be inserted;
- hinge pins and mounting screws should always be mounted toward the protected side of the door;
- hinge pins should always be welded or flanged to prevent unauthorized removal;
- when possible, hinges should be fastened through the doorframe, into the wall stud or other structural member;
- doorframes should be securely fastened to the wall studs or other structural member.

Windows mounted on the exterior of a data center building shell are designed to provide natural light, natural ventilation and visual access, none of which are necessary or advisable for the computer room and many of the secured areas of the data center.

Table 19: Time To Penetrate Industrial Pedestrian Doors

<i>Penetration method</i>	<i>Noise dB</i>	<i>Attack area</i>	<i>Time needed min</i>
Explosives	–	Door face	0.5–1.5
Thermal (Oxy-Lance)	70–76	Door face	1.5–2.5
Thermal (cutting torch)	60–64	Door face	2.0–6.0
Power drill	–	Panic bar	0.5
Axe through metal	72–110	Panic bar	1.5–5.0
Axe through glass	76–100	Panic bar	0.5
Lock pick	–	Lock	0.25–5.0
Wrench	–	Lock	0.5
Pry bar	74–76	Lock frame	0.5
Thermal (cutting torch)	60–73	Hinge pins	0.5–1.5
Hammer and punch	72–75	Hinge pins	1.0–3.0
Explosives	–	Hinge pins	1.0–2.5
Crowbar	60–100	Mesh/window	0.5–2.0

Source: *Barrier Technology Handbook*, Sandia Laboratories

The types of windows used in modern construction include:

- Awning.
- Casement.
- Horizontal sliding.
- Jalousie.
- Picture.
- Projected.

Only picture windows should be installed in any exterior walls of the data center shell.

Exterior windows should be included in the security risk assessment and the appropriate mesh or glazing material consistent with the desired delay or blast resistance desired.

If one or more of the walls of a computer room are exterior walls, there should be no windows of any type on the exterior computer room walls.

Exterior windows should never use putty or molding to secure the panes of glass or plastic in the frame. Only frame mounted (grooved) type of window mounting should be permitted for the data center shell.

Table 20 should be used as a guide when determining the amount of delay desired for a window.

Table 20: Time To Penetrate Windows

<i>Type of Window</i>	<i>Tool</i>	<i>Penetration time min</i>
<i>Glass</i>		
6 mm (1/4 in) tempered	Fire axe	0.05–0.15
6 mm (1/4 in) wire	Fire axe	0.15–0.45
6 mm (1/4 in) laminated	Fire axe	0.30–0.90
14 mm (9/16 in) security	Sledgehammer, Fire axe	0.75–2.25
<i>Plastic</i>		
6 mm (1/4 in) Lexan [®] , Lucite [™] , or Plexiglas [®]	Fire axe Demolition saw	0.05–0.15 0.15–0.45
13 mm (0.5 in) Lucite [™] or Plexiglas [®]	Fire axe Demolition saw	0.05–0.15 0.35–1.05
13 mm (0.5 in) Lexan [®]	Fire axe Sledgehammer	2.0–6.0 2.0–6.0
25 mm (1 in) Lucite [™] or Plexiglas [®]	Sledgehammer Fire axe	0.05–0.15 0.10–0.30
<i>Glass with enhancements</i>		
Glass with 2.9 mm (9-gauge) Mesh	Fire axe, Bolt cutters	0.25–1.35
Glass with 19 mm (3/4 in) Quarry screen	Demolition saw Cutting torch	0.75–2.25 1.35–4.05
Glass with 13 mm (0.5 in) Diagonal bars	Bolt cutters Hacksaw	0.5–1.5 1.3–3.9

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.10.2.5 Glazing

Glazing is the installation of glass, plastic or glass/plastic laminates to increase building surface (especially windows and doors) resistance to explosion, impact, fire or other threats.

When glass is utilized to fill building openings on the exterior of the data center building shell, or interior wall openings, consideration should be given to the danger to occupants and equipment should an explosion occur. If interior or exterior glass is broken, the following undesirable events could occur:

- Unauthorized entry
- Physical injury due to sharp glass fragments, especially when they become airborne as the result of an explosion
- Property damage to data center assets due to airborne sharp glass fragments following an explosion
- Physical or property damage due to fragments of glass falling.

In conjunction and compliance with local codes and safety regulations, tempered glass should always be used in data center windows and doors. It is 3 to 5 times stronger than ordinary glass and due to the effects of the tempering process, there is a decreased risk of injury and reduced fragment size of glass fragments following an explosion or penetration.

Plastic or polyester film should also be considered as a method to reduce the risk of injury, damage and penetration from explosion or forced entry. Film reinforced windows reduce the fragment hazards by retaining glass fragments following an explosion or shattering incident.

Wired glass should also be considered for use in both interior and exterior installations. Many fire and safety codes require the use of glass with wire mesh embedded. It is important to note that while wired glass offers resistance to penetration from large objects, it offers little or no protection from shattered glass fragments or smaller projectiles.

Laminated glass, consisting of alternate layers of glass and plastic, should be considered for any window or door where impact resistance is essential. Tempered, wired and film reinforced glass all resist the initial impact but frequently fall away allowing unauthorized entry. Conversely, laminated glass remains in place and retains the ability to deter and further delay entry.

Some laminated glass has electrical properties that permit its use as an alarm. During the attempted penetration of the glass, an alarm is triggered allowing a) the sounding of audible burglar alarms, or b) security or law enforcement personnel to gain valuable response time.

Due to their overall strength and resistance to breakage, designers should consider the use of acrylic and polycarbonate-based windows and door glass. These materials are approved for safety and have up to 17 times more resistance to breakage than glass of comparable thickness.

12.10.2.6 Bullet resistant glass or glazing

If the threat of gunfire or other projectiles is present, the data center should consider the use of bullet-resisting glass. It is important to fully evaluate the nature and type of attacks being protected against, since bullet-resisting glass is available in a variety of thicknesses – 19 mm (3/4 in) to 119 mm (4.7 in)– and construction. Attacks can range from individuals with rocks or hammers to high-powered rifles, machine guns or missiles. It is important to properly assess the risk and threat before selecting bullet-resisting glass.

Security designers should consider the eight levels of resistivity defined in UL 752, which quantifies resistivity based upon the ammunition used and shot pattern or placement:

- Level 1 – 4.8 mm (3/16 in) thick, solid, open-hearth steel with a tensile strength of 345000 kPa (50,000 psi) or 9 mm full copper jacket with lead core, 124 grain at 358 m/s (1,175 ft/s) – 3 shots;
- Level 2 – 0.357 Magnum lead soft point, 158 grain at 381 m/s (1,250 ft/s) – 3 shots.
- Level 3 – 0.44 Magnum lead, semiwadcutter gas checked, 240 grain at 411 m/s (1,350 ft/s) – 3 shots;
- Level 4 – 0.30 caliber rifle lead core soft point, 180 grain at 774 m/s (2,540 ft/s) – 1 shot;
- Level 5 – 7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 1 shot;
- Level 6 – 9 mm full copper jacket lead core, 124 grain, 427 m/s (1,400 ft/s) – 5 shots;
- Level 7 – 5.56 mm rifle lead core full copper jacket, 55 grain, 939 m/s (3,080 ft/s) – 5 shots;
- Level 8 – 7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 5 shots;
- Supplemental – All tests have a supplemental shotgun test using a 12-gauge shotgun with 1 rifled lead slug, 437 grain, 483 m/s (1,585 ft/s) and the other 00 lead buckshot with 12 pellets, 650 grain, 366 m/s (1,200 ft/s).

12.10.2.7 Burglary resistant glass or glazing

The data center may be at a high risk for burglary due quantity and value of the ITE located there. Any window or door containing glass should be evaluated for its resistance to burglary. Some of the criteria used to evaluate the resistance of glass to burglary include:

- single blow impact testing (*smash and grab*);
- multiple impact testing;
- high-energy impact testing;
- performance.

Data center security designers should also be aware of the five classes of protection defined by ASTM F1233, which evaluate and compare security-glazing methods against three metrics, a) ballistic attack, 2) forced entry, and 3) a combination of both.

Forced entry testing involves attacking security glazing using a predefined sequence of tools and weapons. The list below each class is in order of occurrence during classification.

- Class I – ball peen hammer;
- Class II – ball peen hammer, 38 mm (1.5 in) pipe/sledge, fire extinguisher, sledge hammer, propane torch, ripping bar;
- Class III – ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, ripping bar, chisel/hammer, gasoline, angle iron/sledge, sledge hammer;
- Class IV – ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, fire axe, sledge hammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledge hammer, chisel/hammer, wood maul;
- Class V – ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, fire axe, sledge hammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledge hammer, chisel/hammer, wood splitting maul.

12.10.2.8 Fences and metal barriers**12.10.2.8.1 General**

Fences should not be considered as a permanent barrier to forced entry. They introduce delay but not prevention and should be layered with other countermeasures like alarms, surveillance, and guards.

Security designers should consider that even 2.4 m (8 ft) tall fencing with three strands of barbed wire could be compromised in less than 10 seconds.

Fencing should be considered useful as a barrier for:

- psychological deterrent.
- mark property boundaries.
- limited vehicle barrier.
- most small animals.
- casual intruders.
- opportunistic offenders.

Fence design must take into consideration the type of risk and threat. Many fencing designed to prevent pedestrian entry have little or no delay factor for vehicles. Guard railing along a highway is one type of vehicular fence, which has almost no impact on the delay of pedestrians or animals.

12.10.2.8.2 Chain link fencing

The most widely used fencing for security purposes is the chain link fence.

The Chain Link Fence Manufacturers Institute (CLFMI) and the American Society for Testing and Materials (ASTM) maintain the specifications intended as the recognized standards for quality of manufacturing and installation.

Recommended design and installation guidelines for chain link fencing include:

- Line posts should not exceed 3 m (10 ft) spans on average.
- Post hole depths should be at a minimum of 600 mm (24 in) plus an additional 75 mm (3 in) for each 300 mm (12 in) increase in fence height over 1.2 m (4 ft).
- Terminal posts should be braced diagonally to the closest line post, if no top rail is present, and with no more than a 50 degree angle between the brace and the ground.

- If no top rail is used, then top tension wire must be installed. NOTE: Top rails can be used as handholds for climbing the fence.
- The fencing fabric should be 2.9 mm (9 gauge) or greater and the mesh openings should not be larger than 50 mm (2 in).
- Fencing fabric should reach within 50 mm (2 in) of firm ground, paving or concrete.
- On soft ground, the fencing fabric should extend below ground and can be set into a concrete apron.
- Any bolts or nuts that are used to fasten any hardware to a fence should be spot welded.
- Any opening for drainage larger than 62,000 mm² (96 in²) should have additional grates, fencing, mesh, grills or other barriers installed to discourage unauthorized access; drainage should not be impaired.
- For additional delay, a top guard, consisting of three strands of barbed wire, spaced 150 mm (6 in) apart and mounted on the top of the fence at a 45-degree angle outward, inward or both directions, should be considered; since the primary purpose of this fencing is to discourage or delay human entry, the fencing should be at least 2.1 m (7 ft) high, not including the top guard.
- In addition to barbed wire, other barrier protection obstacles can be added to the fencing, such as spikes and barbed top guards.
- Gates should be the same height as adjacent fencing (including top guards).
- When privacy is required to conceal activity or remove visual identification of high-value or sensitive assets, strips of material can be woven into the chain link fence; plastic, wood and fabric are all commonly used for privacy applications.
- Chain link fencing should also be considered for service provider areas, storage and other areas for temporary security or when hard-walled construction is not an option.

A clear zone should be established for at least 6 m (20 ft) on both sides of the fence, with anything that could be used as an aid to climb the fence removed. This includes the trimming of overhanging tree limbs. Other items that might be used to go over the fence include:

- Vehicles;
- Boxes;
- Ladders;
- Construction material (e.g., wood, poles, concrete blocks);
- Boxes;
- Skids;
- Containers;
- Equipment.

12.10.2.9 Metal and welded wire barriers

12.10.2.9.1 General

Expanded metal fabric consists of sheets of metal (carbon, galvanized, stainless steel, aluminum, and others) that have been cut or shaped and somewhat flattened or thinned for barrier material that:

- Is resistant to cutting;
- Won't unravel or uncoil;
- Is easy to fabricate and install;
- Permits environmental conditioning, lighting, and inspection of secure spaces like storage areas, service provider cages, cabinets, and other data center areas;
- Provides enhanced psychological deterrence.

Expanded metal barrier material comes in four styles that should be designed for the anticipated risks and threats in the area installed. The four types of generally accepted expanded metal are:

- Standard;
- Grate or diamond plate;
- Flattened;
- Architectural.

Welded wire fabric is created by welding a series of wires at right angles forming a wire fabric, where at each intersection the wires are welded together.

Welded wire fabric should be used when a less demanding barrier is needed than expanded wire. Other security applications where welded wire is used include:

- Tool rooms;
- Utility areas;
- Building automation control rooms;
- Computer facilities and rooms;
- Window guards;
- Lockers;
- Animal cages (laboratory environment).

Woven wire fabric is considered a barrier, but is used for less demanding applications, and is not generally acceptable as a security countermeasure.

12.10.2.9.2 Barbed wire

For the purposes of this section, barbed wire will also include barbed tape.

Although its original purpose was as an animal barrier, barbed wire is an important auxiliary security enhancement for many barriers, including fencing. Primary uses of barbed wire include:

- fence fabric;
- top guard for chain link or other fencing;
- concertina coils;
- other barriers.

The key benefit of barbed wire is that it is a psychological deterrent and should not be designed as a primary countermeasure to induce delay.

Recommended considerations when using barbed wire in a security design include:

- number of barbs;
- design of barbs;
- location of barbs.

To discourage potential intruders from gripping the barbed wire, designs for data center perimeters and other barbed wire installations should specify four-pointed barbs located on 75 mm (3 in) centers.

Barbed wire strands should be attached to posts that are less than 1.8 m (6 ft) apart, with distance between the strands never exceeding 150 mm (6 in).

If soft soils, erosion or small animals create vulnerabilities, then a single strand of barbed wire should be at ground level. This will also discourage tunneling.

For additional delay, barbed wire strands should be formed into concertina coils. Concertina coils are used in the following ways:

- top guards on fences and other barriers;
- temporary barriers;
- tactical barriers.

12.10.2.9.3 Gates

Data center perimeters should include no more gates than are necessary. Each gate provides more opportunity for operational failures (left unlocked or open) and vulnerability.

Gates can be manual or motor operated and are available in the following styles:

- single-swing;
- double-swing;
- multifold;
- overhead single slide;
- overhead double slide;
- cantilever slide single;
- cantilever slide double;
- aircraft sliding gates.

12.11 Lighting

12.11.1 Introduction

Effective lighting is a key component to an overall security program; it is a powerful psychological deterrent to criminal activities, and it enables security personnel to perform their work more efficiently. A good lighting design will include the following design parameters:

- higher brightness levels improve the ability to detect objects and recognize people;
- horizontal illumination levels assist in identifying objects that are horizontally oriented, such as streets, sidewalks, steps, and horizontal obstacles; vertical illumination levels assist in identifying vertically oriented surfaces, and assist in visual recognition of other personnel from a safe distance;
- uniformity in the lighting system eliminates harsh shadows around buildings and surrounding areas; this makes the environment safer for pedestrians and drivers;
- glare is excessive brightness coming from poorly designed or misapplied lighting fixtures, or is reflected from glossy surfaces; glare should be minimized to maintain visibility of the area by personnel and video surveillance equipment;
- horizontal and vertical lighting levels in parking lots and parking garages should be within limits recommended for visual identification, and should be uniform with no dark areas around corners or vehicle parking slots, where personnel may hide; entrances to buildings should be illuminated at a higher level than surrounding areas to increase safety and guide visitors into the facility.

12.12 Guards

12.12.1 Introduction

Security guards, also referred to as security officers, have the following basic functions when used for security of the data center:

- patrol of perimeters, site, buildings, and areas;
- control vehicular and pedestrian traffic;
- escorts;
- inspection of shipments, packages, and visitors;
- other special duties.

12.12.2 Recommendations

When present, security officers should monitor and control access through all perimeter openings.

Guards or security officers can be contract, employees, or a mixture of both.

All guards should be trained in the security plan and policy for the data center, building or campus.

Guards should be utilized to identify, log and monitor all nonemployees entering the facility, including vendors, contractors, and visitors.

Access to the facility, building or data center should be granted only under conditions identified by the security plan or policy. Anyone not meeting those preset conditions should not be permitted into the facility, until such time that those conditions are met.

12.13 Disaster recovery

12.13.1 Recommendations

All data centers should have a detailed disaster recovery plan. The physical disaster recovery plan should be complimentary or integrated within the IT disaster recovery plan and the organization's business continuity plan (BCP).

The data center disaster recovery plan must deal with all phases of an emergency including:

- planning;
- predisaster/incident activities;
- the disaster/incident;
- response;
- recovery from the disaster/incident.

The data center should identify a Disaster Recovery Manager (DRM) who is responsible for the coordination and implementation of the disaster recovery plan.

A detailed analysis of the impact of both long and short-term business interruptions should be conducted. The data center should evaluate the impact of total shutdown for up to 30 days.

Specific employees and contractors should participate in the creation and regular updating of the disaster recovery plan.

The planning for and classification of disasters should follow the guidelines outlined in NFPA 1600.

The disaster recovery plan should take into account the following types of major disasters:

- aircraft crashes;
- chemical accidents;
- dust;
- earthquakes;
- epidemics;
- falling objects;
- fire;
- electrical hazards;
- hurricanes;
- landslides;
- loss of utility services, including water, electric, and telecommunications;
- natural disasters;
- weather extremes.

The disaster recovery plan should take into account the following types of criminal activity, which can have disastrous impact on the data center:

- arson;
- blackmail;
- breaking and entering/burglary;
- bribery;
- collusion;
- conspiracy;
- disorderly conduct;
- embezzlement;
- extortion;
- fraud;
- kidnapping;
- looting;
- rape;
- riot;
- terrorism;
- theft;
- trespassing;
- vandalism;
- white-collar crime.

Data centers should regularly and routinely conduct disaster recovery tests.

The test should be evaluated and modifications made in the disaster recovery plan to address any issues.

Disaster recovery planning should include the creation of mutual aid agreements with other businesses or organizations.

Disaster recovery planning should include the identification of key employees or contractors necessary to restore operation to the data center during a disaster.

Backups should be identified in the event that the primary personnel identified are unable to respond.

Data center and security personnel should meet with appropriate federal, state and local authorities that have control of surface roads and disaster zones and determine the forms of identification and authorization that will be required during a natural, technological or human disaster.

Each employee or contractor designated as critical to restoring operation of the data center during a disaster should have some preapproved method of identification and authorization to enter disaster zones, should the data center facility be classified as part of such.

Disaster plans should include the identification and listing of likely emergency routes.

Disaster plans should identify primary and secondary methods of communications between key personnel needed to restore operations to the data center.

Identified employees and contractors should have or have easy access to a contact list containing the names, addresses, telephone numbers, and other contact information for each primary and backup responder.

Due to the variable nature of the availability of communications during a disaster, multiple methods of communication should be available, including:

- telephones;
- cellular phones;
- personal communication devices (e.g., Blackberry);
- IP phones;
- pagers;
- land mobile radios;
- citizens band (CB) radios.

Disaster recovery plans should include detailed plans for all aspects of emergency operation of the data center, including:

- access/egress badges, keys, cards for all areas, including those normally off limits;
- access control plans for nonemergency personnel;
- operational checklists, with detailed documentation and instructions on operation of equipment with which the emergency responder may not be familiar;
- facility shutdown procedures;
- emergency security procedures;
- the location of all emergency equipment;
- the use of fire and emergency equipment.

12.14 Building site considerations

12.14.1 Introduction

The purpose of building site security is to prevent unauthorized entry or exit by employees and/or others, to determine likely human, man-made, and natural threats and implement countermeasures. Site security also involves the control of pedestrian and vehicular traffic, and should ensure that employees, visitors, contractors, and other pedestrians and vehicles can be monitored and inspected as needed.

12.14.2 Recommendations

12.14.2.1 General

All exterior building openings larger than 62,000 mm² (96 in²) should be covered with a security grill, using an approved wire fabric and tool resistant 13 mm (0.5 in) steel bars spaced no less than 200 mm (8 in) on center.

All security devices should be installed using security fasteners. Security fasteners eliminate the risk of easy removal and include:

- one-way screws;
- bolts;
- non-removable pins;
- setscrews;
- spot welds.

Door hinges that mount to the exterior of the door should have non-removable pins, fixed pins, or center pivots.

Burglar-resistant window/door glazing shall meet the following minimum requirements:

- Total thickness of glass laminate shall be 6 mm (0.25 in) plus 60 mil vinyl film sandwiched between the glass.
- Glass shall be tempered, tested, and certified to ASTM Class III of F1233 or UL Standard 972.
- If the window is insulated, the laminated assembly shall be on the exterior of the window.
- Bullet-resistant or blast-resistant glazing is recommended in high crime areas or for building near parking areas and/or roadways.

Bullet-resistant material should at a minimum meet UL super small arms (SSA) threat level using UL 972 test methods.

All exterior doors should have a lock with a deadbolt or equal locking capability.

Mortise locks used for security must adhere to ANSI/BHMA A156.13 standards and must have a deadbolt throw of 25 mm (1 in) minimum.

12.14.2.2 Threat history

Historical information should be gathered during the planning for any security system design, whether new or retrofitted into an existing data center. Typical information gathered during this investigation would include:

- Within the past 5 years, has anyone been successful at this location in damaging any part of the data center facility;
- What is the frequency of natural disasters for the data center site? What types of natural disasters have occurred and how often?
- Have any natural, technological or human disasters rendered the data center or any business inoperable within the last five years? Ever?
- What is the frequency of the following within a 1.6 km (1 mi) radius of the data center facility?
 - assault
 - armed robbery
 - auto theft
 - burglary
 - drug trafficking
 - fires
 - floods
 - hurricane/tornado/cyclone
 - kidnapping
 - murder
 - terrorism
 - riot
 - vandalism
 - workplace violence

The most common threats to all personnel should be identified and training should be conducted to address these risks.

Employees should be trained to ensure that they act appropriately in high-risk situations, such as workplace violence, sabotage, kidnapping, natural disasters, and robbery.

12.14.2.3 Perimeter fencing and barriers

Perimeter fencing due to threats from local crime, breaking and entering, workplace violence or other concerns should include the following design guidelines:

- fencing should be placed along property lines;
- when employee parking is separate from general parking, fencing or barriers should be used;
- fencing should be placed along street frontage in high crime areas;
- fencing should be placed along abutting buildings due to local crime concerns.

Perimeter fencing and gates for the data center should be constructed using the following minimum design requirements:

- constructed of a 2.9 mm (9-gauge) steel wire with 50 mm (2 in) mesh chain link (minimum);
- for aesthetic purposes vinyl cladding is acceptable;
- 2.4 m (8 ft) high with no top guard;
- 2.1 m (7 ft) high with top guard (fence height only);
- installed in a straight line at ground level no more than 50 mm (2 in) from the pavement, hard ground or concrete;
- ties fastening the fence fabric to the posts and rails should be 2.3 mm (11-gauge) steel or screw type fasteners.

The top guard should face outward and upward and be constructed at a 45 degree angle. The top guard should only increase the height of the fence by 300 mm (12 in) but should have three strands of double-twisted, four-point barbed wire mounted 150 mm (6 in) equidistant apart.

When fencing is adjacent to vehicular traffic lanes or parking areas, it should be protected by wheel stops, curbs, bollards or guardrails as required.

When possible, clear zones should be established on either side of the fencing. The planting of even low shrubbery or plantings should be avoided if possible, but at a minimum should be placed no closer to the fence than 0.6 to 0.9 m (2 or 3 ft). Trees or other plantings should never provide points of concealment or assist in unauthorized access to the facility or site.

Signage should be placed on the fence warning of restricted or limited access. All security signage should be placed at 30 m (100 ft) intervals and 1.5 m (5 ft) above the ground.

The following special areas are known to cause breaches of the perimeter and will increase the risk of unauthorized entry:

- sidewalk elevators;
- utility tunnels;
- storm sewers;
- piers, docks, and wharves.

12.14.2.4 Lighting

Lighting is one of the primary considerations for providing the security of occupants and assets in the data center. The following types of lighting should be considered for security use based upon their respective properties, life cycle, environmental conditions and impact on other security systems (e.g., CCTV):

- incandescent;
- gaseous discharge (mercury/sodium vapor);
- quartz.

Security or protective lighting should consider one of the four following types:

- continuous;
- emergency;
- movable;
- standby.

Basic security lighting should be provided to protect the safety of pedestrians, vehicles and assets, as well as preventing concealment for unauthorized access to the data center site or buildings. Lighting should be provided at the following areas (at a minimum):

- perimeter fencing;
- the building perimeter;
- all entrance gates – pedestrian and vehicular;
- all building entrances and exits;
- vestibules and lobbies;
- gatehouses/guardhouses;
- windows and exterior openings when the risk of unauthorized access through them is determined;
- all public areas;
- pedestrian walkways;
- stairwells.

Lighting should meet the minimum levels of intensity, measured in foot-candles, as listed in Table 21.

Table 21: Minimum Lighting Levels

<i>Area</i>	<i>Minimum Lighting lx (fc)</i>
Outer perimeter	1.5 lx (0.15 fc)
Inner perimeter	4 lx (0.4 fc)
Base of perimeter fence	10 lx (1.0 fc)
Vehicular entrances	10 lx (1.0 fc)
Pedestrian entrances	20 lx (2.0 fc)
Restricted structures	20 lx (2.0 fc)
Clear zones	2 lx (0.2 fc)
Parking areas	10 lx (1.0 fc)

12.14.2.5 Transportation threats and concerns

12.14.2.5.1 Automotive Due to concerns over vehicle bombs, the following recommendations should be followed when designing parking areas and site traffic control:

- Maintain a minimum perimeter of 30 m (100 ft) from the building.
- Utilize concrete barriers at the curb.
- When possible, have all cars park at a distance from the building.
- Reduce or eliminate underground parking, immediately under the data center building.

If possible, data centers should not be located in buildings adjacent to mid or high-rise parking garages.

If possible, elevators should never go directly from the parking garage to office space. Elevators should open and discharge into the lobby.

Parking garages should contain emergency phones or intercoms spaced no less than every 18 m (60 ft). Each telephone or intercom should be clearly marked as such, and should be illuminated with blue or some other locally accepted color associated with police or security.

Any onsite parking facility should address the security of pedestrian and vehicular traffic. Surveillance is crucial for security in parking garages and is capable of providing adequate coverage. Key considerations in protecting property and safety include the placement of cameras in the following locations:

- Entrance and all exits
- Guard and cashier booths
- Elevator lobbies and elevators
- Ramps, driveways, and emergency call stations

The following is a list of potential threats that should be considered when assessing the risk of parking areas within or adjacent to data center buildings:

- assault;
- carbon monoxide;
- chemical, biological, radiological, nuclear, or explosive incidents;
- explosion;
- fire;
- medical emergencies;
- robbery;
- terrorism;
- theft.

12.14.2.6 Natural threats and concerns

If possible, the data center should not be located within 80 km (50 mi) of an active volcano, earthquake fault line or high erosion area.

The data center should not be located in any area where there is a substantial risk of flooding from dams, oceans, lakes or other bodies of water.

The data center should not be located on a flood plain.

The data center should not be located below grade.

See Section 6: Site Selection for other factors regarding the location of the data center.

12.14.2.7 Chemical, biological, radiological, nuclear and explosives

Preparation for potential CBRNE threats should be conducted by security and operations personnel for each data center. Each data center should:

- include CBRNE threat response in the security plan;
- classify threats and the appropriate response;
- include coordination with local EMS and law enforcement;
- include the CBRNE response in the disaster recovery/business continuity planning process.

Nuclear power plants should be at least 80 km (50 mi) away.

The data center site should not be located within a 13 km (8 mi) radius of defense contractors or installations, government laboratories, or military facilities.

Explosions, whether accidental, because of sabotage or workplace violence or terrorism all should be considered as a threat to the data center building and computer room. The risks associated with explosions or bombs include:

- Injury or death of occupants.
- Structural damage to the building.
- Damage to the equipment and contents of the building.
- Interruption of operations (downtime).

12.14.2.8 Medical disasters and epidemics

The data center should have personnel trained in first aid and cardiopulmonary resuscitation on duty anytime the data center site or buildings are occupied.

First aid supplies should be located in places and marked for easy identification and quick access in the event of an emergency.

First aid supplies should include automatic defibrillator(s) in a quantity recommended by the manufacturer to serve the number of occupants and buildings.

12.15 Building shell

12.15.1 Recommendations

12.15.1.1 General

The data center should have an evacuation plan, including procedures on notifying all building occupants and posted evacuation routes.

Public tours should not be conducted in areas where sensitive computer operations are active, personal or sensitive data is visible, or high-value items are stored. If public tours of the data center and/or computer room are conducted, cameras and camera phones should be prohibited.

All areas through which data passes (e.g., entrance rooms, TRs, media storage rooms, computer rooms) should have some level of access control installed.

High-value computer, satellite, network equipment and other hardware/software should be stored in rooms with EAC to ensure that only authorized personnel enter, and to provide a tracking log in the event of loss.

Media storage, waste disposal, and chemical storage should be separated from computer, network and telecommunications equipment.

All service personnel, including janitorial, technical, and construction contractors, should be prescreened by security. Unscreened substitutes should be denied access to the site/building/data center.

12.15.1.2 Doorways and windows

Skylights, light monitors, atriums, open courts, light courts, windows or any other openings that penetrate the security of the roof should be approved by the security designer, including appropriate countermeasures to provide security appropriate with the area or room.

All heating, ventilation and air conditioning openings larger than 5100 mm² (8 in²) should have some form of barrier installed to prevent unauthorized entry into the building. This recommendation also applies to any other utility openings that penetrate the roof or walls.

Doors located in lobby areas must have glazing that conforms to local building codes. View panes and glass doors must consist of burglar-resistant glass.

All exterior doors should be at least 1.3 mm (16 gauge) steel reinforced solid core.

Roof hatches should be manufactured from a minimum of 1.3 mm (16 gauge) steel and should lock from the inside only.

When ladders for the rooftop are mounted on the building exterior, a security ladder cover should protect the first 3 m (10 ft) of the ladder.

All permanent roof access should be from the interior of the building.

Doors leading to the roof should meet the security requirements for exterior doors, including double-cylinder deadbolt locks.

Windows should not be placed in the computer room, storage areas, equipment rooms, restrooms, locker or utility rooms. If windows are necessary or preexisting, the windowsill must be at least 2.4 m (8 ft) above finished floor or any other surface that might provide access.

Window frames should be constructed with rigid sash material that is anchored on the inside and is resistant to being pried open.

The doors to all utility rooms, entrance rooms, TRs, and computer rooms should be locked at all times when not in use. Doors to these rooms should be equipped with door position sensors that trigger an alarm if the door is propped or held open for more than 3 minutes.

12.15.1.3 Signage and displays

All closed, limited-access, restricted, and secured areas should be designated by the use of prominent signage.

Computer room, secure areas and sensitive areas should not be located on all publicly accessible directories, signs and maps.

12.15.1.4 Construction

When the data center is being planned for an existing structure, the security survey should include a structural analysis of the floors, ceilings, and walls to determine the estimated time needed to penetrate them.

Added intrusion alarm and surveillance systems should be designed when the resistance to penetration of any exterior or interior ceiling, wall or floor is identified a risk. This includes open plenum areas above dropped ceilings that extend over controlled areas or are separated only by drywall.

Exterior building doors should be constructed of solid metal, wood, mesh reinforced glass or covered with a rated metal screen.

When possible there should be no external windows or doors leading into the computer room.

12.15.1.5 Elevators

Elevators opening to secure areas should have one or more electronic access control systems to ensure proper identification and authentication of passengers that visit the selected floor.

If possible, separate elevators should be designed to serve secured or sensitive areas.

12.15.1.6 Emergency exits

Emergency exits should be configured so they are only capable of being operated from the inside.

Planners should consider installing automatic door closers and removing door handles from the outside of the emergency exit doors, discouraging use of the door to reenter the facility.

12.15.1.7 Utilities

All utility feeds should be located underground. If utilities must enter the data center above ground, they must do so at the highest possible distance above ground and must be enclosed in a conduit until safely inside the building shell.

12.15.1.8 Hazardous material storage

Caustic or flammable clean fluids should always be stored in closets or rooms designated for that purpose. They should never be stored in entrance rooms, computer rooms, media storage rooms, TRs, or other locations where telecommunications, network, or computer equipment is installed or stored.

Cleaning fluids and all other caustic or flammable liquids should always be stored in approved containers, and in as small of quantities as possible.

12.16 Data center security design considerations

12.16.1 Recommendations

12.16.1.1 General

If possible, the computer room and data center support areas should be located on floors above grade, and in a multistory structure above the level known to be at risk for flood.

Prominently displayed signage, bearing language such as “Restricted Area” or “Controlled Area” should be posted at every access point into the data center.

If the data center occupies an entire campus, the warning should be posted at every vehicle entry point, and at regular intervals along the perimeter fencing or other barrier.

If security officers are assigned to monitor or patrol the data center areas, the frequency of patrol should be specified in the security plan or policy, and manual or electronic methods should be implemented that ensure the required frequency of patrols.

User access should be carefully monitored and controlled when any of the following circumstances apply:

- New hires
- Employees under any significant or extended disciplinary procedure or probation
- Employees who have been flagged due to unusual patterns of behavior or work hours

12.16.1.2 Office area security

Data center management should periodically conduct a live site survey, with the goal of identifying vulnerabilities in employee behavior, office and cubicle design and placement, as well as insufficient locks, doors, access control, alarms, and other countermeasures. If the data center does not have a security officer or department, the site survey should be conducted by a qualified outside security consultant or agency.

Employees should lock offices, desks, file cabinets at all times when not in use.

Sensitive, confidential or operational information should not be left on desks or in the open when not in use.

Mail should not be left for longer than one business day in open trays or boxes.

All planning charts, white boards and easels should be erased immediately after use.

Presentations, photographs and other documents should be marked as such if they are sensitive or confidential.

Any proprietary or confidential information leaks should be investigated and the appropriate modifications made to the security plan, including policy, procedure, and training.

If a crime has been committed, the appropriate federal, state or local law enforcement agency should be immediately notified.

The monitors and terminal displays for data center employees displaying sensitive or confidential information should be oriented in such a way as to not reveal the information to visitors or pedestrian traffic, commonly referred to as “shoulder surfing”.

12.16.1.3 Screening for weapons and contraband

When determined necessary by site conditions, threats, or other business indicators screening for weapons, explosives, and other contraband should be conducted for all personnel entering the data center.

Screening procedures should be included in the security plan.

Screening procedures may include the use of metal detectors, x-ray machines, explosive detectors, vapor detectors, particle detectors and/or canines.

12.16.1.4 Disposal of media and printed material

All confidential and proprietary information should be disposed of as dictated by data center policy and procedure.

Until media and printed material is destroyed, it should be stored in secure containers.

The pickup of confidential material for destruction should be supervised and logged. If the material is destroyed onsite, the process should be constantly supervised.

The disposal of confidential materials should be coordinated with the disaster recovery plan so that confidential material is protected even during a disaster.

12.16.1.5 Computer room special considerations

12.16.1.5.1 General

The security plan should contain special considerations for computer rooms.

All computer rooms and other areas mission critical to the operation of the data center should be considered restricted areas.

All security personnel should be made aware of the location of these areas.

All sides of a computer room, including ceiling and underfloor when those areas represent possible points of entry, should be protected by intrusion alarms and/or surveillance.

Electronic access control (EAC) shall be installed to track and control all ingress and egress to the computer room.

The use of access control, surveillance and alarms should be deployed as detailed in the policies and procedures outlined of the security plan to protect all computer rooms. Typical countermeasures deployed to protect computer rooms include:

- access control devices, including locks and barriers;
- CBRNE detection and protection;
- guard patrols;
- intrusion alarms;
- man traps;
- sensor driven alarms, including fire, smoke, water, and temperature;
- signage;
- surveillance.

In a “lights out” data center, or when employees and/or security personnel are not on site 24 hours per day, the intrusion alarms should be monitored by a central station.

Access to the computer room shall be controlled at all times.

All data center and computer room main and backup power supplies, entrance rooms, TRs, and other mission-critical utilities should be located in a secure area, with periodic inspections for sabotage.

Badging policy should be strictly enforced in the computer room. If an employee loses or forgets a badge, they should be required to wear a visitor badge, complying with any visitor escort policy(s) until such time that the badge is replaced or found.

The ability to authorize access in to the computer room should be limited to as few personnel as possible.

Computer room doors should remain closed and locked at all times. When possible, the door(s) should be alarmed to prevent propping open the computer room door.

All visitors and contractors should be required to sign an entry/exit log prior to entering the computer room, even when they are escorted.

Employees should be trained and encouraged to challenge unknown individuals found in the computer room.

Data centers should consider implementing the two-man rule for the computer room and other areas containing high value or sensitive contents.

All after hour entry/exit into the computer room should be tracked and reviewed by data center security or management personnel.

All removable recording media should be secured when not in use to reduce the likelihood of theft or damage.

Critical information storage areas, such as tape vaults should be prohibited for use as a work area.

It is a good practice to inspect all containers (including lunch boxes and briefcases) that leave the computer room, high-value, and sensitive areas. This helps prevent the unauthorized removal of proprietary information and storage media.

Authorized data center personnel should be required to remain with all hardware, software, and integration vendors while installation, maintenance or upgrades are being performed.

Unless job functions requires it, programming or coding personnel should not automatically be granted access to the computer room.

12.16.1.6 Construction

When possible, computer rooms should be physically separated from less secure areas. These areas should be marked as “restricted” or “controlled areas” consistent with signage policy.

Computer rooms should always contain a drainage system with a capacity large enough to handle potential leakage from sprinklers, chilled water pipes and any potable water pipes that pass through or adjacent to the computer room.

Computer room floor drains should always be fitted with back-flow valves.

The computer area ceiling should be constructed to drain or guide water away from the computer room.

The data center should have a supply of waterproof sheets or covers available to adequately cover all hardware, equipment, and supplies.

An industrial wet/dry vacuum cleaner should be kept close to the computer room in the event of a water leak. Vacuum cleaners used in the computer room should be micro filtered with a minimum 99.8% HEPA filter to prevent particles from being released back into the data center. Allowed particulate size may be predetermined thus the vacuum cleaner used should correspond to this determination.

12.16.1.6.1 Human factor

All employees should sign a confidentiality agreement when first hired.

Any abnormal or suspicious behavior on the part of employees or should be reported to facility security or data center management. Reportable activity would include:

- illegal use of or attempts to access restricted files;
- misuse of computer-related resources, including software and hardware;
- unauthorized destruction of any property;
- unauthorized loading of software or other information;
- examining wasted receptacles for sensitive information;
- presence in an unauthorized area or room.

There should be a periodic review of all keys, codes, magnetic cards, badges, and the personnel who have them to ensure current employees and contractors possessing keys, cards, codes, badges, and tokens still have a confirmed need to enter the computer room.

Human resources termination procedures should include a termination checklist that must be completed and require that all items returned before the employee receives their final paycheck and/or departing benefits. The checklist should include:

- the return of:
 - parking passess, badges and cards (including those mounted on vehicles).
 - company identification badges.
 - parking passes, badges and cards (including those mounted on vehicles).
 - all access cards, magnetic cards, proximity cards.
 - all keys.
 - all company mobile phones and radios.

- cipher locks and combination locks should have their codes immediately changed, or if permanently coded, new locks installed.
- voicemail passwords changed or deleted.
- PBX, computer, network, VPN and any other passwords changed or the user account deleted.
- computer, network, and telephone equipment returned.
- sensitive or proprietary information returned.
- data center owned software returned.
- data center owned property returned, including hardware, vehicles, uniforms, or any other real property.
- business memberships, calling cards, and credit cards should be surrendered and cancelled.
- business bills, such as expense reports, should be reconciled.

12.16.1.6.2 Theft

The data center should have a detailed asset log or database in which all computer, network, and telecommunications equipment is tracked, including removable media.

The use of an electronic asset program (EAP) is encouraged.

EAP tags should be affixed to all computers, network equipment, telecommunications equipment and removable media, such as magnetic and other media.

Sensors should be located at the entry/exit points for all locations where high-value or sensitive items are stored.

The EAP system should be integrated with the facility CCTV, access control and alarm systems so that entry/exit events can be recorded and suspicious events acted upon, and a time-stamped video of an event can be saved for investigative purposes.

Unique identification numbers should be permanently affixed, etched or stamped on all computer, network and telecommunications equipment.

In high-risk areas or situations, personal computers, laptops and other computer and network equipment should be permanently fastened to some part of the building or piece of furniture.

12.16.1.6.3 Eavesdropping

Computer rooms handling highly sensitive or valuable data should consider the installation of electronic field emanation reduction features (Tempest) to prevent electronic eavesdropping of data processing activities.

When highly sensitive or valuable data is presented the computer room and any data center area processing this data should be periodically checked for electronic eavesdropping devices.

12.16.1.6.4 Media

The computer room should contain a certified fireproof magnetic media cabinet/safe for the storage of critical documents and removable media.

The marking, handling, storing, destroying or using of storage media should be limited to specific authorized employees or contractors.

12.16.1.6.5 Fire prevention

Waste containers should always have metal lids to assist in quickly extinguishing fires.

Computer room waste receptacles should be emptied frequently to reduce the accumulation of flammable materials.

Caustic or flammable cleaning fluids shall not be stored in the computer room.

12.16.1.6.6 Dust

Computer room trash receptacles should be emptied outside the room to minimize the launching of airborne dust particles and air pollution.

Paper shredding, paper bursting and report separation equipment should always be located outside of the computer room.

Paper products and supplies should always be stored outside of the computer room.

If paper products are required to be stored in the computer room, then the supply should be limited to no more than one day's worth.

This page intentionally left blank

13 Building automation systems

13.1 Introduction

A building automation system (BAS) can be defined as an assemblage of products designed for the control, monitoring, and optimization of various functions and services provided for the operation of a building. Building systems typically include lighting, heating/ventilation/air conditioning (HVAC) systems, power, security, telecommunications services and life safety systems. Building automation's basic control technologies have been in existence for some time. The term *intelligent building* is used as a synonym for facilities using advanced BAS technology. BAS hardware is typically represented by one or more control and processing units and by a number of peripheral devices that control the operation of building systems. The control unit, based on the information supplied by the peripheral devices, as well as preset instructions, runs the system. The control unit can be as simple as a relay or timer to control a water heater on/off switch, or as sophisticated as a microprocessor operating on fuzzy logic. The cabling linking the control unit to the peripheral units can be unshielded twisted-pair (UTP), shielded twisted-pair, optical fiber, low-voltage, or even power cables.

A building monitoring system (BMS) enables an operator or building engineer to monitor some or all of the systems and equipment that manage the building environment. BMSs typically do not include the control and optimization functions of a BAS.

For the purposes of this standard, automated controls will be defined as a system that provides monitoring and control of a mechanical, electrical, or electronic system designed for a specific process or operation, such as automatic door openers, conveyor systems, or manufacturing machinery. Automated controls are not included in this standard.

Structured cabling provides several benefits to BAS, including systems that use IP protocols and those that do not. A standards-compliant structured cabling system provides a generic cabling system that can transport a wide range of protocols used for BAS, including Ethernet, ARCnet, and TIA/EIA-485-A, allowing the BAS to evolve without changing cabling. A generic standards-compliant structured cabling system is also designed to support a wide variety of other applications such as voice, LANs, and video, allowing the installed cabling to be efficiently utilized and allowing new services to be deployed without running new cable. A structured cabling system is also easier to administer and troubleshoot than an unstructured cabling system. The disadvantage of structured cabling is that some proprietary or legacy BAS equipment may not function properly on standard-compliant structured cabling, thus requiring the installation of two parallel networks, which should be segregated to minimize maintenance errors.

NOTE: For additional details on general BAS, refer to ANSI/TIA-862, and for data center communications cabling refer to Section 14 and ANSI/TIA-942.

13.2 Components

13.2.1 Cabling

13.2.1.1 Recommendations

Use standard structured cabling to support BAS as it provides the greatest flexibility in choice of a BAS system protocol, including BACnet, LONTalk, SNMP, XML, or HTTP (web) open protocols.

13.2.1.2 Additional information

Typically, BAS and BMS systems will require dedicated interconnect wiring between the mechanical systems of a building, such as boilers, chillers, chiller control systems, plumbing systems, water treatment, expansion tanks, and unit heaters, and the peripheral devices that provide the most immediate level of system monitoring and control. In most modern systems, this level of cabling is the most likely to require proprietary or nonstandard communications cabling. Because of the inherent limitations this type of cabling may have, these peripheral devices should be located within close physical proximity to the mechanical systems to which they are connected.

Most BAS and BMS systems can then utilize structured cabling infrastructure, including cabling pathways and telecommunications spaces, that can provide network connectivity between the peripheral devices and a central control unit. The cabling infrastructure can also be used for connection to the operator interface (workstation).

13.2.2 Hardware

13.2.2.1 Introduction

A BAS system includes the following components:

- Input/output devices – these provide control for a single function, such as a pressure meter, damper, or valve actuator;
- Unitary controllers – these provide limited control functions for a single mechanical system, such as an AHU, boiler, or water pump;
- Distributed processors – these provide control functions for one or more unitary controllers, or complex mechanical systems such as chilled water systems;
- Head end – this controls one or more distributed processors, and can include a connection for a laptop computer, one or more installed workstations, and servers that provide database functions; the head end can be used to provide real-time control, programming, and historical data that can be used to display trends under multiple environmental conditions. These trends can be used to provide ways to run a facility more efficiently.

13.2.2.2 Requirements

All hardware shall be fault tolerant; that is fail in the “open” or “on” condition.

The amount of hardware redundancy of equipment shall be determined by the Class of the data center (see Section 14.8).

13.2.3 Communications

13.2.3.1 Requirements

BMS/BAS systems shall conform to an open architecture specification for interfaces to the equipment and systems to be monitored, and support SNMP to report status to other management systems.

Monitoring of BMS/BAS alarms shall be available in the data center’s operations center or a similar location wherever the network is being monitored.

13.2.3.2 Recommendations

Many mechanical and electrical systems manufacturers are using open protocols for BAS connections, such as BACnet, LONTalk, SNMP, and HTTP. Each protocol has advantages and disadvantages, and each data center owner/operator will use different criteria to choose which system to use. Typically, however, control and head end systems can be designed to communicate with mechanical systems using any of these open protocols.

The building automation should interface with the data center central power and environmental monitoring and control system (PEMCS). The PEMCS should include a remote engineering console and manual overrides for all automatic controls and set points.

13.2.3.3 Additional information

Proprietary communications are becoming less common, but may still be an issue in an existing facility with an older BAS system. Where newer BAS systems may be added in such a facility, gateways can possibly be used to translate a proprietary protocol to a modern open protocol.

BASs that perform systems integration can communicate with mechanical systems and associated controllers supplied by different manufacturers, even if the BAS, mechanical systems, and controllers are installed at different times. The use of open protocols is essential to the success of systems integration.

13.3 Cabling design considerations

13.3.1 General cabling standards

13.3.1.1 Introduction

BAS cabling is intended to:

- integrate common services;
- accommodate diverse BAS applications;
- facilitate on-going maintenance and provide the capability of rapid deployment of BAS services;
- provide redundancy for safety and security requirements;

- satisfy requirements for systems and service such as:
 - building control and monitoring device services;
 - building automation data telecommunications;
 - audio;
 - telecommunications;
 - CCTV;
 - other low-voltage systems provided for building infrastructure.

13.3.1.2 Requirements

Networks supporting a mission-critical data center's BAS must be highly reliable and available. In the presence of equipment and cable faults, such as power outage, fires and broken cables, the communication should be designed to continue without interruption. To ensure security systems availability, the design and construction shall take into account the potential for network survivability. Specifically:

- dual (or multiple) network cabling may be considered to interconnect vital equipment and platforms; the dual network cables should be laid along different paths to minimize the chances of being damaged at the same time;
- separate TRs may be allocated to host the redundant equipment and be placed with sufficient physical separation to reduce the chances of all the equipment being damaged at once due to fire or some other localized catastrophic event.

Active components and equipment shall only be installed at the ends of the link and never within.

PoE midspan devices shall be installed in the TR, HDA, MDA, or where the link end resides.

13.3.1.3 Recommendations

Horizontal connection point (HCP) is similar in function and design as a consolidation point (CP). The number of links served by an HCP should be limited to 12. A HCP and a CP can be housed within the same zone box utilizing the same patch panel. If done this way, voice/data circuits should be assigned from the first port, as the BAS service should be assigned starting at the last port.

13.3.2 Topology

13.3.2.1 Requirements

Unless strictly specified otherwise by the BAS equipment manufacturer the cabling shall use a hierarchical star topology and follow the specifications of ANSI/TIA-862 for the portion of the BAS cabling that uses structured cabling. Some equipment, such as sensors, may require a topology other than a hierarchical star topology for the portion of the system that does not use structured cabling. In that case, follow manufacturer's instructions and local codes.

A centralized BAS must be deployed according to the manufacturer's instructions.

13.3.2.2 Recommendations

A centralized BAS can use the star topology even though this approach may have distance limitations.

A zone-based topology is recommended for large data centers.

Each cabinet/rack line-up (or pod) may have its own zone management enclosure or patchpanel. However, they shall allow for uninterrupted links for alarms and control systems monitoring from a central location.

13.3.3 Media

13.3.3.1 Introduction

Media are the different cabling materials used to transport, information and commands throughout the links.

13.3.3.2 Recommendations

BAS devices are interconnected with the same physical layer cabling that supports many other applications in the data center environment. As such, preferred BAS media are the same as other applications media. For additional information about the categories/classes of cabling, refer to Section 14.5.

13.3.3.3 Additional information

Media conversion is employed whenever two different media must interface to create a communications link. For example, a balanced twisted-pair to fiber media conversion unit may be used at the ends of an optical fiber link to allow for equipment with balanced twisted-pair ports to communicate with each other through longer distances or an environment with a higher EMI potential, depending on its pathway environment.

Some devices may require cable types not typically used in structured cabling. However, this may prevent future upgrades or vendor replacement.

13.3.4 Pathways and spaces**13.3.4.1 Introduction**

Pathways are the systems of cable trays, conduits, ducts and non-continuous supports used to route and protect the cables.

13.3.4.2 Requirements

The BAS cabling and communications systems cabling shall use separate pathways whenever there is likely to be electromagnetic interference between them.

Pathways and spaces used exclusively for BAS cabling shall be clearly marked as such.

13.3.4.3 Recommendations

Consider dedicated pathways for cabling dedicated to security and other mission-critical BAS systems.

Some BAS subsystems, such as life safety and security, may require separate pathways and spaces by local codes.

13.3.5 Cabling management and termination**13.3.5.1 Introduction**

Cabling management is the system and standards by which cabling and cabling infrastructure systems are installed, maintained and labeled both initially and throughout the data center's lifespan.

13.3.5.2 Recommendations

Data center BAS cabling should terminate in separate dedicated IDC blocks and patch panels, and not share IDC blocks and patch panels terminating communications links.

Data center BAS IDC blocks and patch panels should be clearly marked as such.

13.3.6 Enclosures**13.3.6.1 Requirements**

Enclosures for BAS are classified as either wall mountable or rack or cabinet mountable. Rack or cabinet mountable enclosures shall meet applicable ISO/IEC or ANSI requirements and allow for mounting within 19 in or 23 in racks.

External enclosures shall:

- provide enough securing points for a safe attachment to a wall;
- provide protection from outdoors harsh environment at least to the level required by the equipment installed inside;
- be lockable.

Internal enclosures shall:

- have dimensions allowing for fitting in wall spaces and provide enough space to terminate and properly protect incoming and outgoing wiring;
- be lockable, if required;
- meet local fire codes, wherever applicable, to ensure equipment survivability and/or reliability during a fire.

13.3.6.2 Recommendations

Enclosures dedicated to security systems should allow for installation of extra locks to prevent unauthorized access.

14 Telecommunications

This section specifies the minimum requirements for the telecommunications infrastructure of data centers and computer rooms, including single tenant enterprise data centers and multitenant internet hosting data centers. The topology specified in this standard is intended to be applicable to any size data center.

14.1 Access providers and outside plant

14.1.1 Security of underground telecommunications entrance pathways

14.1.1.1 Requirements

Telecommunications entrance pathways shall terminate in a secure area within the facility.

14.1.1.2 Recommendations

The secure area that houses the telecommunications entrance facility (pathway termination) should preferably be in a telecommunications entrance room that is separate from the computer room.

14.1.2 Pathway adjacencies with other systems

14.1.2.1 Requirements

The telecommunications entrance pathways shall be coordinated with other electrical underground pathways (e.g., conduits) and mechanical underground piping systems (e.g., water, waste) while maintaining pathway separation from physical and operational perspectives.

14.1.3 Entrance facilities

14.1.3.1 Introduction

The reliability of the telecommunications infrastructure as it relates to designing and provisioning of the telecommunications spaces (e.g., Entrance Facilities), can be increased by providing redundant cross-connect areas and redundant pathways that are physically separated. Although availability cannot be directly supplemented by additional provisioning; to achieve higher levels of redundancy it is common for data centers and associated computer rooms to have multiple access providers, redundant components such as routers, core distribution and edge switches. The telecommunications topology Classes listed in this standard are fully defined in Section 14.8 Telecommunications Infrastructure Classes.

14.1.3.2 Requirements

Access providers that serve the building shall be contacted to ascertain the point(s) of entry to the property and the requirements for their telecommunications cabling, terminations, and equipment. See also 14.1.5.1 and 14.2.5.2.

14.1.3.3 Recommendations

Class F2 and higher data centers should have diverse entrance facilities preferably with route diversity from the data center to different access providers. For example, a Class F2 data center may be served from multiple central offices and multiple service provider point-of-presences that enter the property at different locations.

Where possible, entrance facilities should be served from multiple entry points from the access provider's outside plant facilities. Each building point-of-entry should extend from the access provider outside plant facilities to different (or even opposite) sides of the building. Conduit duct banks and their associated maintenance holes, and other pathways from the access provider central offices and service provider point-of-presences to the building's entrance facilities should be separated by at least 20 m (66 ft) along their entire routes.

A conduit duct bank with appropriately placed maintenance holes that surrounds a data center and incorporates multiple building entrance facilities should be considered for the data center.

The location of each building entrance facility should be coordinated with routing of access provider pathways as well as internal pathways and should not conflict with the location of other building facilities such as power, gas, and water.

Telecommunications entrance cabling for data centers should not be routed through a common equipment room unless cabling is segregated from common access via conduit or other means.

See Section 14.2.5 regarding the design of the entrance facilities.

14.1.3.4 Additional Information

Where used for the purpose of demarcation, the entrance room typically has separate areas for access provider demarcation:

- Demarcation for low-speed balanced twisted-pair circuits (e.g., DS-0, ISDN BRI, telephone lines)
- Demarcation for high-speed balanced twisted-pair circuits (e.g., DS-1 [T-1 or fractional T-1], ISDN Primary Rate, E-1 [CEPT-1])
- Demarcation for high speed coaxial cabling circuits, (e.g., DS-3 [T-3] and E-3 [CEPT-3])
- Demarcation for high speed optical fiber circuits (e.g., SONET, Fast Ethernet, 1/10/40/100 Gigabit Ethernet).

If an access provider demarks their services in their racks, the customer typically installs tie cabling from that access provider's demarcation point to the desired patching location (e.g., meet-me racks, circuit patching racks) or user equipment.

14.1.4 Underground pathways**14.1.4.1 Recommendations**

Maintenance holes and hand holes on the data center property should have locks or other means of deterring access such as nonstandard bolts to resist unauthorized entry. The maintenance holes and hand holes should have intrusion detection devices connected to the building security system and monitoring of the maintenance holes and hand holes by CCTV.

14.1.5 Access provider coordination**14.1.5.1 Requirements**

Data center designers shall coordinate with all access providers to determine the access providers' requirements and to ensure that the data center's circuit, demarcation, and entrance facility requirements are provided to the access providers.

14.1.5.2 Additional Information

Access providers typically require the following information when planning entrance facilities:

- address of the building;
- general information concerning other uses of the building, including other tenants ;
- plans with detailed drawings of telecommunications entrance conduits from the property line to the entrance rooms, including location of maintenance holes, hand holes, and pull boxes;
- assignment of conduits and innerducts to the access provider;
- floor plans for the entrance rooms;
- assigned location of the access providers' protectors, racks, and cabinets;
- routing of cabling within entrance room (e.g., under access floor, over racks and cabinets, other);
- expected quantity and type of circuits to be provisioned by the access provider;
- media types and approximate distances of circuits to be provisioned by the carrier;
- service level agreements;
- detailed schedules for the project including date that the access provider will be able to install entrance cabling and equipment in the entrance room and required service activation date;
- requested location and interface for demarcation of each type of circuit to be provided by the access provider;
- carrier office diversity desired – preferably at least two separate access provider offices and service provider point-of-presences;
- carrier route diversity desired – preferably a minimum distance between any two routes of at least 20 m (66 ft) along their entire routes;
- specification of pathways to be used for access provider cabling (e.g., aerial cabling allowed or all underground);
- requested service date;
- name, telephone number, and e-mail address of primary customer contact and local site contact;
- security requirements for lockable containment and cabinets.

The access providers typically provide the following information:

- space and mounting requirements for protectors and terminations of balanced twisted-pair cabling;
- quantity and dimensions of access provider racks and cabinets or space requirements if they are to be hosted in client racks and cabinets;
- power requirements for equipment, including receptacle types;
- access provider equipment service clearances;
- location of serving access provider central offices;
- route of access provider cabling and minimum separation between routes;
- specification on pathways used (e.g., all underground or portions of routes that are served by aerial cabling);
- installation and service schedule.

14.1.6 Access provider demarcation

14.1.6.1 Introduction

The centralized location for demarcation to all access providers may be referred to as “meet-me” areas or “meet-me” racks. Access providers should provide demarcation for their circuits in a common owner specified rack or cabinet rather than in their own racks or cabinets. This simplifies cross-connects and management of circuits.

14.1.6.2 Recommendations

Separate meet-me/demarcation racks/cabinets for each type of circuit may be desirable – low speed, E-1/T-1, E-3/T-3, and optical fiber for STM-x/OC-x services as well as for Ethernet delivery. Cabling from the computer room to the entrance room should terminate in the demarcation areas.

14.1.7 Demarcation of low-speed circuits

14.1.7.1 Recommendations

Access providers should provide demarcation for their circuits in a common owner specified rack or cabinet rather than in their own racks or cabinets. This simplifies cross-connects and management of circuits.

Access providers should be asked to provide demarcation of low-speed circuits on IDC connecting hardware. While service providers may prefer a specific type of IDC connecting hardware (e.g., 66-block), they may be willing to hand off circuits on another type of IDC connecting hardware upon request.

Cabling from the low-speed circuit demarcation area to the main distribution area should be terminated on IDC connecting hardware near the access provider IDC connecting hardware.

Circuits from access providers are terminated using one or two pairs on the access provider IDC connecting hardware. Different circuits have different termination sequences, as illustrated in figure 54 and figure 55

Each 4-pair cable from the entrance room to the other spaces in the data center should be terminated in an IDC connector or an eight-position modular jack of compatible performance where the cable terminates outside the entrance room. The IDC connector or eight-position modular jack telecommunications outlet/connector should meet the modular interface requirements specified in IEC 60603-7 series of standards.

Pin/pair assignments should be as shown in the T568A sequence or, optionally, per the T568B sequence if necessary to accommodate certain 8-pin cabling systems. The colors shown are associated with the horizontal distribution cable. These illustrations depict the front view of the telecommunications outlet/connector and provide the list of the pair position for various circuit types.

14.1.7.2 Additional Information

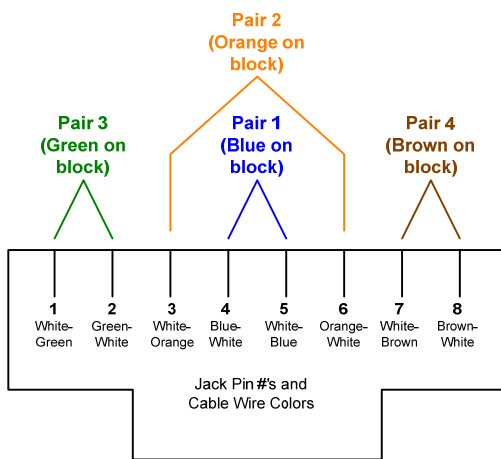
The conversion from access provider 1-pair and 2-pair cabling to 4-pair cabling used by the data center structured cabling system can occur either in the low-speed circuit demarcation area or in the main distribution area.

The access provider and customer IDC connecting hardware can be mounted on a plywood backboard, frame, rack, or cabinet. Dual-sided frames should be used for mounting large numbers of IDC connecting hardware (3000+ pairs).

14.1.8 Demarcation of E-1 and T-1 circuits

14.1.8.1 Introduction

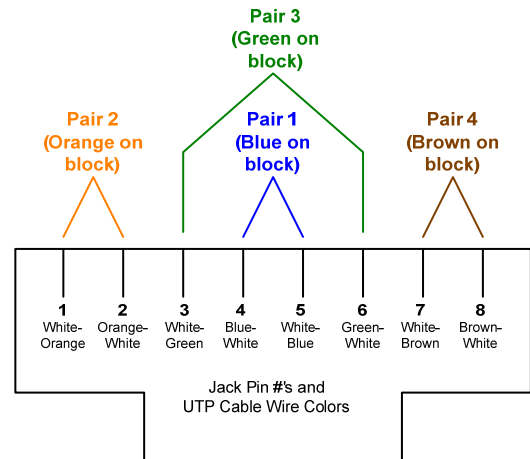
Coordinate with the local access providers that will install DS-1/E-1 DSX panels in the DS-1/E-1 demarcation area. Their equipment will preferably fit in 482.6 mm (19-inch) racks/cabinets. However, 584.2 mm (23-inch) racks/cabinets may be required by some local access providers, particularly in the United States and Canada.



(View from Front of Jack or Back of Plug)

- 1) Phone Lines: 1-pair cross-connect to Pair 1 (Blue)
- 2) ISDN BRI U-Interface (U.S.): 1-pair cross-connect to Pair 1 (Blue)
- 3) ISDN BRI S/T-Intf (Intf): 2-pair cross-connect to Pairs 1 & 2 (Blue & Orange)
- 4) 56k/64k Leased Line: 2-pair cross-connect to Pairs 3 & 4 (Green & Brown)
- 5) E1/T1: 2-pair cross-connect to Pairs 1 & 3 (Blue & Green)
- 6) 10Base-T/100Base-T: 2-pair cross-connect to Pairs 2 & 3 (Orange & Green)

Figure 54: Cross-Connection Circuits To IDC Connecting Hardware Cabled To Modular Jacks In The T568A 8-Pin Sequence



(View from Front of Jack or Back of Plug)

- 1) Phone Lines: 1-pair cross-connect to Pair 1 (Blue)
- 2) ISDN BRI U-Interface (U.S.): 1-pair cross-connect to Pair 1 (Blue)
- 3) ISDN BRI S/T-Intf (Intf): 2-pair cross-connect to Pairs 1 & 3 (Blue & Green)
- 4) 56k/64k Leased Line: 2-pair cross-connect to Pairs 2 & 4 (Orange & Brown)
- 5) E1/T1: 2-pair cross-connect to Pairs 1 & 2 (Blue & Orange)
- 6) 10Base-T/100Base-T: 2-pair cross-connect to Pairs 2 & 3 (Orange & Green)

Figure 55: Cross-Connection Circuits To IDC Connecting Hardware Cabled To Modular Jacks In The T568B 8-Pin Sequence

14.1.8.2 Recommendations

The DSX-1 patch panels may require power for indicator lights. Thus, racks or cabinets supporting access provider DSX-1 patch panels should have at least one electrical circuit or power strip to power DSX-1 panels. As most DSX-1 facilities use -48 VDC or +24 VDC to power their indicators, provisions for dc power sources and fuse panels should be included in any DSX facility.

Rack or cabinet space should be allocated for access provider and customer patch panels, including growth. Access providers may require rack or cabinet space for rectifiers to power DSX-1 patch panels.

A single 4-pair cable can accommodate one T-1 transmit and receive pair. When multiple T-1 circuits are driven through a multipair cable arrangement, multiple cables should be provided; transmit signals should be driven through one multipair cable and the receive signals driven through a separate multipair cable.

If support staff have the test equipment and knowledge to troubleshoot T-1 circuits, the DS-1 demarcation area can use DSX-1 panels to terminate T-1 cabling to the main distribution area. These DSX-1 panels should have either modular jacks or IDC terminations at the rear, although wirewrap terminations are acceptable and may still be used.

DSX-1 panels for the main distribution area can be located on the same racks, frames, or cabinets as the ones used for distribution cabling. If DSX panels are separate, they should be located in a space adjacent to the racks or cabinets used for distribution cabling.

The owner or the owner's agent may decide to provide multiplexers (e.g., M13 or similar multiplexer) to demultiplex access provider T-3 circuits to individual T-1 circuits. With consideration multiplexers may be placed in the computer room, extending the distance from the entrance rooms that T-1 circuits can be provisioned. T-1 circuits from a customer-provided multiplexer should not be terminated in the entrance room T-1 demarcation area.

The coaxial or optical fiber connecting hardware can be located on the same or separate racks, frames, or cabinets as the ones used for other access provider patch panels. If they are separate, they should be adjacent to the racks/cabinets assigned to the access provider's equipment.

As with other services, the access provider should be consulted to determine and agree to the format of the demultiplexed services from an E-1 carrier. The normal practice is to have these services provided via telecommunications outlet/connectors.

Access providers should be asked to hand-off T-1 circuits on RJ48X jacks (individual 8-position modular jacks with loop back), preferably on a DSX-1 patch panel mounted on a customer-owned rack installed in the DS-1

demarcation area. Patch panels from multiple access providers and the customer may occupy the same rack or cabinet.

14.1.8.3 Additional information

Access providers can alternatively hand off DS-1 circuits on IDC connecting hardware. These IDC connecting hardware can be placed on the same frame, backboard, rack, or cabinet as the IDC connecting hardware for low-speed circuits.

The customer may request that the demarcation for E-1 or T-1 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See ANSI/TIA-942-1 for distances for T-1 and E-1 circuits in data centers. As described in ANSI/TIA-942-1, note that customer side-DSX panels provide test access for circuits, but reduce maximum circuit distances.

14.1.9 Demarcation of T-3 and E-3 coaxial cabling circuits

14.1.9.1 Recommendations

Access providers should be asked to hand-off E-3 or T-3 coaxial circuits on pairs of female BNC connectors, preferably on a DSX-3 patch panel on a customer-owned rack/cabinet installed in the E-3/T-3 demarcation area. Patch panels from multiple access providers and the customer may occupy the same rack/cabinet.

Coordination with the local access providers should involve the installation of DS-3 DSX panels in the DS-3 demarcation area. This equipment should be mounted in 482.6 mm (19-inch) racks or cabinets in order to maintain consistency with other racks/cabinets. However, 584.2 mm (23-inch) rack/cabinets may be required by some local access providers, particularly in the United States and Canada.

If support staff have the test equipment and knowledge to troubleshoot E-3 or T-3 circuits, the E-3/T-3 demarcation area can use DSX-3 panels to terminate 734-type coaxial cabling to the main distribution area. These DSX-3 panels should have BNC connectors at the rear.

The DSX-3 patch panels may require power for indicator lights. Thus, racks/cabinets supporting access provider DSX-3 patch panels should have at least one electrical circuit and a power strip. As most DSX-3 facilities use -48 VDC or +24 VDC to power their indicators, provisions for dc power sources and fuse panels should be included in any DSX facility.

Allocate rack/cabinet space for access provider and customer patch panels, including growth. Access providers may require rack/cabinet space for rectifiers to power DSX-3 patch panels.

Cabling from the E-3/T-3 demarcation area to the main distribution area should be 734-type coaxial cable. Cables in the E-3/T-3 demarcation area can be terminated on a customer patch panel with 75-ohm BNC connectors, or directly on an access provider DSX-3 patch panel. Access provider DSX-3 patch panels typically have the BNC connectors on the rear of the panels. Thus, BNC patch panels for cabling to the main distribution area should be oriented with the front of the patch panels on the same side of the rack/cabinet as the rear of the access provider DSX-3 panels.

All connectors and patch panels for E-3 and T-3 cabling should use 75-ohm BNC connectors.

14.1.9.2 Additional information

The customer may request that the demarcation for E-3 or T-3 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See the applicable cabling standard (e.g., ANSI/TIA-942-1) for maximum distances of T-3 and E-3 circuits over coaxial cabling in data centers. As described in ANSI/TIA-942-1, note that customer side-DSX panels provide test access for circuits, but reduce maximum circuit distances.

14.1.10 Demarcation of optical fiber circuits

14.1.10.1 Recommendations

Access providers should terminate optical fiber circuits on optical fiber patch panels installed on racks or cabinets in the fiber demarcation area. Optical fiber patch panels from multiple access providers and the customer may occupy the same rack/cabinet. The optical fiber interface should comply with requirements defined in the cabling standards being followed (e.g., IEC 61754-20 [duplex LC-APC]). If requested, access providers may be able to provide a different format connector that is compatible with existing connector formats being used to simplify equipment cord and patch cord requirements.

Coordination with the local access providers should involve the installation of optical fiber patch panels in the optical fiber demarcation area. This equipment should be mounted in 482.6 mm (19-inch) racks or cabinets in order to maintain consistency with other racks/cabinets. However, 584.2 mm (23-inch) rack/cabinets may be required by some local access providers, particularly in the United States and Canada.

Cabling from the optical fiber demarcation area to the main cross-connect in the main distribution area should be single-mode optical fiber cabling. If the access providers provide services terminated in multimode optical fiber cable, the cabling from the fiber demarcation area to the main cross-connect (MC) in the main distribution area can also include multimode optical fiber cabling.

14.1.10.2 Additional information

The customer may request that the demarcation of optical fiber circuits be provisioned in the MDA rather than in the entrance room to ensure that service provision performance requirements and onward de-multiplexed circuit distance restrictions are not exceeded.

14.1.11 Aerial service to facility

14.1.11.1 Requirements

Routes for antenna access pathways shall follow same provisioning guidelines from availability and security perspective as the terrestrial data pathways.

14.1.11.2 Recommendations

The use of aerial cabling for telecommunications cabling into the data center should be considered only after other cabling distribution methods are first considered. Aerial cabling should generally be avoided because of vulnerability to outages. Aerial cabling route selection should take into consideration, a number of factors including; terrain, soil conditions, aesthetics, proximity to direct-buried and underground utilities, access and other factors.

Customer owned satellite dish farms or aerial towers should be located as close as possible to the perimeter of the facility in a secure area if practicable.

14.1.12 Underground pathway types and quantities to facility

14.1.12.1 Recommendations

The data center should include multiple duct banks from property line to data center with customer owned maintenance holes.

Duct bank should consist of a minimum of four 100 mm (4 in) conduits. If initial plans include more than three access providers providing service to the facility, one additional 100 mm (4 in) conduit should be provided for every additional access provider.

14.1.13 Redundancy of underground pathways

14.1.13.1 Recommendations

Redundant duct banks should have a 20 m (66 ft) separation minimum along the entire route from the property line to the facility.

Where possible, redundant maintenance holes should be connected with at least one 100 mm (4 in) conduit.

14.1.14 Security of underground pathways

14.1.14.1 Recommendations

When multiple access providers are providing service to the facility, coordination of security requirements of each individual access provider should be within the secure space.

14.2 Telecommunications spaces

14.2.1 Design and structural considerations

14.2.1.1 Requirements

Data center telecommunications spaces such as the main distribution area(s) and entrance room(s) shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

The computer room shall provide an operational environment in line with the limits and requirements set out in the applicable telecommunications cabling and data center standards for an M₁I₁C₁E₁ environment (see ISO/IEC TR 29106).

See Section 7 regarding architectural requirements and recommendations for telecommunications spaces, including door sizes and ceiling heights.

14.2.1.2 Recommendations

Where seismic requirements dictate consider using passive dampers to provide base isolation and building energy dissipation.

14.2.1.3 Additional information

Where the HVAC and cabinet solution has been designed to suit, having a ceiling partition where hot air can be fed into and directed to the air handling units thus preventing the hot air from recirculating into general room space is better than having a high ceiling alone.

14.2.2 Airborne particles created by telecommunications pathways components**14.2.2.1 Requirements**

Avoid metal whiskers, which can become airborne and disrupt equipment, by using floor tiles, raceways, racks, cabinets, stringers or other material in the computer room that are not:

- tin plated;
- zinc electroplated;
- conductive painted surface finish.

They shall instead be pregalvanized (G90), wrought aluminum alloy, stainless steel, hot-dipped galvanized (HDC or Galvanneal), or powder-coated finish.

14.2.2.2 Recommendations

Airborne particles can further be minimized by:

- Doing all unpacking, cutting, and drilling outside the computer room
- Keeping cardboard boxes and manuals outside the computer room
- Prohibiting food or drink inside the computer room
- Avoiding carpets in computer rooms
- Using ceiling panels that have an impervious surface such as drywall panels with a vinyl covering
- Use of air filtration with regular replacement of filters
- Keeping printers, copiers, and tape media in separate rooms with separate HVAC systems
- Occasional professional cleaning of the access floor, subfloor, and overhead ducts.

14.2.3 Ramps**14.2.3.1 Requirements**

The maximum slope for ramps is 8 degrees from horizontal for movement of cabinets with equipment. However, some wheelchair accessibility regulations specify a maximum rise of 1:12, or about 4.8 degrees. Additionally the ramp shall be at least 900 mm (36 in) clear width, have hand rails on both sides, and have a 1.5 m (5 ft) clear landing at the top and bottom.

If the computer room has only one ramp, it shall meet AHJ accessibility requirements. One ramp for equipment and an elevator or ramp for wheelchair access is acceptable.

14.2.4 Computer room space allocation and layout**14.2.4.1 Recommendations**

Consider spreading out equipment with high electrical loads rather than clustering them to avoid creating hot spots and to avoid overloading of power distribution units.

Computer tapes should be located in a separate room from the computer room.

Production, development, and test systems should be in separate areas of the computer room, preferably in separate rooms served by dedicated networks.

Separate areas of the computer room may be designated to accommodate special structures or cabinets for equipment with high heat loads.

14.2.5 Entrances**14.2.5.1 Entrance rooms****14.2.5.1.1 Introduction**

The entrance room may include both access provider and customer-owned cabling. This space may include the access provider demarcation hardware and access provider equipment and the location where conversion takes place between cabling that is suitable for outside plant applications and cabling that is suitable for premises (i.e., inside plant) applications.

14.2.5.1.2 Recommendations

The entrance room should be outside the computer room proper to improve security. However, it may be placed in the computer room or consolidated with the main distribution area if cabling distances for circuits is an issue, security is not a issue, or other security measures are used to ensure security (such as escorting and monitoring the activities of all technicians in the computer room).

Additional entrance rooms may be required for redundancy or to serve areas of the computer room that need an entrance room nearby to support distance limited circuits such as T-1, E-1, T-3, and E-3.

The entrance room interfaces with the data center through the MDA. However, direct connections from IDAs or HDAs to the entrance rooms are permitted to avoid exceeding circuit distance limitations. The entrance room may be adjacent to or combined with the MDA.

14.2.5.2 Redundant access provider services**14.2.5.2.1 Introduction**

Having multiple access providers protects against total loss of service in the event of a service outage affecting one of the access providers but not the others. However, it is necessary to ensure that the access providers are not sharing facilities that would result in one or more single points of failure that would cause a total service outage, despite having multiple access providers.

14.2.5.2.2 Recommendations

Continuity of telecommunications access provider services to the data center can be improved by using multiple access providers, multiple access provider central offices, and multiple diverse pathways from the access provider central offices to the data center.

The customer should ensure that its services are provisioned from different access provider offices and the pathways to these access provider cabling centers and central offices are diversely routed. These diversely routed pathways should be physically separated by at least 20 m (66 ft) at all points along their routes.

14.2.5.3 Entrance room redundancy**14.2.5.3.1 Recommendations**

Multiple entrance rooms may be installed for redundancy rather than simply to alleviate maximum circuit distance restrictions. Multiple entrance rooms improve redundancy, but complicate administration. Care should be taken to distribute circuits between entrance rooms.

Access providers should install circuit-provisioning equipment in both entrance rooms so that circuits of all required types can be provisioned from either room. The access provider provisioning equipment in one entrance room should not be subsidiary to the equipment in the other entrance room. The access provider equipment in each entrance room should be able to operate in the event of a failure in the other entrance room.

The two entrance rooms should be at least 20 m (66 ft) apart and be in separated fire protection zones. The two entrance rooms should not share power distribution units or air conditioning equipment.

14.2.6 Redundant main distribution area**14.2.6.1 Requirements**

For each functional telecommunications space within a data center there shall be no more than two main distribution areas.

Both main distribution areas shall meet all requirements of the MDA as specified in the applicable data center standard.

14.2.6.2 Recommendations

A second main distribution area provides additional redundancy. Core routers and switches should be distributed between the two main distribution areas. Circuits should also be distributed between the two spaces.

A secondary main distribution area may not make sense if the computer room is one contiguous space, as a fire in one portion of the data center will likely require that the entire data center be shut down. The two main distribution areas should be in different fire protection zones, be served by different power distribution units, and be served by different air conditioning equipment.

14.2.7 Data center redundancy

14.2.7.1 Introduction

The availability of the telecommunications infrastructure can be increased by providing duplication of services and physically separated services, supplemented by additional cross-connect areas. It is common for data centers to have multiple access providers providing services, redundant routers, redundant core distribution, and edge switches. Although this network topology provides a certain level of redundancy, the duplication in services and hardware alone does not ensure that single points of failure have been eliminated.

14.2.8 Pathway and equipment support and attachment

14.2.8.1 Requirements

Two post racks, four post racks, cabinets and pathway systems shall be secured in accordance with AHJ, seismic zone requirements, and the planned long-term loading. When access floor systems are used, any one of the following methods shall be permitted:

- attachment to metal struts that are captured below the floor by two or more access floor stringers,
- attachment to metal struts below the access floor that are suitably attached to the permanent floor,
- attachment via threaded rod directly to the permanent floor.

14.2.8.2 Recommendations

In locations where seismic activity could create a potential risk, cabinets and four-post racks in the computer room should be anchored at their base to the permanent floor and preferably braced at the top (the raceway and/or overhead auxiliary framing can be used for this).

In locations where seismic activity could create a potential risk, telecommunications pathways should be braced per AHJ and applicable standards (see Section 8).

14.2.9 Miscellaneous considerations

14.2.9.1 Recommendations

Unpack equipment in the storage or staging area. Use a cart to move heavy equipment.

Any pull boxes or splice boxes for data center cabling (entrance cabling or cabling between portions of the data center) that are located in public spaces or shared tenant spaces should be lockable. They should also be monitored by the data center security system using either a camera or remote alarm.

Entrance to utility tunnels used for telecommunications entrance rooms and other data center cabling should be lockable. If the tunnels are used by multiple tenants or cannot be locked, they should be monitored by the data center security system using either a camera or remote alarm.

14.3 Telecommunications and computer cabinets and racks

14.3.1 General

As with all other systems of the data center – power, HVAC, and flooring – cabinets and racking systems provide the vital services of proper structural and secure housing for data center equipment. Active and passive equipment have different requirements for mounting, power, ventilation, and cable management.

14.3.2 Two post racks

14.3.2.1 Requirements

The following criteria shall conform to applicable codes, standards and regulations (e.g., EIA/CEA-310-E).

- Channel dimensions and spacing
- Channel hole dimensions and thread systems
- Channel equipment mounting hole vertical spacing (U or RU)
- Panel opening and usable aperture opening

Performance specifications and overall physical dimensions shall conform to applicable codes, standards and regulations (e.g., ATIS 0600336, EIA/CEA-310-E).

Two-post racks shall be constructed of noncombustible materials.

14.3.2.2 Recommendations

Maximum height should not exceed 2.4 m (8 ft).

14.3.3 Four post racks

14.3.3.1 Requirements

The following criteria shall conform to applicable codes, standards and regulations (e.g., EIA/CEA-310-E).

- Channel dimensions and spacing
- Channel hole dimensions and thread systems Channel equipment mounting hole vertical spacing (U or RU)
Panel opening and usable aperture opening

Performance specifications and overall physical dimensions shall conform to applicable codes, standards and regulations (e.g., ATIS 0600336, EIA/CEA-310-E).

Four-post racks shall be constructed of noncombustible materials.

14.3.3.2 Recommendations

Maximum height should not exceed 2.4 m (8 ft).

14.3.4 Cabinets

14.3.4.1 Requirements

The following criteria shall conform to applicable codes, standards and regulations (e.g., EIA/CEA-310-E).

- Equipment mounting rail dimensions and spacing
- Equipment mounting rail hole vertical spacing (U or RU)

Overall physical dimensions shall conform to applicable codes, standards and regulations (e.g., EIA/CEA-310-E, ATIS 0600336).

Options for cable access into the cabinet shall be available from both the top and bottom.

Access floor openings beneath cabinets for cable entry shall offer:

- protection against damage to the cables
- restrictions against intrusion of dirt and debris
- restriction of air passage.

Cabinets shall be constructed of noncombustible materials.

14.3.4.2 Recommendations

Maximum height should not exceed 2.4 m (8 ft). Width should conform to applicable codes, standards and regulations (e.g., EIA/CEA-310-E), allowing for the exceptions noted therein.

Top access ports should provide a means to be closed when not in use.

14.3.5 Cabinets and rack configurations

14.3.5.1 Recommendations

Select cabinets, racks, and vertical cable managers whose design minimizes obstruction of exhaust air and recirculation of hot air from behind the equipment to air intakes in the front of the equipment.

In data centers that employ hot aisle / cold aisle orientation, ensure that the warm air is always exhausted towards the hot aisle. Optical fiber and balanced twisted-pair ports are located at the rear of many servers.

To simplify patching and maintenance, structured cabling patch panels should be mounted so that the ports face the same direction as the network ports on the equipment to which they are patched. These ports are commonly on the rear of servers and the front of network switches.

For equipment that is cooled side-to-side (e.g., certain networking equipment), cabinets, racks, and vertical cable managers should be selected that introduce the least disruption to the proper functioning of the hot and cold aisles and that minimize recirculation of hot air toward the air intakes.

Finishes should conform to applicable codes, standards and regulations (e.g., ANSI/TIA-942, ATIS 0600336) – conductive finishes are recommended to ensure a good bond between equipment and rack or cabinet ground and to prevent oxidation of the base metal. For painted racks, a supplementary bonding/grounding busbar system may be used to ensure a good bond between equipment and rack or cabinet ground. Rack and cabinet bonding and grounding should comply with applicable codes, standards and regulations (e.g., ANSI/NECA/BICSI 607-2010).

Racks in entrance rooms, main distribution areas and horizontal distribution areas should have dimensions and cable management capacities in accordance with applicable codes, standards and regulations (e.g., ANSI/TIA-942).

With non-angled balanced twisted-pair or coaxial cabling patch panels, a minimum of one rack unit of horizontal cable management should be provided for each rack unit of patch panel. Larger vertical cable management is required if angled patch panels are used and horizontal cable managers are not installed.

Shorter power cords, equipment cords, patch cords, and keyboard-video-mouse (KVM) cabling should be specified to reduce the cable management density in the back of the rack or cabinet.

A ground busbar or 16 mm² (6 AWG) ground wire should be installed in each rack or cabinet, mounted on the backside of one upright running the entire height of the cabinet; to provide an easy access grounding facility within cabinet or rack. See Figure 56.

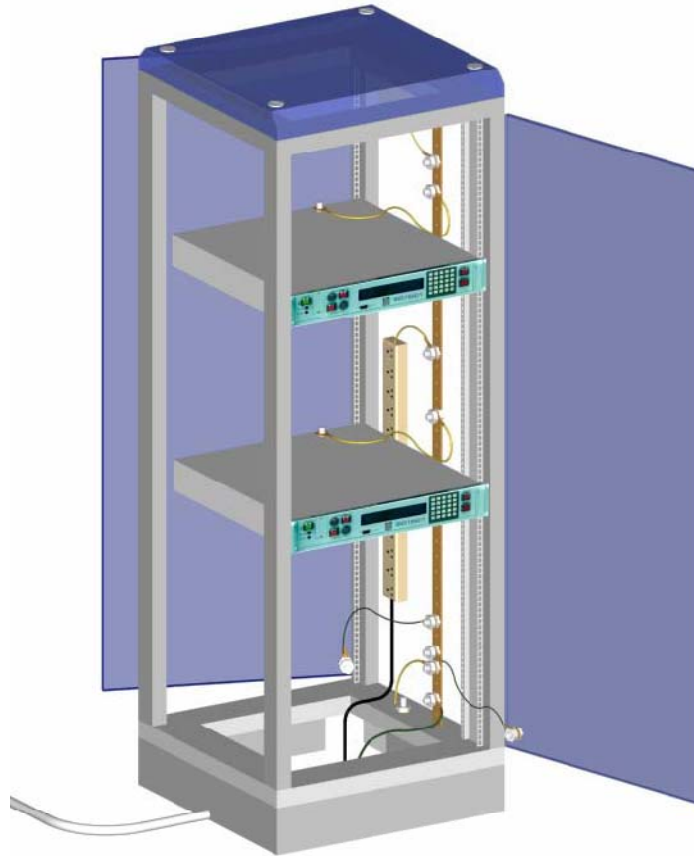


Figure 56: Cabinet Ground Busbar Example

14.3.6 Product configurations for racks

14.3.6.1 Recommendations

Rack depth should meet the mounting and protection needs of the equipment they are to host and, as a minimum, conform to the criteria established in applicable standards (e.g., CEA-310-E).

Each rack should have vertical cable managers, sized for maximum rack capacity attached on both sides. Vertical cable managers between two racks should be sized to serve both racks simultaneously.

14.3.7 Product configurations for cabinets

14.3.7.1 Recommendations

Equipment mounting rails should be adjustable front-to-rear and should have rack unit number indications (with numbers starting at the bottom).

Equipment mounting rail dimensions should conform with applicable codes, standards and regulations (e.g., CEA-310-E).

To ensure adequate airflow and to provide adequate space for power strips, telecommunications cabling and safe access for work, the cabinet depth should be at least 150 mm (6 in) deeper than the deepest equipment to be housed if the cabinet is 700 mm (27.5 in) wide or larger. If the cabinet is less than 700 mm (27.5 in) wide, 11.5 mm (0.45 in) depth should be added for every 10 mm (0.4 in) reduction from 700 mm (27.6 in) width.

Table 22: Example Of Cabinet Depth Guidelines

<i>Cabinet Width</i>	<i>Deeper than the deepest equipment housed in the cabinet</i>	<i>Additional depth for narrow cabinets</i>
600 mm (24 in)	150 mm (6 in)	115 mm (4.5 in)
700 mm (27.5 in)	150 mm (6 in)	N/A
750 mm (29.5 in)	150 mm (6 in)	N/A
800 mm (31.5 in)	150 mm (6 in)	N/A

Doors should be removable without tools. Door hinge orientation should be reversible or dual hinged.

Where mesh doors are used for ventilation, the doors should be a minimum 63% open to airflow for allowing chilled air entrance or evacuating heated exhaust air from the cabinet.

It is recommended that the following formulae be used to calculate door airflow capacity (*AFC*):

Airflow capacity calculations:

For cabinets with mesh doors

$$AFC_{MD} = \frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \quad (4)$$

For cabinets with solid doors with ventilation slots/openings

$$AFC_{SD} = \left(\frac{S_A}{S_D} \right) \times \frac{S_A}{A_C \times H_{RMU} \times N_{RMU}} \quad (5)$$

where:

AFC_{MD} is airflow capacity for cabinets with mesh doors;

AFC_{SD} is airflow capacity for cabinets with solid doors with ventilation slots /openings;

S_D is total surface area of the door panel, in mm² (in²);

F_{EA} is effective (open) area factor of the door mesh material (e.g., 0.65 [65%]);

S_A is integral area of the solid door with ventilation slots/openings, mm² (in²);

A_C is useable cabinet aperture opening at the door plane, mm (e.g., 450.85 mm [17.75 in]);

H_{RMU} is height of one rack unit (44.5 mm [1.75 in]);

N_{RMU} is quantity of rack units in the cabinet.

Example 1: Network cabinet or server cabinet design with mesh doors

- 19-in equipment cabinet,
- height: 42 RMU,
- mesh door with $F_{EA} = 0.65$, 1,930 mm x 635 mm (76 in x 25 in)
- 1 RMU = 44.5 mm (1.75 in),
- cabinet open aperture: 450.85 mm (17.75 in).

Airflow capacity:

$$AFC_{MD} = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \right) \times \left(\frac{1,930 \text{ mm} \times 635 \text{ mm} \times 0.65}{450.85 \text{ mm} \times 44.5 \text{ mm} \times 42} \right)$$

$$AFC_{MD} = \frac{1,225,550 \text{ mm}^2 \times 0.65}{842,639 \text{ mm}^2} = 0.9454$$

$$AFC_{MD} = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \right) \times \left(\frac{76 \text{ in} \times 25 \text{ in} \times 0.65}{17.75 \text{ in} \times 1.75 \text{ in} \times 42} \right)$$

$$AFC_{MD} = \frac{1,900 \text{ in}^2 \times 0.65}{1,304.63 \text{ in}^2} = 0.9467$$

Conclusion: the cabinet mesh door open airflow capacity (ACF_{MD}) falls within the recommended limits (e.g., 0.63-1.00 [63%-100%]).

Example 2: Network cabinet or server cabinet design with solid doors with slots/openings

- 19-in equipment cabinet,
- height: 42 RMU,
- solid door with ventilation slots:
- Solid door size: 1930 mm x 635 mm (76 in x 25 in),
- Slot size: 254.0 mm x 12.7 mm (10 in x 0.5 in) each, 2 vertical rows x 72 slots each,
- 1 RMU = 44.5 mm (1.75 in),
- cabinet open aperture: 450.85 mm (17.75 in).

Airflow capacity:

$$AFC_{SD} = \left(\frac{S_A}{S_D} \right) \times \frac{S_A}{A_C \times H_{RMU} \times N_{RMU}} = \left(\frac{254.0 \text{ mm} \times 12.7 \text{ mm} \times 2 \times 72}{1930 \text{ mm} \times 635 \text{ mm}} \right) \times \frac{254.0 \text{ mm} \times 12.7 \text{ mm} \times 2 \times 72}{450.85 \text{ mm} \times 44.5 \text{ mm} \times 42}$$

$$AFC_{SD} = \frac{464,515.2 \text{ mm}^2}{1,225,550 \text{ mm}^2} \times \frac{464,515.2 \text{ mm}^2}{842,638.65 \text{ mm}^2} = 0.3790 \times 0.5513 = 0.2089$$

$$AFC_{SD} = \left(\frac{S_A}{S_D} \right) \times \frac{S_A}{A_C \times H_{RMU} \times N_{RMU}} = \left(\frac{10 \text{ in} \times 0.5 \text{ in} \times 2 \times 72}{76 \text{ in} \times 25 \text{ in}} \right) \times \frac{10 \text{ in} \times 0.5 \text{ in} \times 2 \times 72}{17.75 \text{ in} \times 1.75 \text{ in} \times 42}$$

$$AFC_{SD} = \frac{720 \text{ in}^2}{1,900 \text{ in}^2} \times \frac{720 \text{ in}^2}{1,304.63 \text{ in}^2} = 0.3789 \times 0.5519 = 0.2091$$

Conclusion: the cabinet solid door with slots/openings airflow capacity (AFC_{SD}) is below the recommended limit (e.g., 0.63 [63%]). The cabinet design requires reconsideration.

NOTE: Input data and criteria used in the examples above are provided as samples only. For actual parameters, please, refer to the particular network cabinet or server cabinet design requirements.

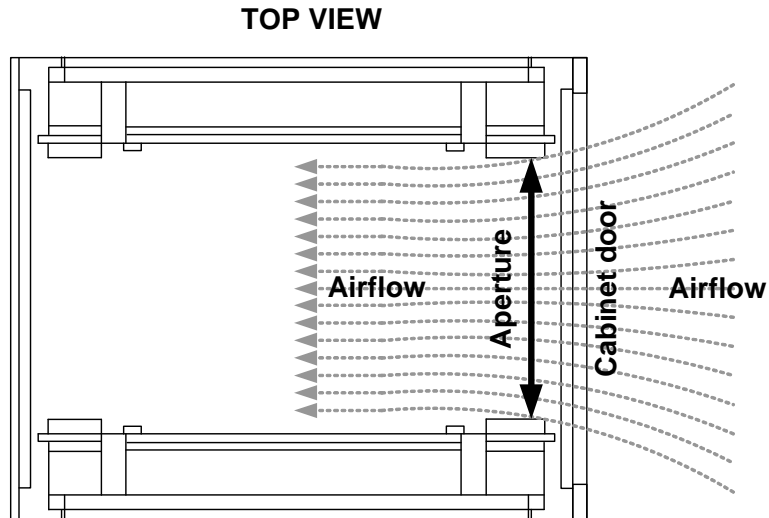


Figure 57: Cabinet Aperture Opening

Side panels should be removable and lockable without requiring intrusion into the equipment mounting area within the cabinet.

Blank panels should be installed in unused rack positions to maintain separation between hot aisles and cold aisles and prevent hot exhaust air from recirculating and mixing with chilled air at equipment in-takes. Blank panels also improve rigidity of cabinets.



Figure 58: Blank Panels Installed In Empty RUs

In applications where active equipment, patch panels and horizontal cable distribution are mixed, floor-tile-width (e.g., 600 mm [24 in] width) cabinets may lack adequate vertical cable management space.

In order to estimate the number of cables the cabinet can accommodate, the following formulae can be used:

$$N = \frac{S_U}{S_{cable}} \times f_{fill} = \frac{S_I - S_E - S_O}{S_{cable}} \times f_{fill}, \quad (6)$$

where

N is the number of cables the cabinet can accommodate,

S_U is the useful cabinet area, where cables can be installed, mm² (in²),

S_{cable} is the cable cross-sectional area, mm² (in²):

$$S_{cable} = \pi \times \frac{d_{cable}^2}{4} = 3.14 \times \frac{d_{cable}^2}{4} = 0.79 \times d_{cable}^2, \quad (7)$$

where

d_{cable}^2 is the cable diameter, mm (in),

f_{fill} is required or recommended cable pathway fill factor (e.g., 0.4 [i.e., 40 %]),

S_I is the cabinet internal area, mm² (in²):

$$S_I = (W_C \times f_D) \times (D_C \times f_D) = W_C \times D_C \times f_D^2, \quad (8)$$

where

W_C is cabinet width, mm (in),

D_C is cabinet depth, mm (in),

f_D is dimensional de-rating factor for internal space (e.g., 0.95);

S_E is the area allocated for active equipment and connecting hardware, mm² (in²):

$$S_E = A_C \times (D_C \times f_D), \quad (9)$$

where

A_C is useable cabinet aperture opening, mm (e.g., 450.85 mm [17.75 in]);

S_O is the area occupied by various obstructing elements, such as rails, power strips, etc., mm² (in²):

$$S_O = (S_I - S_E) \times f_O, \quad (10)$$

where

f_O is de-rating factor taking into account the obstructing elements (e.g., 0.3);

Illustrations of S_I , S_E , and S_O components are provided in Figure 59.

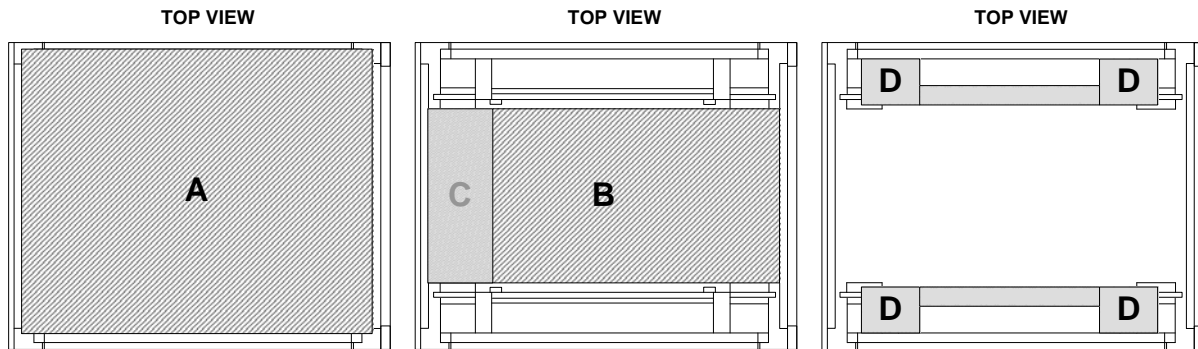


Figure 59: Illustration Of Components For Cable Capacity Formulae

As an alternative to separate calculations of each component provided above (which may be required for detailed design analysis), the following reduced formulae may be used:

$$N = \frac{D_C \times f_D \times f_{fill} \times (W_C \times f_D - A_C) \times (1 - f_O)}{0.79 \times d_{cable}^2} \quad (11)$$

where:

- A: cabinet internal area, S_I ;
- B: area allocated for active equipment and connecting hardware including area C, S_E ;
- C: “dead zone,” spare space behind active equipment and connecting hardware;
- D: area occupied by various obstructing elements, such as rails, power strips, etc., S_O .

NOTE: Boundaries of areas shown in Figure x2 are for illustration purposes only, actual boundaries may vary depending on the cabinet design and layout.

Where available, vendor cable manager calculators should be used to specify a correctly sized cabinet. Where such calculators are not available, Table 23 provides cable capacity estimates based on total available space outside of the equipment mounting area and between the rear equipment mounting rail (located at 762 mm [30 in] behind the front frame piece) and the rear frame and allowing 152mm² (0.24 in²) for vertical power strips, regardless of the presence or lack of vertical cable management accessories.

Cabinets should have adequate width and depth to avoid routing of cabling behind equipment exhausts where they may obstruct proper airflow.

Cable management capacity requirements should be calculated prior to either specifying a cabinet or even specifying a cabinet footprint.

Vertical cable management should be available and should be deployable in either the zero U space or, in deeper, more cabling intensive applications, in the equipment mounting space behind the mounted equipment.

Cabinets should include integral features for attaching any sort of external bracing structures.

Front and rear clearances around cabinets should conform to applicable codes, standards and regulations (e.g., ANSI/NFPA 70 or this standard – see clause 5.6.3.2). Minimum clearances should be optimized with either 150 degree or larger door swing, or split doors with hinges on both sides and latching in the center.

Table 23: Available Space For Calculating Cabinet Vertical Cable Capacity*Cross-sectional values in mm² (inches²) for noted cabinet depths and widths*

Cabinet Frame Depth (mm)	Cabinet Width (mm)			
	600 mm	700 mm	750 mm	800 mm
900	15700 (24)	45300 (70)	58400 (90)	71400 (111)
900a ³	10500 (16)	40100 (62)	53200 (82)	66300 (103)
900b ⁴	5400 (8)	35000 (54)	48000(74)	61100 (95)
950	21500 (33)	62100 (96)	80000 (124)	97900 (152)
950a ³	16300 (25)	56900 (88)	74800 (116)	92700 (144)
950b ⁴	11200 (17)	51700 (80)	69600 (108)	87500 (136)
1000	27300 (42)	78800 (122)	124300 (157)	124300 (193)
1000a ³	22100 (34)	73700 (114)	119200 (149)	119200 (185)
1000b ⁴	17000 (26)	68500 (106)	91300 (141)	114000 (177)
1050	32800 (51)	94800 (147)	122100 (189)	149500 (232)
1050a ³	27600 (43)	89600 (139)	117000 (181)	144300 (224)
1050b ⁴	22500 (35)	84500 (131)	111800 (173)	139100 (216)
1100	38600 (60)	111500 (173)	143700 (223)	175900 (273)
1100a ³	33500 (52)	106400 (165)	138600 (215)	170700 (265)
1100b ⁴	28300 (44)	101200 (157)	133400 (207)	165600 (257)
1150	44400 (69)	128300 (199)	165300 (256)	202400 (314)
1150a ³	39300 (61)	123200 (191)	160200 (248)	197200 (306)
1150b ⁴	34100 (53)	118000 (183)	155000 (232)	192000 (298)
1200	49900 (77)	144300 (224)	185900 (288)	227500 (353)
1200a ³	44800 (69)	139100 (216)	180700 (280)	222300 (344)
1200b ⁴	39600 (61)	133900 (208)	175500 (272)	217200 (337)

NOTES:

1. Standard front-to-rear mounting rail spacing = 750mm (29.5 in)
2. Front rail is set back 25mm (1 in) from cabinet frame
3. Capacity de-rated for one vertically mounted power strip
4. Capacity de-rated for two vertically mounted power strips
5. IMPORTANT: Capacities are calculated on available space. Vendor specifications need to be referenced to determine actual cable management capacity

NOTE: Use the cross sectional values from Table 23 to calculate the cable capacity of a cabinet per the following procedure:

$$N = \text{round_down} (A_{\text{cable management space}} \div A_{\text{cable}}) \times f$$

Where:

N = Number of cables

$A_{\text{cable management space}}$ = cross sectional space from Table 23 in mm² (in²)

A_{cable} = cross sectional area of cable, mm² (in²)

f = fill rate

For example, a 1050 mm (41.3 in) deep and 700 mm (27.5 in) wide cabinet with one power strip and 8 mm (0.31 in) diameter cable would be calculated as follows for a 40% fill rate:

$$A_{\text{cable management space}} = 89600 \text{ mm}^2$$

$$A_{\text{cable}} = \pi \times 4^2 = 50.24 \text{ mm}^2$$

$$N = (89600/50.24) \times 0.4 = 713.3758 = 713$$

14.3.8 Rack and cabinets installations

14.3.8.1 Requirements

Where the cabinets and racks are on an access floor, they shall be placed so that there are liftable tiles in front and behind each cabinet and rack. This typically means placing the rows of cabinets and racks parallel (rather than at an angle) to the rows of floor tiles and placing the front edge of the cabinets along the edge of the floor tiles to lock down the minimum number of tiles under the cabinets.

All overhead cable management (e.g., ladder racks, cable tray, etc) shall remain free of obstructions such as sprinklers, lighting, and electrical outlets (refer to Section 14.4.8 for additional considerations of overhead cable routing).

The designer shall anticipate the weight of the equipment in the racks and cabinets – ensure that the cabinets, racks and floors (both access floors and slabs) are rated to handle the expected mechanical loads.

Adequate power shall be available to all racks and cabinets that will hold active equipment and must be installed in accordance with applicable codes and the AHJ.

Each cabinet and rack shall be labeled on the front and back with its identifier. See Section 14.7 and applicable standards (e.g., ANSI/TIA/EIA-606-A-1) for additional information.



Figure 60: Cabinets Are Identified And Labeled

All patch panels, cables, equipment cords, and patch cords shall be properly labeled per applicable standards (e.g., ANSI/TIA/EIA-606-A-1).

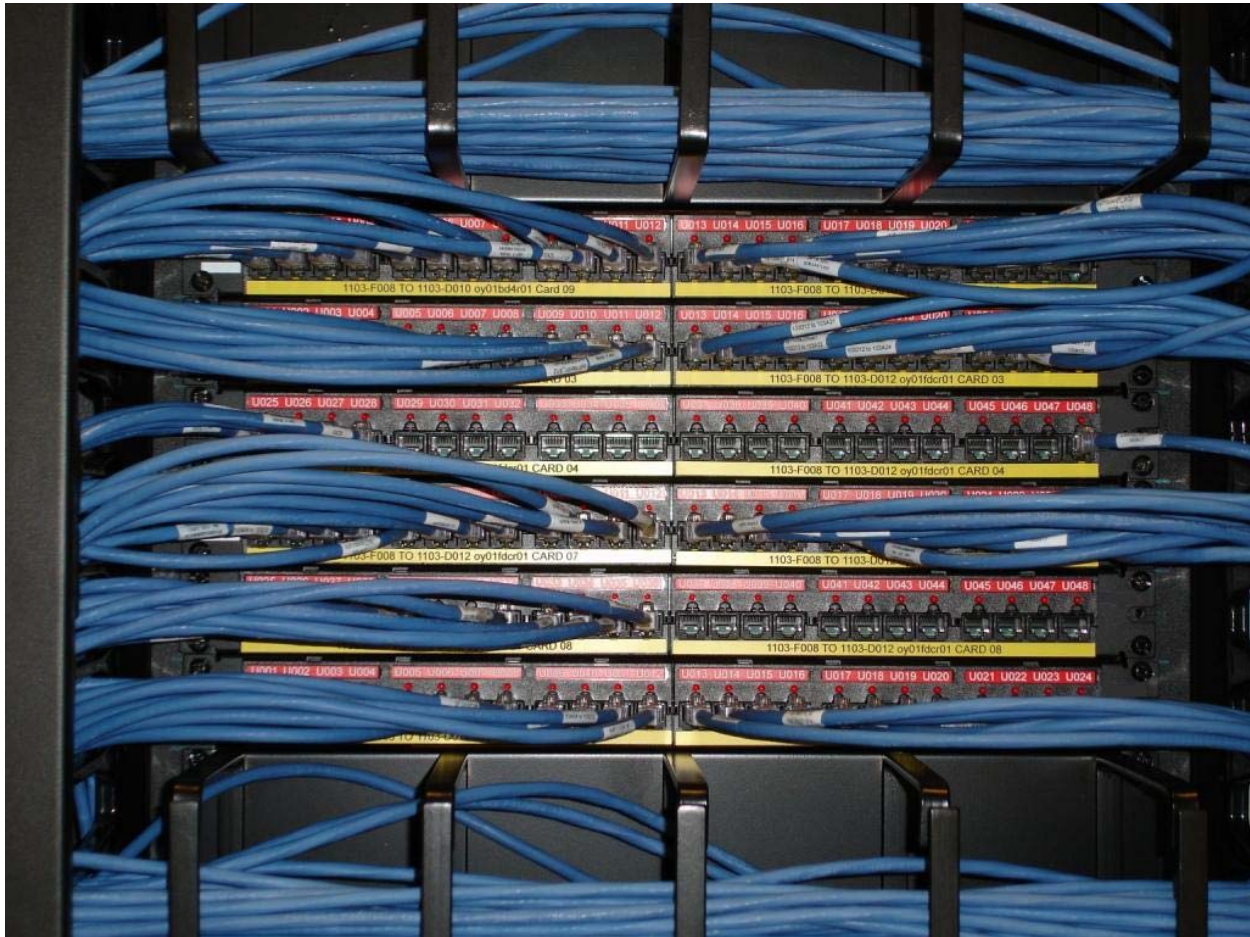


Figure 61: Termination Ports And Equipment Cables Are Clearly Labeled

14.3.8.2 Recommendations

Rack and cabinet layout designs should be harmonized with lighting (luminaire) delivery layout designs.

Anticipate growth and leave room for expansion when/if possible.

Power strips should be labeled with power distribution unit or panelboard identifier and circuit breaker number.

14.3.9 Rack installations

14.3.9.1 Recommendations

Equipment in the computer room should be mounted to rack or cabinet rails rather than placed on shelves, as equipment on shelves provides a return path for air between the rear and front of the cabinet or rack.

Floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings.

Consider using openings with gaskets or brush grommets to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See Figures 63 and 64 for examples.

Power cords should not be installed under equipment, mats, or other covering other than access floor tiles.

A dedicated pathway should be provided for equipment cords or patch cords within an MDA, IDA, or HDA that is separate from those used for horizontal and backbone cabling.

Ensure all active devices are properly supported and securely mounted to the rack to prevent equipment damage from improper installation.

In seismic zones, it is recommended that the design of the attachment methods and the installation be reviewed by a licensed structural engineer. Many jurisdictions will require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

To the degree possible, racks should be located on the raised floor so that a minimum of floor tiles are made unremovable by the racks, and attachment points are not located over floor tile stringers.

Mounting surface should be prepared for the specific anchors required for the application. Refer to manufacturer's and structural engineers recommended practices and verify those practices are acceptable to the AHJ. Racks in a line-up where they are properly attached together may require fewer anchors per rack than those installed as standalone units. When drilling into the mounting surface use proper technique to ensure dust or particles do not get air born. For example, vacuum or foam can prevent dust or particles while drilling in floors or walls.

Racks should be set in place and leveled throughout the line-up. Shimming of any anchoring point should not exceed 13 mm (0.5 in) unless specified by the project engineer. If racks require more than 13 mm (0.5 in) of shimming an engineered solution should be used to ensure rack line-ups are properly supported. Adjacent racks in the line-up should be ganged together before anchors are installed. Install anchors per manufacturer specification making sure all shims are properly located.

Some line-ups require additional bracing to meet customer specifications or local codes. Required bracing may be based on rack style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on rack lineup. All bracing should be installed before racks are populated.

14.3.10 Cabinet installations

14.3.10.1 Recommendations

Avoid empty cabinet or rack positions in equipment rows. Replace removed cabinets or frames and fill any gaps in a row of cabinets with a substitute blanking panel of the same height as the cabinet or frames to either side to avoid recirculation of air between hot and cold aisles. For the same reason, cabinets and racks should be installed with no blank spaces between them. In the case of vacant cabinets and racks, and where blank spaces exist in populated cabinets and racks, install blanking panels. Vertical cable managers can provide cable management and block recirculation of air between racks. Cabinets should be butted up against each other. Where possible, bayed cabinets should still share a side panel or include other means to seal the rear-to-front airflow path along the side of rack-mounted equipment.

Given a choice, where placing one edge of the cabinet creates unequal aisle sizes, the front aisle should be the larger one as it provides more working space for installation of equipment into cabinets and a greater area for providing cool air to cabinets.

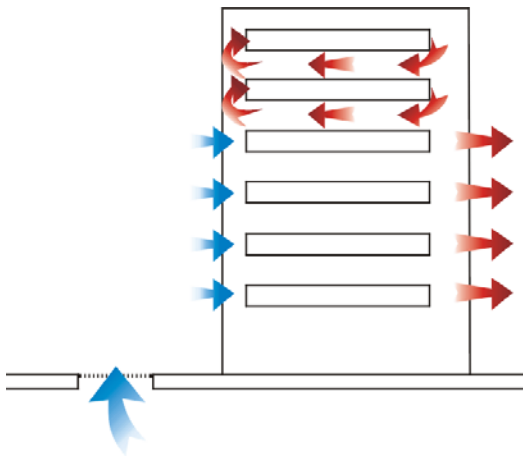


Figure 62: Effect Of Internal Hot Air Recirculation

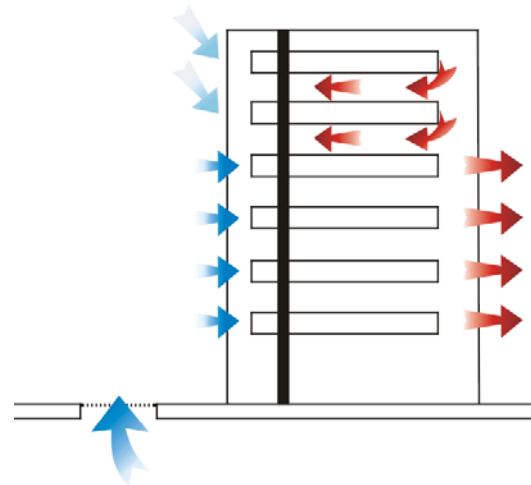


Figure 63: How Reducing Internal Hot Air Recirculation Reduces Input Air Temperature

On access floors, floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings taking into account anticipated growth.

Consider using openings with gaskets or brush grommets to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See the following figures for examples.

Power cords should be routed so that they are visible and accessible, not run under mats or other covering other than access floor tiles.



Figure 64: Gasket Seals Off Access Floor Tile Cutout In Vertical Cable Manager



Figure 65: Brush Grommet Seals Access Floor Tile Cutout Under Equipment Cabinet

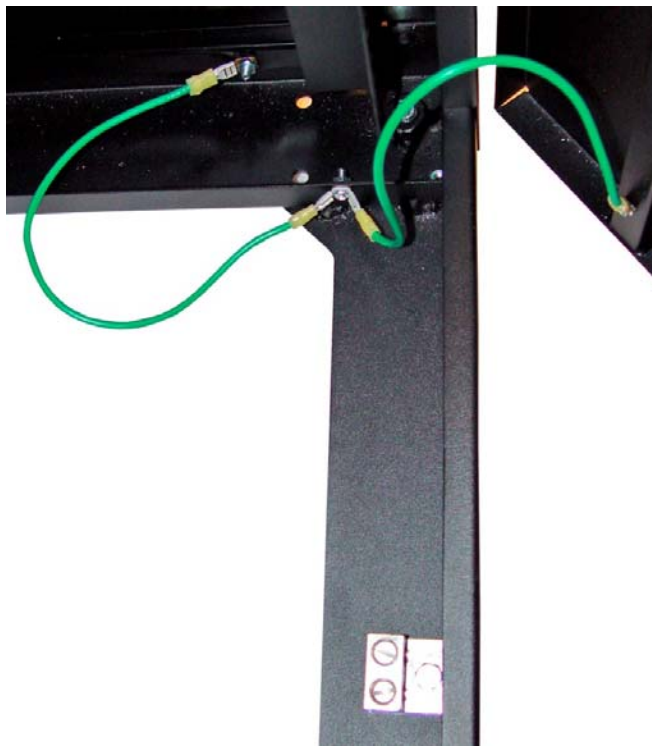


Figure 66: Cabinet Door And Side Panel Are Bonded To Cabinet Frame. Frame Ground Terminal Block Is In Bottom Of Picture

To avoid creating hot spots and avoid over loading of power distribution units consider distributing equipment with high loads relative to the average load in the data center across the computer room instead of clustering them.

Ensure all active devices are properly supported and securely mounted to the cabinet to prevent equipment damage from improper installation.

Plan equipment, power strip, cable manager, and cabling layouts in cabinets before making a major purchase. Either create detailed drawings or preferably create a mock up to ensure that:

- all equipment and cable managers fit properly;
- there is adequate space and access to power strips;
- there is adequate access to cabinet floor and top openings;
- there is adequate space for cable management;
- equipment can properly slide in and out as required;
- equipment intakes and exhausts are not blocked by cabling, cable management, or cabinet structure so that air can flow freely within the rack and to exit out the hot side;
- cabinets, racks, and vertical management do not have large openings for recirculation of air from hot to cold aisles.

When placed on an access floor, cabinets should be located so either the front of the cabinet or the rear of the cabinet coincides with a floor tile boundary to permit floor tiles to be lifted.

Temporarily remove any doors and panels that may interfere with the cabinet installation.

The mounting surface should be prepared for the specific anchors required for the application. Refer to manufacturer's recommended practice and verify those practices are acceptable to the local AHJ. Cabinets in a line-up where they are properly attached together may require fewer anchors per cabinet than those installed as standalone units. When drilling into the mounting surface use proper technique to ensure dust or particles do not get air born. Using a drill with attached vacuum is an effective way to prevent dust or particles while drilling in floors or walls.

On solid or slab floors, cabinets should be set in place and leveled throughout the line-up. Most cabinets are equipped with leveling feet. If leveling feet are not provided, consult manufacturer for proper shimming hardware.

On access floors, if cabinets in the line-up are to be ganged, attachment hardware should be installed before anchors are installed. Install anchors per manufacturer's specification, making sure all shimming hardware is properly located.



Figure 67: Method For Securing Racks And Cabinets On An Access Floor Using Threaded Rod Connected To Steel Channel Bolted To Concrete Slab

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable. Floor tile panels should have correctly sized and placed cutouts for the cabinet or equipment placed over them. The cutout should be under the cabinet/equipment cable opening and properly sized for the quantity and type of cables to be routed through the opening.

14.3.11 Thermal management in cabinets

14.3.11.1 Recommendations

There is no one thermal management configuration that works best in every instance. Each may be optimal depending upon different factors unique to the customer, application and environment. Serious consideration should be given to understanding the upfront installed costs as well as ongoing operation cost from an energy efficiency and maintenance perspective. At a minimum, equipment should be installed in cabinets with the air intake oriented toward the front of the rack or cabinet and the air exhaust oriented toward the rear of the rack or cabinet, when possible, with the cabinet rows oriented in a “hot aisle/cold aisle” configuration – rears of cabinets facing each other and fronts of cabinets facing each other.

Use of any supplementary cooling mechanisms on a cabinet must take into consideration its effect on the overall fluid dynamics of the air space and how other equipment will be affected.

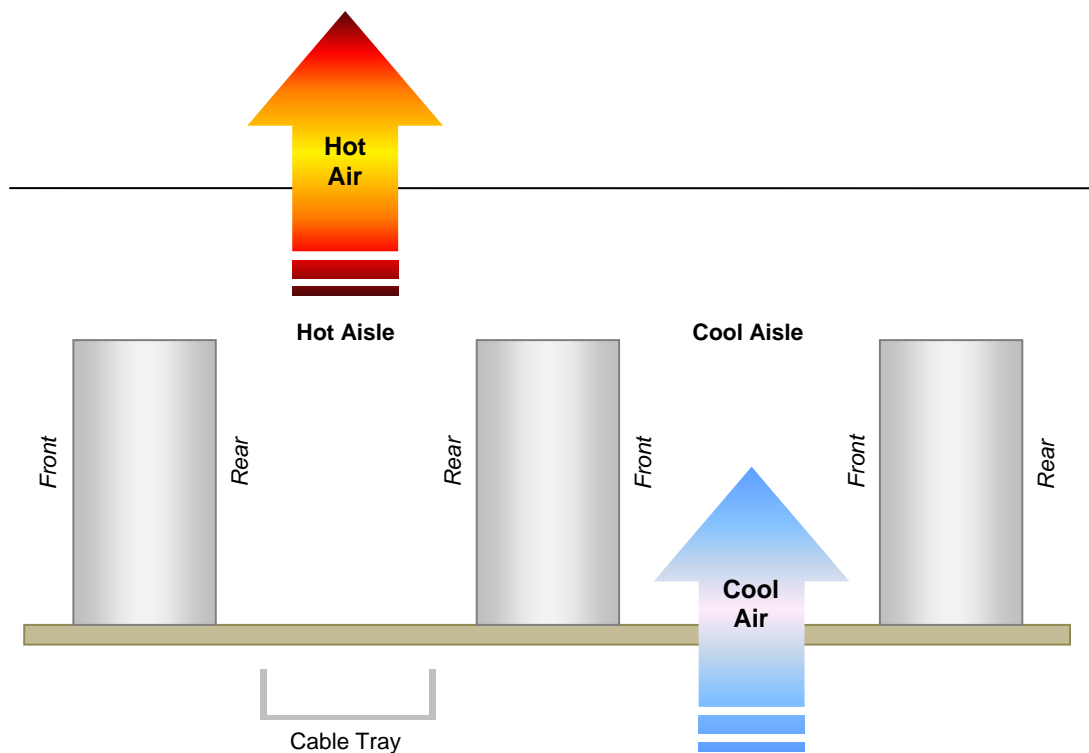


Figure 68: Hot Aisle/Cold Aisle Cabinet Layout

Considerations of supplemental cooling systems need to include criticality and required levels of redundant backup. Cabinets with good passive air management systems in well- designed rooms remove concerns about single points of failure and can support heat loads of twenty kW and higher.

Cabinet fans for cabinets specially designed to handle high heat loads should be on UPS power and have redundant power cords or be on transfer switches to ensure continuous operation.

Cabinet fans should be on separate circuits from the equipment in the cabinet as fans are susceptible to ground faults.

The perimeter of the equipment mounting area is also a path for cold air bypass or hot air recirculation and should be blocked accordingly.

Careful planning is needed for capacities, heat loads and redundancies required for desired availability and reliability. See Annex B.

14.3.11.2 Additional information

Specify/purchase the highest quality racks and rack components the budget will allow. They hold up better in the long run through numerous changes.

Over tightening mounting screws will strip out threads in the racks (especially the poorer quality racks). Minimum torque setting on drill/driver is usually sufficient to secure anything in the rack. Refer to manufacturer's specifications for recommended hardware. Specify toolless construction wherever possible.

Information Technology Equipment (ITE) original equipment manufacturers (OEM) cabinets may provide insufficient space to meet operational cable management requirements or cabling architecture.

Current generation servers will operate with, and high availability environments require, multiple network connections. For example, a single server might typically have two production LAN connections, one or two clustering or virtualization LAN connections, an out-of-band software management LAN connection, a hardware lights out management (LOM) LAN connection, and two (primary and secondary) SAN network connections. Additionally there may be redundant power supplies requiring two or more power cords per server. Therefore, in a server cabinet that houses twelve servers, the application could potentially encounter 72 balanced twisted-pair equipment cords, 24 duplex optical fiber equipment cords, and 24 power cords for a total of 120 individual cords, plus any KVM cabling.

Some line UPSs require additional bracing to meet customer specifications or local codes. All bracing should be installed before cabinet doors or panels are installed and before cabinet is populated. Required bracing may be based on cabinet style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on cabinet line-up.

Changes in floor tile cuts can be disruptive and time-consuming. To mitigate the change of reworks, floor tile panel cuts should be carefully planned, taking into account current and anticipated power and data cabling requirements, as well as all necessary route diversity considerations.

Cabinet roof fans and fan trays generally offer little benefit and can actually be counterproductive, creating hot spots within a cabinet particularly when used in conjunction with high airflow mesh front doors. Additionally these fans may disrupt the proper function of hot and cold aisles. Caution should be applied to any use of cabinet fans to assure they will enhance rather than disrupt the proper functioning of hot and cold aisle separation. Rear door fans can be used as long as the actual delivered fan capacity is not less than the cumulative throughput of the equipment fans in the cabinet.

In suboptimized spaces, hot aisle containment or cold aisle containment may compensate for otherwise inadequate cooling by isolating source air from return air.

NOTE: As an installation tip, make a floor cut template on cardboard or directly on the floor panel from the access opening in the cabinet being placed.

14.4 Telecommunications cabling pathways**14.4.1 General****14.4.1.1 Requirements**

Except where otherwise specified, data center cabling pathways shall adhere to the specifications of relevant cabling and containment specifications such as TIA-569-B, CENELEC EN 50174-2 or ISO/IEC 14763-2.

Pathways shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

The maximum depth of telecommunications cabling in cabling pathways (e.g., cable tray, cable ladder, or any other form of cabling pathway system) shall not exceed 150 mm (6 in) for a solid bottomed pathway regardless of the depth of the cable pathway. For cabling pathway systems that are not solid bottomed, the maximum depth of installed cabling shall be determined by the spot loading and pressure it exerts on the support points of the pathway system. See Table 24.

14.4.1.2 Recommendations

Where it is not possible to adequately size pathways for full data center occupancy, including future expansions and applications, consider other media (such as optical fiber) or different network architectures (such as distributed LAN and SAN switching) to reduce cabling requirements.

Table 24: Maximum Cable Stacking Height In Cabling Pathways

<i>L</i> <i>Distance between points of support</i>	<i>H</i> <i>Maximum stacking height in cable pathways</i>
0 mm (0 in)	150 mm (6.0 in)
100 mm (4 in)	140 mm (5.5 in)
150 mm (6 in)	137 mm (5.4 in)
250 mm (10 in)	128 mm (5.0 in)
500 mm (20 in)	111 mm (4.4 in)
750 mm (30 in)	98 mm (4 in)
1000 mm (40 in)	88 mm (3.5 in)
1500 mm (60 in)	73 mm (3 in)

Where: $H = 150 \text{ mm}/(1 + L \times 0.0007 \text{ mm})$
H = maximum stacking height (in mm)
L = distance between points of support (in mm).

14.4.2 Security

14.4.2.1 Requirements

Telecommunications cabling for data centers shall not be routed through spaces accessible by the public or by other tenants of the building unless the cables are in enclosed conduit or other secure pathways. Any pull boxes or splice boxes in a shared space or in a public area of the data center shall be fitted with lockable access.

14.4.2.2 Recommendations

Any maintenance holes or hand holes on the data center property should have a lock or other means to prevent unauthorized access.

14.4.3 Separation of power and telecommunications cabling

14.4.3.1 Requirements

To minimize coupling between power cabling and balanced twisted-pair cabling the separation and segregation between power cabling and balanced twisted-pair cabling shall follow the requirements defined in the cabling standards being followed.

AHJ may require a barrier or greater separation than specified in the cabling standards.

Where they are used, metallic cabling pathways shall be properly bonded and grounded as per AHJ requirements and applicable standards (e.g., ANSI/NECA/BICSI 607, ANSI-J-STD-607-A).

Refer to Sections 14.4.8.1 and 14.4.8.2 for additional considerations of overhead and underfloor cable routing.

14.4.3.2 Recommendations

For computer rooms that use the space under access floor systems for the routing of power and copper data cabling; allocate separate aisles for power and telecommunications cabling whenever possible. Where it is not possible to allocate separate aisles for power cabling and telecommunications cabling in the main aisles, then provide both horizontal and vertical separation of power cabling and telecommunications cabling in the same aisles. Provide horizontal separation by allocating different rows of tiles in the main aisles for power cabling and telecommunications cabling, with the power cabling and telecommunications cabling as far apart from each other as possible. Additionally provide vertical separation should be provided by placing the telecommunications cabling in cable trays (e.g., as wire basket tray) as far above the power cables as possible, preferably with the top of the cable tray 50 mm (2 in) below the bottom of the access floor tile.

14.4.3.3 Additional information

There are no requirements for separation of power and telecommunications cabling crossing at right angles, except the separation requirements mandated by applicable electrical codes.

Refer to applicable cabling standard (e.g., ISO/IEC 14763-2, CENELEC 50174-2, ANSI/TIA-942) regarding requirements for separation of power and telecommunications cabling.

The performance of a cabling pathway system is dependent on its proper installation, including supports and cabling. Neglecting installation and maintenance guidelines could lead to personal injury as well as damage to property.

14.4.4 Separation and installation of cabling**14.4.4.1 Requirements**

Cabling shall be installed and dressed neatly, taking care to adhere to minimum cable bend radii for cables. Take particular care not to leave excess optical fiber loops on the floor or in places where they can be damaged.

Structured cabling shall not share space within a dedicated optical fiber raceway with optical fiber equipment cords and patch cords.

14.4.4.2 Recommendations

There should be separate raceways or a divider in the raceway to separate balanced twisted-pair and optical fiber cabling.

Optical fiber equipment cords and patch cords should be installed in a dedicated optical fiber pathway that ensures proper bend radius control is maintained throughout the installation.

Where it is not practical to separate optical fiber and balanced twisted-pair cabling, optical fiber cabling should be on top of rather than underneath balanced twisted-pair cabling.

Optical fiber cabling should not touch the slab or lay on top of access floor when they exit the cable tray.

14.4.5 Distribution method**14.4.5.1 Recommendations**

Cabling and cabling pathways should be installed overhead if ceiling heights permit.

All telecommunications cabling under the access floor should be installed in a cabling pathway that is listed or classified by a nationally recognized testing laboratory (NRTL). In the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling. Telecommunications cabling should be in the hot aisles (the aisles at the rear of the cabinets) and the power cabling should be in the cold aisles (the aisles at the front of the cabinets). Placing the telecommunications cabling in the cold aisles is not recommended as the telecommunications raceways may block airflow to perforated tiles, which should be located in the cold aisles.

14.4.6 Redundant backbone cabling**14.4.6.1 Introduction**

Redundant backbone cabling protects against an outage caused by damage to the primary backbone cabling. Redundant backbone cabling may be provided in several ways depending on the degree of protection desired.

14.4.6.2 Recommendations

Backbone cabling between two spaces (e.g., a horizontal distribution area and a main distribution area) can be provided by running two cabling channels between these spaces, preferably along different routes. If the computer room has two main distribution areas, redundant backbone cabling to the horizontal distribution area may not be necessary, although the routing of cabling to the two main distribution areas should follow different routes.

Some degree of redundancy can also be provided by installing backbone cabling between horizontal distribution areas. If the backbone cabling from the main distribution area to the horizontal distribution area is damaged, connections can be patched through another horizontal distribution area.

14.4.7 Redundant horizontal cabling**14.4.7.1 Recommendations**

Horizontal cabling to critical systems should be diversely routed to improve resilience. Care should be taken not to exceed maximum horizontal cabling lengths when selecting cabling pathways. Critical systems can be supported by two different horizontal distribution areas, as long as maximum cabling length limitations are not exceeded. This degree of redundancy may not provide much more resilience than diversely routing the horizontal cabling if the two horizontal distribution areas are in the same fire protection zone.

14.4.8 Cable tray support system

14.4.8.1 General

14.4.8.1.1 Requirements

When routing telecommunications cabling from a cabling pathway to entry into cabinets or frames or when changing between levels of cabling pathways, the cabling shall be managed to maintain their minimum bend radius requirements and be protected from damage or compression when crossing any edge of the cabling pathway system.

Cable ladders and cable tray shall be installed per manufacturers' recommendations.

Supports for the cable ladders and cable tray shall be independent from non-telecommunications utilities (e.g., ducts, conduits, plumbing, luminaires).

WARNING: Do not use a cable tray as a walkway, ladder, or support for people; cable tray is a mechanical support system for cabling and raceways. Using cable trays as walkways can cause personal injury and damage cable tray and installed cabling.

14.4.8.2 Overhead cable trays

14.4.8.2.1 Requirements

In data centers that use overhead cable trays, 150 mm (6 in) access headroom between the top of a tray below to the bottom of the tray above is the minimum requirement.

Typical cable tray types for overhead cable installation include wire basket cable tray, ladder type, or center spine cable tray. Adjacent sections of metallic cable tray shall be bonded together and grounded per AHJ (e.g., NFPA 70) and shall be listed by a NRTL for this purpose. The metallic cable tray system shall be bonded to the data center common bonding network.

When they are supported from above, overhead cable ladders or trays (if used) shall be suspended from the structure above utilizing M12 (0.5 in) or greater threaded rods as required for structural support. Alternatively, the cable trays or ladders may be supported by an overhead support structure using support pillars or a suspended frame designed to support the load of the cable tray and cables.

If used for seismic bracing, ladder racks and cable tray shall be continuous wall to wall to form a brace for the equipment.

Cable tray shall not be routed directly below fire suppression or sprinkler systems.

14.4.8.2.2 Recommendations

In data centers that use overhead cable trays, 300 mm (12 in) access headroom between the top of a tray below to the bottom of the tray above should be provided.

Overhead cabling improves cooling efficiency and is a best practice where ceiling heights permit because it can substantially reduce losses due to supply airflow obstruction and turbulence caused by underfloor cabling and cabling pathways. Other potential advantages of overhead cable tray systems include elimination of access floor, separation of telecommunications cabling from power cabling and plumbing, flood survival, and improved access to cabling. Methods can include ladder racks or cable trays. Care must be taken in placement of overhead cabling to ensure that return air flow is not obstructed. (See also the mechanical section discussion of overhead and under-floor cabling in Section 10.5.7.2).

Overhead cable trays may be installed in several layers to provide additional capacity. An installation may include two or three layers of cable trays, one for power cabling and one or two for telecommunications cabling. These overhead cable trays may be supplemented by a duct or tray system for optical fiber equipment cords or patch cords, and if there is no access floor system, by brackets for the computer room bonding network.

In aisles and other common spaces in internet data centers, collocation facilities, and other shared tenant data centers, overhead cable trays should be protected by one of the following means:

- solid bottoms and covers;
- height at least 2.7 m (9 ft) above the finished floor to limit accessibility;
- protected through alternate means from accidental and/or intentional damage.

When choosing between supporting cable trays from overhead or from below, overhead suspension is preferred; suspended cable trays provide more flexibility for supporting cabinets and racks of various heights, and provide more flexibility for adding and removing cabinets and racks. However, they may require that a dedicated support infrastructure be suspended from the ceiling and require extra planning to preserve the structural integrity of the ceiling. Mechanically fastening of cable trays directly to racks or cabinets offers a more compact design that does not affect the structural integrity of the ceiling. However, this method is only suitable if cabinets and racks to which

these cable trays are attached will remain throughout the life of the computer room and it is certain that no equipment, cabinets, or racks taller than those to which the cable trays are attached will be needed.

14.4.8.3 Underfloor cable trays

14.4.8.3.1 Requirements

When telecommunications cabling is installed under the access floor, it shall be installed in cabling pathways that have no sharp edges that can potentially damage cables.

If the underfloor cable tray attaches to the access floor pedestals or stringers, the loading and attachment method shall comply with the floor manufacturers' specifications.

Clearance from the bottom of the access floor tile to the top of the cable tray or other raceway shall be at least 50 mm (2 in) to permit cable bundles and innerduct to exit out the top of the tray without incurring damage.

Metallic cable trays utilized in underfloor applications shall be listed or classified by an applicable nationally recognized testing laboratory (NRTL). Adjacent sections of metallic cable tray shall be mechanically bonded to one another. Subsequently the metallic cable tray shall be bonded to the data center common bonding network.

The maximum depth of telecommunications cabling in cable tray shall not exceed 150 mm (6 in) regardless of the depth of the cable tray.

14.4.8.3.2 Recommendations

The underfloor cable trays may be installed in multiple layers to provide additional capacity. Typical installations include two or three layers of cable trays, one for power cabling, and one or two for telecommunications cabling. These underfloor cable trays may be supplemented by a duct or tray system to manage optical fiber jumpers, patch cords, and equipment cords. There should be 300 mm (12 in) and no less than 150 mm (6 in) clearance between layers of underfloor cable trays run in parallel and stacked directly above each other.

When mixing balanced twisted-pair telecommunications cabling and power cabling in the same location, separation and segregation shall be maintained between power and balanced twisted-pair cabling respecting the minimum requirements of the pertinent cabling standards and the AHJ.

14.4.8.4 Coordination of cable tray routes

14.4.8.4.1 Recommendations

Planning of overhead cable trays for telecommunications cabling should be coordinated with architects, mechanical engineers, electrical engineers, and plumbing and structural engineers that are designing luminaries, plumbing, HVAC, power, and fire protection systems. Coordination should consider routing, clearances, and accessibility – consider use of three-dimensional drawings to simplify coordination. (Refer to Sections 14.4.8.1 and 14.4.8.2 for additional considerations of overhead and underfloor cable routing).

Lighting fixtures (luminaries) and sprinkler heads should be placed between cable trays, not directly above cable trays.

Underfloor cable tray routing should be coordinated with other underfloor systems during the planning stages of the building.

14.4.8.5 Underfloor foam mats

14.4.8.5.1 Requirements

Where foam matting is used as an underfloor pathway or containment then the foam matting shall be secured to prevent lifting where low or no cables are present and to prevent disturbance of the underfloor airflow.

Foam matting shall also comply with the fire performance requirements for the space it occupies.

14.4.8.5.2 Recommendations

Where foam matting is used as an underfloor pathway or containment then it should be a minimum of 13 mm (0.5 in) thick and fill the aisle between the floor pedestals.

14.5 Telecommunications cabling

14.5.1 Introduction

This section is intended to provide design standards for the telecommunications cabling requirements relating to:

- new data centers;
- additions to existing data centers;
- modifications and/or renovations to existing data centers.

See ANSI/TIA-942, CENELEC EN 50173-5, ISO/IEC 24764 or other applicable data center telecommunications cabling standards regarding data center telecommunications cabling topologies and distributors.

Telecommunications distribution consists of two basic elements – the distribution pathways and related spaces and the distribution cabling system.

Telecommunications cabling is therefore one subset of telecommunications distribution and may be described as a specific system of balanced twisted-pair, unbalanced cable types and optical fiber cables, equipment/patch cords, connecting hardware, and other components supplied as a single entity.

The data center support areas are spaces outside the computer room that are dedicated to supporting the data center facility. These may include the operation center, support personnel offices, security rooms, electrical rooms, mechanical rooms, storage rooms, equipment staging rooms, and loading docks.

14.5.2 Data center cabling system infrastructure

14.5.2.1 Introduction

Data center spaces dedicated to supporting the telecommunications cabling system are listed below. These telecommunications spaces are dedicated to support telecommunications cabling and related equipment. These spaces include:

- entrance room;
- main distribution area (MDA);
- intermediate distribution area (IDA);
- horizontal distribution area (HDA);
- zone distribution area (ZDA);
- equipment distribution area (EDA).

These spaces may or may not be walled off or otherwise physically separated from the other data center spaces. Following is a brief description of each of these spaces:

14.5.3 Main distribution area (MDA)

14.5.3.1 Introduction

The MDA includes the main cross-connect (MC), which is the central point of distribution for the data center structured cabling system. The main cross-connect is called the main distributor or MD in CENELEC EN 50173-5 and in ISO/IEC 24764.

Equipment typically located in the MDA includes:

- core routers;
- core LAN switches;
- core SAN switches;
- high-performance computing switches;
- PBX;
- T-3 (M13) multiplexers.

14.5.3.2 Requirements

Every data center shall have at least one MDA.

14.5.3.3 Additional information

The MDA may include the horizontal cross-connect (HC) when equipment areas are served directly from the MDA. This space is inside the computer room; it may be located in a dedicated room for improved security.

The MDA may serve one or more IDAs, HDAs and EDAs within the data center and one or more TRs located outside the computer room space to support office spaces, operations center, and other external support rooms.

Access provider provisioning equipment (e.g., M13 multiplexers) are often located in the MDA rather than in the entrance room to avoid the need for a second entrance room due to circuit distance restrictions.

14.5.4 Intermediate distribution area (IDA)

14.5.4.1 Introduction

The intermediate distribution area (IDA) is the space that supports the intermediate cross-connect. It may be used to provide a 2nd level cabling subsystem in data centers too large to be accommodated with only MDAs and HDAs. The IDA is optional and may include active equipment.

The IDA may include the horizontal cross-connect (HC) when equipment areas are served directly from the IDA.

14.5.4.2 Recommendations

The IDA is inside the computer room but may be located in a dedicated room within the computer room for additional security. Equipment typically located in an IDA includes LAN and SAN switches.

14.5.5 Horizontal distribution area (HDA)**14.5.5.1 Introduction**

The HDA is used to serve equipment not supported by a horizontal cross-connect (HC) in an IDA or MDA. The HDA is the distribution point for cabling to the EDAs.

The horizontal cross-connect is called the zone distributor or ZD in CENELEC EN 50173-5 and in ISO/IEC 24764.

14.5.5.2 Recommendations

The HDA is inside the computer room but may be located in a dedicated room within the computer room for additional security. Equipment typically located in the HDA includes:

- LAN switches;
- SAN switches;
- keyboard/video/mouse (KVM) switches

This equipment is used to provide network connectivity to the end equipment located in the EDAs. A small data center may not require any HDAs, as the entire data center may be able to be supported from the MDA. A typical data center will have several HDAs.

14.5.6 Zone distribution area (ZDA)**14.5.6.1 Introduction**

The ZDA is an optional interconnection point within the horizontal cabling, located between the HDA and the EDA to allow frequent reconfiguration and added flexibility.

The consolidation point in the ZDA is called the local distribution point or LDP in CENELEC EN 50173-5 and in ISO/IEC 24764.

14.5.6.2 Requirements

Horizontal cabling shall contain no more than one ZDA between the HC in the HDA and the mechanical termination in the EDA.

14.5.6.3 Recommendations

The zone distribution area may also serve as a zone outlet serving multiple nearby equipment in the computer room.

14.5.7 Equipment distribution area (EDA)**14.5.7.1 Introduction**

The EDA is the space allocated for end equipment, including all forms of telecommunications equipment (e.g., computer equipment, telephony equipment).

The telecommunications outlet in the EDA is called the equipment outlet (EO) and the consolidation point (CP) is called a local distribution point (LDP) in CENELEC EN 50173-5 and in ISO/IEC 24764.

14.5.7.2 Requirements

EDA areas shall not serve the purposes of an entrance room, MDA, IDA, or HDA.

14.5.8 Cabling topology**14.5.8.1 Introduction**

The basic cabling elements of the data center star topology include:

- horizontal cabling.
- backbone cabling.
- equipment cabling.
- main cross-connect (MC) in the main distribution area (MDA).
- intermediate cross-connect (IC) intermediate distribution area (IDA),
- horizontal cross-connect (HC) in the TR, horizontal distribution area (HDA), intermediate distribution area (IDA), or main distribution area (MDA).
- zone outlet or consolidation point (CP) in the zone distribution area.
- outlets in the equipment distribution area (EDA).

14.5.9 Horizontal cabling topology

14.5.9.1 Requirements

The horizontal cabling shall be installed in a star topology. Each EDA shall be connected to a HC in either a HDA, IDA, or MDA via horizontal cabling.

14.5.10 Backbone cabling topology

14.5.10.1 Requirements

The backbone cabling shall use the hierarchical star topology as illustrated by Figure 69 wherein each HC in the HDA is cabled directly to an MC in the MDA or an IC in an IDA. There shall be no more than two hierarchical levels of cross-connects in the backbone cabling.

Direct backbone cabling to the HC shall be allowed when distance limitations are encountered.

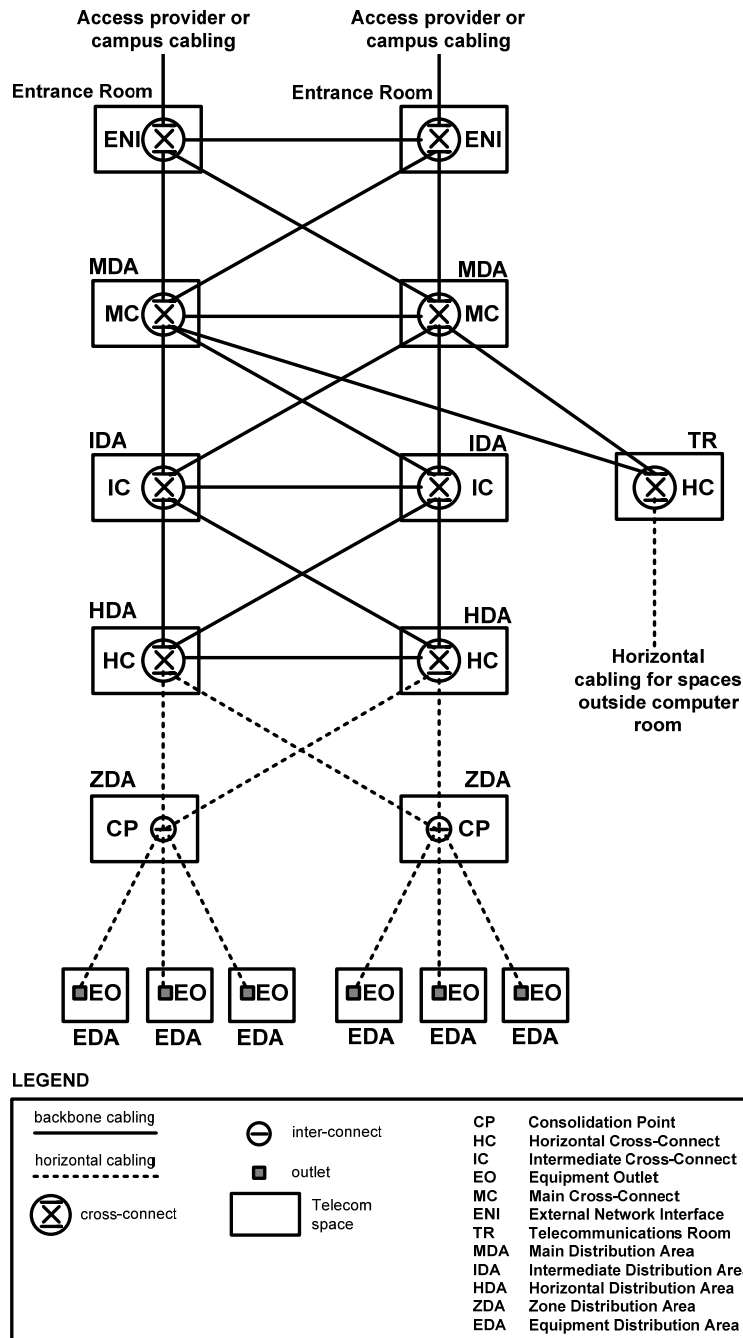


Figure 69: Data Center Cabling Topology Example

14.5.10.2 Recommendations

The presence of an HDA or IDA is not mandatory. Cabling extending from the HC in the HDA, IDA, or MDA to the mechanical termination in the EDA is considered horizontal cabling. Sufficient horizontal cable slack should be considered to allow migration to a cross-connect in the HDA, IDA, or MDA.

Backbone cabling cross-connects may be located in TRs, computer rooms, MDAs, IDAs, HDAs or at entrance rooms.

14.5.11 Accommodation of nonstar configurations**14.5.11.1 Introduction**

The topology in Figure 69, with appropriate interconnections, electronics, or adapters in data center distribution areas, accommodate systems that are designed for nonstar configurations such as ring, bus, or tree.

14.5.11.2 Recommendations

Cabling between entrance rooms, MDAs, IDAs, and HDAs is permitted to provide redundancy and to avoid exceeding application cabling distance restrictions for connections that route through two HDAs.

14.5.12 Redundant cabling topologies**14.5.12.1 Introduction**

Redundant topologies can include a parallel hierarchy with redundant distribution areas. These topologies are in addition to the star topology specified in this standard.

See Figure 69 for each of these elements and their relationships in the data center cabling star topology.

14.5.13 Horizontal cabling**14.5.13.1 Introduction**

The horizontal cabling is the portion of the telecommunications cabling system that extends from the mechanical termination in the EDA to the HC in an HDA, IDA, or MDA.

The horizontal cabling includes:

- horizontal cables;
- mechanical terminations;
- equipment cords, patch cords, or jumpers;
- zone outlet or a consolidation point in the zone distribution area.

14.5.13.2 Recommendations

The following partial listing of common services and systems should be considered when the horizontal cabling is designed:

- voice, modem, and facsimile telecommunications service;
- switching and server equipment;
- computer and telecommunications management connections;
- keyboard/video/mouse (KVM) connections;
- intelligent infrastructure management (IIM);
- wide area networks (WAN);
- local area networks (LAN);
- storage area networks (SAN);
- other building signaling systems (building automation systems such as fire, security, power, HVAC, and EMS).

In addition to satisfying today's telecommunications requirements, the horizontal cabling should be planned to reduce ongoing maintenance and relocation. It should also accommodate future equipment and service changes. Consideration should be given to accommodating a diversity of user applications in order to reduce or eliminate the probability of requiring changes to the horizontal cabling as equipment needs evolve. The horizontal cabling can be accessed for reconfiguration under the access floor or overhead on cable raceway systems. However, in a properly planned facility, disturbance of the horizontal cabling should only occur during the addition of new cabling.

14.5.14 Horizontal cabling types

14.5.14.1 Requirements

Due to the wide range of services and site sizes where horizontal cabling will be used, more than one transmission medium is recognized. This standard specifies transmission media, which shall be used individually or in combination in the horizontal cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, and equipment cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801, ANSI/TIA-568-series).

Horizontal cabling shall consist of one or more of the following media types:

- 4-pair 100-ohm balanced twisted-pair Category 6/Class E minimum, (Category 6_A/Class E_A or higher recommended);
- OM3, 50/125 μm laser-optimized multimode optical fiber cable minimum, (OM4, 50/125 μm laser-optimized multimode optical fiber cable recommended where fiber cabling lengths exceed 100m [328 ft]);
- OS1 or OS2, single-mode optical fiber cable.

Notes:

- 1) Category 5e/Class D cabling may be used in an existing data center that already utilizes Category 5e/Class D cabling.
- 2) 734-type and 735-type 75-ohm coaxial cable as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
- 3) If specific applications require other types of cabling (e.g., Infiniband cabling, EIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards should apply to local requirements.
- 4) To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.

14.5.15 Balanced twisted-pair cabling

14.5.15.1 Introduction

Balanced twisted-pair cabling performance is described using a scale based on classes or categories, as defined by ISO/IEC and TIA, respectively. While Category 3/ Class C is the minimum acceptable performance for backbone network cabling, Category 5e/ Class D is the minimum recommended by most standards, and Category 6_A/Class E_A is the recommendation of this Standard.

Table 25: Balanced Twisted-Pair Cabling Channel Performance

<i>ISO classes/categories</i>	<i>TIA categories</i>	<i>Frequency characterization</i>
Class D/Category 5	Category 5e	100 MHz
Class E/Category 6	Category 6	250 MHz
Class EA/Category 6 _A	Augmented Category 6	500 MHz
Class F/Category 7	N/A	600 MHz
Class FA/Category 7 _A	N/A	1000 MHz

NOTE: TIA does not define cabling above Category 6_A. Category 7/Class F and higher cabling are defined by CENELEC and ISO/IEC. Each of these standards writing organizations defines component performance by the term “Category” while ISO/IEC and CENELEC define system performance by the term “Class”.

14.5.15.2 Additional information

14.5.15.2.1 Balanced twisted-pair cabling supportable distances

Maximum supportable distances for applications using balanced twisted-pair cabling can be found in the cabling standard being followed (e.g. ISO/IEC 11801, CENELEC EN 50173-5, or ANSI/TIA-568-C.0). The table is based on the minimum performance requirements of specific balanced twisted-pair cabling.

14.5.16 Optical fiber cabling

14.5.16.1 Introduction

There are four classes of multimode optical fiber cabling (OM1, OM2, OM3, and OM4) and two classes of single-mode optical fiber cabling (OS1 and OS2). Table 26 shows the minimum bandwidth or optical performance for each cabled optical fiber cable by type.

14.5.16.2 Requirements

OS1 single-mode and OM3 multimode are the minimum performance optical fiber types specified in this standard.

Table 26: Optical Fiber Cable Performance By Type

<i>Classification</i>	<i>Optical fiber type</i>	<i>Performance</i>
OM1	62.5/125 μm multimode	Minimum overfilled launch bandwidth of 200 and 500 MHz•km at 850 and 1300 nm, respectively
OM2	50/125 μm multimode 62.5/125 μm multimode	Minimum overfilled launch bandwidth of 500 and 500 MHz•km at 850 and 1300 nm, respectively
OM3	50/125 μm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 1500 and 500 MHz•km at 850 and 1300 nm respectively, and an effective modal bandwidth of 2000 MHz•km at 850 nm using a restricted mode launch (e.g., vertical cavity surface emitting laser [VCSEL]).
OM4	50/125 μm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 3500 and 500 MHz•km at 850 and 1300 nm respectively, and an effective modal bandwidth of 4700 MHz•km at 850 nm using a restricted mode launch (e.g., VCSEL)
OS1	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 1.0 dB per km at 1310 nm and 1550 nm for indoor and 0.5 dB per km at 1310 nm and 1550 nm for outdoor.
OS2	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 0.4 dB per km at 1310 nm, 1383 nm, and 1550 nm for both indoor and outdoor. OS2 fiber is optimized for performance at the 1383 nm window (and is defined in ITU-G652.D)

14.5.16.3 Component channel method versus application based method

There are two methods used for the design and implementation of optical fiber cabling solutions; component channel method and application based method.

14.5.16.3.1 Component channel method

14.5.16.3.1.1 Introduction

Traditionally the component method has been used to design and assemble optical fiber cabling solutions without detailed consideration for the applications that eventually will run over the optical fiber cabling channel. This lack of coordination can result in many discussions and disagreements between designers, installers and operations staff over who is responsible for what when the equipment is found to be not working.

Knowledge of the applications to be supported is critical to the effective delivery and future proofing of the optical fiber cabling infrastructure. The designer should first determine what applications are required, the type of connectors, the bandwidth performance and optical fiber type. The designer should then relate this to the optical performance charts and tables in the cabling standards being followed. The designer can then obtain the maximum permitted loss per optical fiber type and maximum distance over which the application can be supported. Selection and assembly of components is concluded on an accumulated loss basis; the resulting performance is measured against the whole channel and does not identify or acknowledge a worst individual event or component loss figure.

This approach can be used to the designer's and operator's advantage when considering the use of more than two connectors or lossier connectors over a shorter channel distance. It effectively converts bandwidth gains into

connector loss. Most manufacturers will not recommend or support more than six connectors in an optical fiber channel.

The demands from the latest and next generation high-speed applications have considerable distance limiting aspects. The applications can only be expected to operate effectively when the balance of media choice, distance, bandwidth and component loss are all within the prescribed parameters for each application to be supported.

14.5.16.3.2 Application based method

14.5.16.3.2.1 Introduction

If the applications to be deployed are known, the data center cabling designer can get detailed information about channel losses and maximum channel distance supported for each optical fiber media type from the cabling standards being followed. Dedicated home run optical fiber cabling solutions can be configured from approved component sets.

14.5.16.3.3 Optical fiber cabling supportable distances

14.5.16.3.3.1 Introduction

Maximum supportable distances and maximum channel attenuation for applications using optical fiber cabling can be found in applicable standards (e.g., ANSI/TIA-568-C.0, ISO 11801 Ed.2). Tables in these standards are based on the minimum performance requirements of 62.5/125 μm , 50/125 μm , 850 nm laser-optimized OM3 50/125 μm , 850 nm laser-optimized OM4 50/125 μm , and single-mode fiber.

14.5.17 Single-mode and multimode connector color

14.5.17.1 Recommendations

The single-mode connector or a visible portion of it should be blue in color, referring to a flat-polished optical fiber endface; the color green should signify a connector featuring an angle polished optical fiber endface. Where a mixture of OS1 and OS2 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

The multimode connector or a visible portion of it should be:

- beige for a 62.5 μm connector;
- black for a 50 μm connector;
- aqua for a 50 μm laser-optimized connector (where a mixture of OM3 and OM4 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used).

Adapter housing color should represent the cabling performance of the installed permanent fiber using the connector color scheme above.

14.5.18 Shared sheath guidelines

14.5.18.1 Introduction

Shared sheath guidelines described in this section are not intended to cover all system designs and installations. It is recommended that the user consult with equipment manufacturers, applications standards and system providers for additional information.

In general, applications using no common frequencies tend not to interfere with each another. A good example of this is mixing analog voice and digital data signals within the same cable sheath. In a single balanced twisted-pair cable, multiple applications of the same type may operate on different twisted pairs simultaneously without any problems.

14.5.18.2 Recommendations

The designer and installer should follow the recommendations for shared sheath implementation described in the cabling standards being followed.

14.5.19 Hybrid and bundled cable assembly applications

14.5.19.1 Introduction

Hybrid and bundled cable assemblies are used to group multiple individual cables together to form a single cable unit routed along a common path. These individual cables may be of the same or different types (e.g., optical fiber cabling and balanced twisted-pair cabling) or of the same or different categories (e.g., Category 6_A/Class E_A cabling with Category 6/Class E cabling).

Hybrid cable assemblies are manufactured in a factory whereas bundled cable assemblies may be assembled either in a factory, at a third-party facility or on site by the installer.

NOTE: Bundled cables are sometimes referred to as loomed, speed-wrap, or whip cable assemblies.

14.5.19.2 Requirements

When bundled and hybrid cables are used for horizontal cabling, each cable type shall be recognized and meet the transmission (e.g., recognized categories/classes) and color-code specifications (e.g., 4-pair color-code groupings) for that cable type. Additionally, hybrid or bundled cable assemblies shall meet the hybrid or bundled cable assembly requirements of applicable standards (e.g., ISO/IEC 11801, ANSI/TIA-568-series). These requirements apply to hybrid cables and bundled cables assembled prior to installation.

Hybrid and bundled cable assemblies may be installed either as cable or as pre-connectorized assemblies. These assemblies, known as trunk cable assemblies, may be pre-connectorized on one or both ends. When used, these hybrid and bundled trunk assemblies are required to meet the hybrid and bundled transmission performance requirements of applicable standards (e.g., ISO/IEC 11801, ANSI/TIA-568-series).

14.5.19.3 Recommendations

There are a number of other types horizontal cabling that have not been defined in this standard yet may be effective for specific applications. Although these other types of horizontal cabling are not part of the requirements of this standard, they may be used in addition to the best practices offered by this standard.

14.5.20 Trunk cabling assemblies**14.5.20.1 Introduction**

Trunk cabling assemblies consist of two or more preconnectorized, cabling links of the same or different types or categories that may either be covered by one overall sheath or a collection of individual cable units, which are bound together to form a single trunk unit. Trunk cabling assemblies are capable of supporting multiple devices. A trunk cabling assembly may be terminated at one end or both ends with connectors. Trunk cabling assemblies may be a convenient and economical alternative to installing a number of individual cables and then applying field termination techniques to connectorize the cables.

Balanced twisted-pair and optical fiber trunk cabling assemblies offer the following features, benefits, and disadvantages as shown in Table 27.

Table 27: Advantages And Disadvantages Of Trunk Cabling Assemblies

<i>Feature/Benefit</i>	<i>Advantages</i>	<i>Disadvantages</i>
Quality controlled factory terminations	Yes	
Potentially reduced installation labor time	Yes	
Fewer cables improves cable management	Yes	
Less dependence on installer/technician skills and experience	Yes	
Requires a high degree of accuracy when ordering lengths to avoid mistakes		Yes
If a trunk cabling assembly is damaged, multiple cable units within the trunk cabling assembly may be adversely affected		Yes
Factory terminated optical fiber trunk cabling assemblies may yield better permanent link optical mated pair loss vs. field terminated connectors	Yes	

14.5.21 Horizontal cabling length limitations**14.5.21.1 Introduction**

The horizontal cabling length limitations are the cable lengths from the mechanical termination of the cabling at the horizontal cross-connect in the HDA, IDA, or the MDA to the mechanical termination of the cabling in the EDA.

14.5.21.2 Requirements

For maximum and minimum cabling lengths, refer to the applicable cabling standards.

14.5.21.3 Recommendations

Horizontal cabling distances in a computer room may need to be reduced to compensate for longer equipment cords in the data center distribution areas. Therefore, careful considerations to the horizontal cabling distance should be made to ensure cabling distances and transmission requirements are not exceeded when the equipment cords are attached.

NOTE: For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, without further guidance from manufacturers the zone distribution area termination should be located at least 15 m (50 ft) from the horizontal distribution area termination. Consult with the cabling system manufacturer about the minimum distances supported by the chosen product set. Their recommendations may reduce space needed to collect excess cable.

14.5.22 Balanced twisted-pair cord length limitations

14.5.22.1 Introduction

Balanced twisted-pair equipment cords and patch cord assemblies may be constructed with either solid or stranded conductors. The insertion loss (attenuation) performance of stranded cables used in the assembly of these cords is greater than the attenuation of solid conductor cables. While a generic cabling system has a physical channel distance limitation of 100 m (328 ft), there is an assumption made that the combined length of equipment cords and patch cords at both ends of the cabling channel will not exceed 10 m (33 ft). If stranded conductor equipment cords and stranded conductor patch cords with a combined length of more than 10 m (33 ft) are used, refer to the applicable cabling standards for maximum cord lengths.

14.5.22.2 Requirements

Manufacturers shall be consulted to confirm the attenuation characteristics of their stranded cables, equipment cords, and patch cords to help assure that the installed cabling channels will perform to the applicable cabling standards.

Balanced twisted-pair equipment cables used in the context of zone outlets in the ZDA shall meet the minimum performance requirements provided in the cabling standard being followed.

The zone outlet shall be marked with the maximum allowable zone area cable length. One method to accomplish this is to evaluate cable length markings.

If patch cords totaling more than 10 m (33 ft) are used, maximum cabling distance shall be reduced in accordance with the preceding ZDA distance limitations.

14.5.22.3 Recommendations

Where there are anticipated issues with future channel configurations the zone outlet should be marked with the maximum allowable zone area cable length.

14.5.23 Horizontal cabling applications

14.5.23.1 Requirements

For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application shall be considered.

14.5.23.2 Recommendations

For optical fiber and balanced twisted-pair cabling, application distances can be constrained by the cabling category or type. The compilation of application information detailed in applicable standards (e.g., ANSI/TIA-568-C.0 Annex D, EN 50173-5 Annex B, ISO/IEC 11801 Annex F) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

14.5.24 Backbone cabling

14.5.24.1 Introduction

The function of the backbone cabling is to provide connections between the MDA, IDA, HDA, and entrance rooms in the data center cabling system.

Backbone cabling consists of the backbone cables, MC, mechanical terminations, equipment cords, and patch cords or jumpers used for backbone-to-backbone cross-connection.

The backbone cabling is expected to serve the needs of the data center occupants for one or several planning phases, each phase spanning a time scale that may span days, months, or years. During each planning period, the backbone cabling design should accommodate growth and changes in service requirements without the installation of additional cabling. The length of the planning period is ultimately dependent on the design logistics, including material procurement, transportation, and installation and specification control.

14.5.24.2 Requirements

The backbone cabling shall allow network reconfiguration and future growth without disturbance of the backbone cabling.

14.5.24.3 Recommendations

The backbone cabling should support different connectivity requirements, including both the network and physical console connectivity such as local area networks, wide area networks, storage area networks, computer channels, and equipment console connections.

14.5.25 Backbone cabling types

14.5.25.1 Introduction

Cabling specified by this standard is applicable to different application requirements within the data center environment. Depending upon the characteristics of the individual application, choices with respect to transmission media should be made. In making this choice, factors to be considered include:

- flexibility with respect to supported services,
- required useful life of cabling,
- computer room size,
- type and quantity of systems supported,
- channel capacity (transmission performance characteristics) within the cabling system,
- equipment vendor recommendations or specifications.

14.5.25.2 Requirements

Each recognized cable has individual characteristics that make it suitable for a range of applications defined against each category or cabling type in the applicable cabling standards. A single cable may not satisfy all end user requirements. It may be necessary to use more than one medium in the backbone cabling. In those instances, the different media shall use the same facility architecture with the same location for cross-connects, mechanical terminations, and interbuilding entrance facilities.

Due to the wide range of services and site sizes where backbone cabling will be used, more than one transmission medium is recognized. This standard specifies the transmission media which shall be used individually or in combination in the backbone cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801, ANSI/TIA/EIA-568-series).

Backbone cabling shall consist of one or more of the following media types:

- 100-ohm balanced twisted-pair Category 3/Class C minimum, (Category 6/Class E or higher recommended);
- OM3, 50/125 μm laser-optimized multimode optical fiber cable minimum, (OM4, 50/125 μm laser-optimized multimode optical fiber cable recommended where fiber cabling lengths exceed 100 m [328 ft]);
- OS1 or OS2, single-mode optical fiber cable;
- 75-ohm coaxial cabling (Telcordia GR-139-CORE 734-type and 735-type).

Notes:

- 1) Category 5e/Class D cabling may be used in an existing data center that already utilizes this Category/Class of cabling.
- 2) 734-type and 735-type 75-ohm coaxial cable as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
- 3) If specific applications require other types of cabling (e.g., Infiniband cabling, EIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards shall apply to local requirements.
- 4) To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.
- 5) The guidelines, requirements and recommendations described in Section 14.5.15 through Section 14.5.20 shall also apply to the backbone cabling subsystem.
- 6) The guidelines, requirements and recommendations described in Section 14.5.22 shall also apply to the backbone cabling subsystem.

14.5.26 Backbone cabling length limitations

14.5.26.1 Introduction

The supportable backbone cabling topologies for the media types recognized in this standard are application and media dependent. Refer to applicable standards for additional information regarding optical fiber and balanced twisted-pair cabling design considerations, including recommended distances and allowable maximum channel insertion loss based on the application's requirements.

Applications with data rates equal to or greater than 1 Gb/s should be reviewed in detail to assess support over existing cabling as well as the design for new cabling. For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application must be considered. For balanced twisted-pair cabling, application distances can be constrained by the cabling category. The compilation of application information detailed in applicable standards (e.g., ANSI/TIA-568-C.0, EN 50173-5, ISO/IEC 11801) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

Interconnections between the individual areas, which are outside the scope of this standard, may be accomplished by employing equipment and technologies normally used for wide area applications.

14.5.26.2 Requirements

In data centers that use longer balanced twisted-pair equipment cords and patch cords, the backbone cabling distances shall be designed to accommodate the maximum cordage length so that when configuring channels for use with applications the combination of equipment cord, permanent link and patch cords never exceeds the channel loss limits. (See Section 14.5.22).

14.5.26.3 Recommendations

The 90 m (295 ft) distance limitation assumes uninterrupted cabling runs between cross-connects that serve equipment (e.g., no intermediate cross-connect).

Users of this standard are advised to consult the specific standards associated with the planned service, or equipment manufacturers and systems integrators to determine the suitability of the cabling described herein for specific applications.

For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, cabling system manufacturers' guidance should be sought on their recommendations for the minimum distance between connection points in a channel. Without that guidance the backbone cabling lengths shall be at least 15 m (50 ft).

14.5.27 Centralized optical fiber cabling

14.5.27.1 Introduction

Many users of data networks implement their network architecture with centralized electronics versus distributed electronics in the computer room.

Centralized cabling provides connections from EDAs to centralized cross-connects by allowing the use of pull-through cables, interconnection, cross-connections or splices in the HDA and IDA.

14.5.27.2 Requirements

The administration of moves, adds and changes shall be performed at the centralized cross-connect. Centralized cabling design shall allow for migration (in part or in total) of the pull-through, interconnect, or splice implementation to a cross-connection implementation. Sufficient space shall be left in the HDA and IDA to allow for the addition of patch panels needed for the migration of the pull-through, interconnect, or splice to a cross-connection. Sufficient cable slack shall exist in the HDA and IDA to allow movement of the cables when migrating to a cross-connection. Cable slack storage shall provide cable bend radius control so that optical fiber cable bend radius limitations are not violated. Optical fiber cable slack shall be stored in protective enclosures. Centralized cabling design shall allow for the addition and removal of horizontal and backbone optical fiber cabling.

14.5.27.3 Recommendations

Cable slack may be stored as jacketed cable or unjacketed optical fiber (buffered or coated). The layout of the termination hardware should accommodate modular growth in an orderly manner.

14.5.28 Centralized optical fiber length limitations

14.5.28.1 Requirements

Centralized cabling implementations using multimode optical fiber shall be located within the same building as the areas served.

NOTE: Future applications may increase demands on the bandwidth performance from the optical fiber and reduce the operational channel distance. An example of centralized optical fiber cabling is shown in Figure 70.

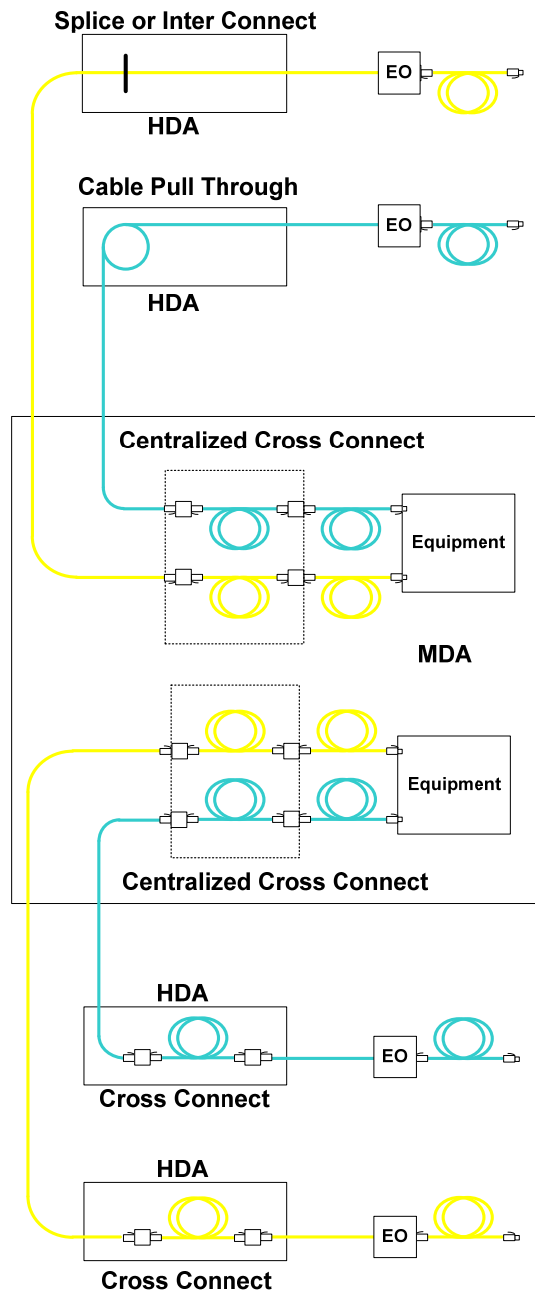


Figure 70: Centralized Optical Fiber Cabling Example

14.5.29 Implementation

14.5.29.1 Requirements

Centralized cabling design shall allow for migration (in part or in total) of the pull-through (continuous sheath cables), interconnect, or splice implementation to a cross-connection implementation. Centralized cabling shall support the administration and labeling requirements of the cabling standards being followed. Administration of moves and changes shall be performed at the centralized cross-connect. In addition, computer room splice and interconnect hardware shall be labeled with unique identifiers on each termination position. Polarity shall adhere to the requirements of the cabling standards being followed. Service loop storage shall provide bend radius control so that optical fiber bend radius limitations are not violated.

14.5.29.2 Recommendations

The computer room backbone subsystem should be designed with sufficient spare circuit capacity to service network equipment needs from the centralized cross-connect without the need to pull additional computer room backbone cables. The computer room backbone optical fiber strand count should be sized to deliver present and future loading to the maximum expected equipment density within the area served by the computer room. Generally, a minimum of two optical fiber strands are required for each network connection device served by the optical fiber cabling system. The design should allow sufficient cable length (service loop) to facilitate the migration of the pull-through (continuous sheath cables), interconnect, or splice implementation to a cross-connection implementation. Service loops may be stored as jacketed cable or unjacketed fiber (buffered or coated).

14.5.30 Cable management

14.5.30.1 Introduction

Performance of cable and connecting hardware may become degraded if initial installation and ongoing cable management recommendations are not followed. Installation and maintenance practices for the pulling and placing of horizontal and backbone cabling differs greatly from that of the associated interconnections and cross-connections.

14.5.30.2 Requirements

While all transmission parameters are sensitive to transmission discontinuities caused by connector terminations, return loss, and all forms of crosstalk (e.g., near-end crosstalk [NEXT], attenuation-to-crosstalk ratio–far end [ACR–F], previously known as ELFEXT), performance of balanced twisted-pair systems are particularly sensitive to conductor untwisting and other installation practices that disturb pair balance and cause impedance variations. To prevent these problems, the installer shall adhere to the following practices:

- remove only as much cable jacket as is required for termination and trimming.
- follow the manufacturer's instructions for mounting, termination, and cable management.
- minimize the amount of untwisting in a pair as a result of termination to connecting hardware; for untwisting cabling, maintain pair twists as close as possible to the termination point; the amount of untwisting must not exceed 13 mm (0.5 in) for Category 5e and higher cables.

NOTE: This requirement is intended to minimize untwisting of cable pairs and the separation of conductors within a pair. It is not intended as a twist specification for cable or jumper construction.

For termination fields that require frequent access (e.g., cross-connects used for configuring a network), one way to control termination consistency is by using factory-assembled equipment cords, patch cords, and patch panels that meet the appropriate performance requirements. Jumpers can provide comparable performance, but typically require a higher skill level to implement changes.

14.5.30.3 Recommendations

Telecommunications cabling should be placed in cabling pathways (containment) that provide sufficient space for placement of the media. Consider the following methods of containment for telecommunications cabling installed in dedicated routes:

- enclosed raceway distribution (e.g., conduit systems);
- zone distribution (e.g., enclosures);
- cable trays (e.g., open top systems);

NOTE: Alien crosstalk is associated with balanced twisted-pair cabling and an issue of which the installer must be aware. This issue can be mitigated by using alien crosstalk compliant products.

CAUTION: Refer to appropriate codes, standards and regulations for compliance with flame spread and smoke index properties of cabling used in cabling pathway systems.

Connecting hardware should only be installed in the access floor space when the connecting hardware is one of the following:

- a consolidation point (CP) or zone outlet in a zone distribution area (ZDA);
- telecommunications outlet for an equipment distribution area (EDA) or workstation;
- building automation systems (BAS) horizontal connection point (HCP).

Cross-connections are designed for flexibility to allow for moves, adds, and changes. The structured cabling system user is typically responsible for altering cross-connections to implement network changes. Skill levels among users vary and should be taken into consideration when designing, providing training on, and performing ongoing management of the cross-connection facility. The following guidelines should be followed for appropriate management practices.

In cabling pathways and telecommunications spaces, use appropriate cable routing and dressing fixtures to organize and effectively manage the different cable types. The cable management precautions that should be followed include eliminating cable stress caused by:

- tension in suspended cable runs.
 - Limit supported spans to 1.5 m (5 ft) or less.
- tightly bound cable bundles.
 - Keep jacket deformation to a minimum.
- twisting the cable jacket during installation.
 - Twisting of cable may affect transmission performance.

NOTE: Never use staples or staple fastening tools to fasten telecommunications cabling in a data center.

The following are cross-connect facility management precautions that should be observed:

- Eliminate or minimize equipment cord, patch cord, and jumper slack in the management field after each cross-connection is completed.
- In cross-connections utilizing balanced twisted-pair or optical fiber equipment cords or patch cords, bend radius can become difficult to control; it is important to achieve desired manageability without loss of performance in a cabling channel by controlling the equipment cord and patch cord bend radii.
- Horizontal cables should be terminated on connecting hardware that is the same performance (Category) or higher. The installed transmission performance of cabling where components of different performance category requirements are used shall be classified by the least-performing component.
- Because horizontal and backbone cables are always terminated on separate connectors, use patch cords or jumpers to make connections between horizontal cables and backbone cables.

14.5.31 Bend radius and pulling tension guidelines

14.5.31.1 Introduction

Pay strict attention to the manufacturer's guidelines on bend radii and maximum pulling tension during installation. Notice that the recommended minimum bend radius for a cable during installation may be greater than the recommended bend radius after the cable is installed. This is to minimize tension and deformation as the cables pass around corners during installation.

Cable bend radius requirements minimize the effects of bends on the transmission performance of installed cabling links. These requirements are distinct from the bend radius specifications for conduits. Consult the manufacturer's specifications for the minimum bend radius during installation. Minimum bend radius utilized should be the greater of the manufacturers' specifications and the specifications provided in this standard.

14.5.32 Balanced twisted-pair cabling bend radius and pulling tension best practices

14.5.32.1 Requirements

The maximum pull force best practices for balanced twisted-pair cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 28.

Table 28: Balanced Twisted-Pair Cable Bend Radius And Pulling Tension

<i>Cabling/Cord Types</i>	<i>Required minimum inside bend radius under no load (No Stress)</i>	<i>Required minimum bend radius under load (Stress)</i>	<i>Recommended maximum tensile load under load (Stress)</i>
4-pair, balanced twisted-pair patch/equip cord	One-times the cord cable outside diameter	One-times the cord cable outside diameter	Follow manufacturer specifications
4-pair, balanced twisted-pair cables	Four times the cable's outside diameter	Four times the cable's outside diameter	110 N (25 lbf)
Multipair balanced twisted-pair cables	Follow manufacturer specifications	Follow manufacturer specifications	Follow manufacturer specifications

14.5.33 Optical fiber cable bend radius and pulling tension best practice

14.5.33.1 Requirements

The maximum pull force best practices for optical fiber cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 29.

Table 29: Optical Fiber Cable Bend Radius And Pulling Tension Best Practices

Cable type and installation details	Maximum tensile load during installation	Minimum bend radii while subjected to:	
		maximum tensile load (during installation)	no tensile load (after installation)
Inside plant horizontal cable with 2 or 4 fibers	220 N (50 lbf)	50 mm (2 in)	25 mm (1 in)
Inside plant cable with more than 4 fibers	Per manufacturer	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with up to 12 fibers	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with more than 12 fibers	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Outside plant cable	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by pulling	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by directly buried, trenched, or blown into ducts	440 N (100 lbf)	20-times the cable outside diameter	10-times the cable outside diameter

NOTE: Non-circular cable bend diameter requirements are to be determined using the minor axis as the cable diameter and bending in the direction of the preferential bend.

14.5.34 Abandoned cable

14.5.34.1 Requirements

Remove abandoned cable as required by the AHJ.

14.5.34.2 Recommendations

It is considered a best practice to remove abandoned cable in the data center.

14.6 Field testing data center telecommunications cabling

14.6.1 Introduction

Field testing is an effective method of evaluating the transmission performance of installed telecommunications cabling. The field test measurement results of installed balanced twisted-pair or optical fiber telecommunications cabling depend on several factors, including the:

- Transmission performance of cable.
- Transmission performance of connecting hardware.
- Transmission performance of equipment cords, patch cords, and cross-connect cabling.
- Total number of connections.
- Installation practices and expertise of the installers.
- Maintenance techniques that are used.

Field testing conducted on balanced twisted-pair and optical fiber cabling shall be conducted in accordance with specified standards.

NOTE: Refer to the list of standards provided in the references section of this standard.

This section provides requirements and recommendations regarding channel and permanent link field-testing, including:

- Installation conformance.
- Specifications for field test instruments.
- Field test measurement methods.
- Interpretation of test results.

14.6.2 Conformance

14.6.2.1 Introduction

Conformance ensures that field test measurements have been completed in accordance with the terms and conditions of a contract.

14.6.2.2 Requirements

The installation contract shall include field test measurement requirements of the installed cabling to specific industry standards as well as to visually inspect the cabling. Performance field test measurement documentation of the installed cabling shall be provided to the building tenant, building owner or agent per contract requirements, or, in lieu of contract requirements, in the format delivered by the certification test instrument. Visual inspection of installed cabling is performed by observing the following:

- The condition, workmanship, and finish are satisfactory, including no obvious damage to the cable (e.g., bend radius, tearing, and separation from sources of EMI).
- The marking (labeling) is legible and placed according to specification.
- Mechanical damage is absent, and there is no undesired movement or displacement of parts.
- Flaking of materials or finishes is absent.

Conformance to visual inspection requires that a form be submitted indicating that a visual inspection has been conducted and the form shall document the results of the visual inspection.

14.6.3 100-ohm balanced twisted-pair cabling field testing

14.6.3.1 Introduction

Certification of the balanced twisted-pair cabling determines whether the cabling meets expected performance requirements such as those specified in one or more of the following Categories/Classes of cabling:

- TIA Category 3 cabling;
- ISO Class C cabling;
- TIA Category 5e cabling;
- ISO Class D cabling using ISO Category 5 components;
- TIA Category 6 cabling;
- ISO Class E cabling using ISO Category 6 components;
- TIA Category 6_A cabling;
- ISO Class E_A cabling using ISO Category 6_A components;
- ISO Class F cabling using ISO Category 7 components;
- ISO Class F_A cabling using ISO Category 7_A components.

NOTE: ISO Class E and TIA Category 6 cabling support IEEE 10GBASE-T at limited distances and may require mitigation techniques. For additional details, see TIA TSB-155-A and ISO/IEC TR 24750.

14.6.3.2 Balanced twisted-pair cabling field test configuration

14.6.3.2.1 Channel

14.6.3.2.1.1 Requirements

The channel test configuration shall be used to certify the channel performance of installed balanced twisted-pair cabling. The channel may include:

- Horizontal cable.
- Patch cords and equipment cords.
- A telecommunications outlet/connector.
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA).
- Up to two connections at the horizontal cross-connect.

The channel configuration description does not apply to those cases where horizontal cabling is cross-connected to backbone cabling. See Figure 71 for an example of a channel.

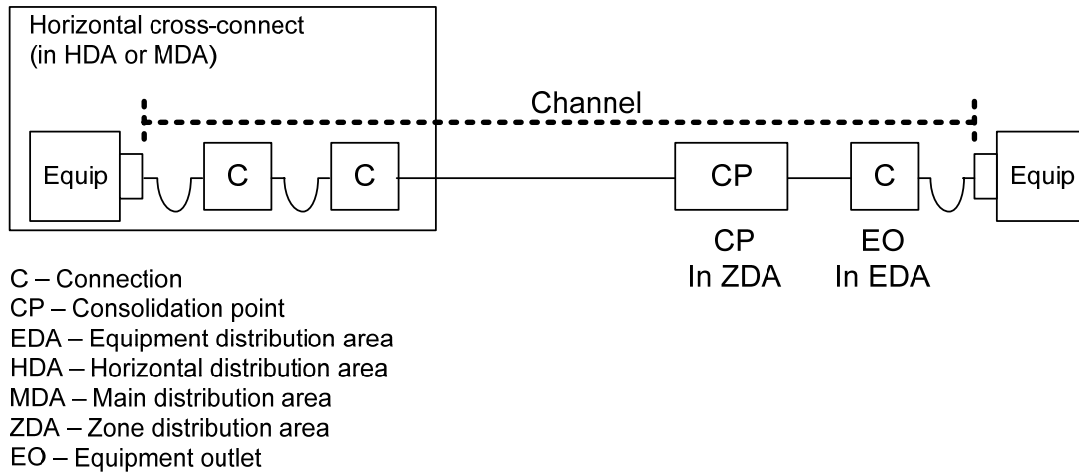


Figure 71: Channel Model Example

14.6.3.2.2 Permanent link

14.6.3.2.2.1 Requirements

The permanent link test configuration shall be used to certify the permanent link performance of permanently installed balanced twisted-pair cabling. The permanent link shall include:

- Up to 90 m (295 ft) of horizontal cable.
- A connection at each end of the horizontal cabling.
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA).

The permanent link configuration excludes the cable portion of the field test instrument cord and the connection to the field test instrument. See Figure 72 for an example of a permanent link.

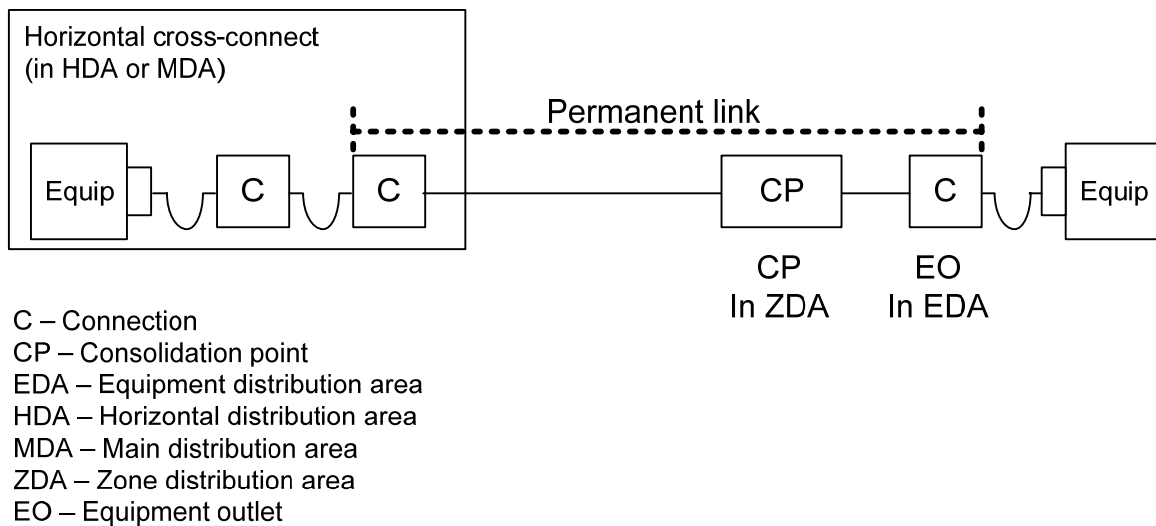


Figure 72: Permanent Link Example

14.6.3.3 Balanced twisted-pair cabling field test parameters

14.6.3.3.1 Requirements

The field test parameters to be measured shall meet the requirements of the cabling standard being followed (e.g., ANSI/TIA-1152, EN 50346). The field test instrument shall support all field test parameters specified by cabling standards.

A pass or fail result for each parameter shall be determined by the allowable limits for that parameter. The test result of a parameter shall be marked with an asterisk (*) when the result is closer to the test limit than the measurement accuracy.

Field test measurements shall be conducted at the temperature the cabling is intended to operate.

14.6.3.4 Balanced twisted-pair cabling field test instrument

14.6.3.4.1 Requirements

Field test instruments shall meet the accuracy requirements for the cabling Category or Class as defined in applicable standards (e.g., ANSI/TIA-1152 or IEC 61935-1). Accuracy Level IIIe or higher (e.g., Level IV) field test instruments are required to measure the appropriate Category/Class of cabling to ensure accurate field test measurements. Table 30 provides information on the minimum accuracy Level of the test instrument for testing ISO Class E_A, TIA Category 6_A and higher Classes/Categories of cabling systems. Table 30 describes the:

- Field testing configurations.
- Frequency range.
- Accuracy levels.
- Applicable industry standard.

Field test results that are outside the uncertainty band of the field test instruments are reported as either 'pass' or 'fail'. Field test results that are inside the uncertainty band of the field test instruments are reported as either '*pass' or '*fail' as appropriate. Measurement results having an asterisk '*' shall be evaluated by the relevant cabling standard, or as agreed upon in the contractual specification.

Table 30: Balanced Twisted-Pair Field Testing

<i>Field test configurations</i>	<i>Frequency range</i>	<i>Minimum accuracy level</i>
10GBASE-T Class E _A /Category 6A Permanent Link	1–500 MHz	IIIe
10GBASE-T Class E _A /Category 6A Channel	1–500 MHz	IIIe
Class F/Category 7 Permanent Link	1–600 MHz	IV
Class F/Category 7 Channel	1–600 MHz	IV
Class F _A /Category 7 _A Permanent Link	1–1000 MHz	IV
Class F _A /Category 7 _A Channel	1–1000 MHz	IV

14.6.3.5 Balanced twisted-pair field test connectors and cords

14.6.3.5.1 Field test equipment interfaces, adapters, and cords

14.6.3.5.1.1 Requirements

Test equipment interfaces, adapters, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these connectors. Test adapters, interfaces, and cords shall be replaced per manufacturer recommendations. Test adapters, interfaces, and cords shall meet the component requirements of the standards being followed.

14.6.3.5.2 User Cords

14.6.3.5.2.1 Requirements

User cords are equipment cords, patch cords or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

14.6.3.6 Balanced twisted-pair field test measurement results

14.6.3.6.1 Requirements

Field test results shall be stored in the native format of the field test instrument. The measured results of all pairs shall be reported in graphical and table format with the specification limits shown on the graphs or in the table at the same frequencies as specified in the relevant cabling specifications. The reports shall explicitly note whether the measured results exceed the test limits. Additionally, the test results shall be carefully reviewed to ensure compliance to specified standards.

Any reconfiguration of cabling components after testing may change the performance and thereby invalidate previous test results. Such cabling shall require retesting to confirm conformance.

14.6.4 Optical fiber cabling field testing

14.6.4.1 General

14.6.4.1.1 Introduction

An optical fiber cabling link may consist of a fiber or concatenated fibers (spliced, cross-connected, or interconnected) with a connector or adapter on each end.

There are two approaches for establishing the limits against which to validate an optical fiber channel, either:

- against the generic requirements set out in the cabling standard being followed for losses based on a predefined channel of a given distance; or
- against the loss requirements for a specific optical fiber application.

Factors that affect the attenuation measurements of installed and field tested optical fiber cabling include:

- The optical fiber type.
- The link length.
- The number and quality of terminations and splices.
- Cable stresses.
- Transmission wavelength.

Link attenuation can be adversely influenced by:

- Severe cable bends.
- Poorly installed connectors.
- The presence of particulate matter (e.g., dirt or dust) on the endface of connectors.

14.6.4.1.1 Requirements

Field testing optical fiber cabling shall be performed on length, optical attenuation and polarity. An optical loss test set (OLTS), also referred to as a power meter and light source, shall be used to measure optical attenuation and length, if capable, and may be used to ensure correct polarity. An optical time domain reflectometer (OTDR) shall be used to characterize anomalies or damaged areas along the installed fiber and to evaluate uniformity of connections (connectors and splices). A visible light source is a visible incandescent, LED or laser source used to trace fibers and may be used to verify polarity. Optical fiber cabling field testing shall be conducted in accordance with the published standards for the cabling solution being used.

Test cords and their connectors used for testing shall meet requirements for reference test cords (e.g., ISO/IEC 14763-3), which will provide accuracy and repeatability of the results obtained.

WARNING: All tests performed on optical fiber cabling that use a laser or light emitting diode (LED) in a test set are to be carried out with safety precautions in accordance with applicable standards (e.g., ANSI Z136.2).

14.6.4.1.1 Recommendations

An OTDR should be used to measure fiber length, reflectance, and optical return loss (ORL).

14.6.4.2 Optical fiber cabling field test configuration

14.6.4.2.1 Introduction

There are three test configurations available for use with an OLTS (see IEC 61280-4-1 and IEC 61280-4-2). These are:

- 1 jumper reference method;
- 2 jumper reference method; or
- 3 jumper reference method.

Used in conjunction with an OLTS, an optical fiber link may also be tested with an OTDR. This can be accomplished from one end of the fiber. However, a tail cord shall be placed at the far end of the link that is at least 100 m in length so that the far-end connector can be characterized.

14.6.4.2.2 Requirements

At the time of assembly or testing of optical fiber the installer shall view the endfaces of the fiber with a microscope. Viewing the endface may indicate that the endface is damaged or that it is contaminated (e.g., dirt, oil from fingers). When needed the connector shall be cleaned, repolished, or replaced before making connections.

Channels - channel links shall be tested with an OLTS using a three jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

Permanent links – permanent links shall be tested with an OLTS using a one jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

14.6.4.3 Optical fiber test parameters

14.6.4.3.1 Requirements

The field test parameters to be measured shall meet the requirements of the cabling standards being followed (e.g., ANSI/TIA-568-C.0, EN 50346). Testing installed optical fiber cabling for attenuation with an optical loss test set (OLTS), as described in cabling standards verifying the cabling length and polarity constitutes the minimum degree of testing.

Each optical fiber link shall be measured for its attenuation with an OLTS. Fiber length verification may be obtained from cable sheath markings or by use of the OLTS (if the OLTS has length measurement capability). Polarity can be verified with the OLTS while performing attenuation tests. A visible light source, such as a visual fault locator, can also be used to verify polarity.

The link attenuation allowance shall be calculated as follows:

$$\text{Link Attenuation Allowance (dB)} = \begin{aligned} & \text{Cable Attenuation Allowance (dB)} + \\ & \text{Connector Insertion Loss Allowance (dB)} + \\ & \text{Splice Insertion Loss Allowance (dB)} + \\ & \text{Reference jumper Repeatability Allowance (dB)} \end{aligned} \quad (12)$$

where:

- Cable Attenuation Allowance (dB) = Maximum Cable Attenuation Coefficient (dB/km) * Length (km)
- Connector Insertion Loss Allowance (dB) = Number of Connector Pairs * Connector Loss Allowance (dB)
- Splice Insertion Loss Allowance (dB) = Number of Splices * Splice Loss Allowance (dB)
- Reference jumper Repeatability Allowance (dB) = see Table 31

Table 31: Reference Jumper Repeatability Allowance

<i>Termination 1</i>	<i>Termination 2</i>	<i>Reference Jumper Repeatability Allowance</i>
MM reference grade	MM reference grade	0.1 dB
MM reference grade	MM standard grade	0.3 dB
MM standard grade	MM standard grade	0.5 dB (see note 2)

NOTES:

1. This table provides the reference jumper repeatability allowance using standard and reference grade terminations in accordance with IEC 60874-19-1.
2. 97% of individual connections are required meet this attenuation limit. As a minimum of two connections are present within installed cabling, a value of 0.5 dB is quoted on a statistical basis

NOTE: The optical lengths of certain cables (e.g., stranded loose tube) may be longer than the cable sheath due to the fiber lay within the cable sheath. However, the recorded length measurement is assumed to be the physical jacketed cable length.

An OTDR trace characterizes the installed fiber link resulting in an indication of fiber segment length, attenuation uniformity and attenuation rate, connector location and insertion loss, splice location and splice loss, and other power loss events such as a sharp bend that may have been incurred during cable installation.

An acceptable attenuation for optical fiber cabling shall be based on an attenuation allowance equation and then compared to the measured installed loss. The loss allowance equation is based on the component losses for each of the components in the permanent link or channel and includes optical fiber type, cable type, wavelength, link distance, number of connections (e.g., mated pairs) and number of splices. The mean insertion loss of each component shall be obtained from the manufacturer and used in the link attenuation allowance calculation.

14.6.4.3.2 Recommendations

An OTDR may be used to measure reflectance and ORL. Reflectance measurements of each connection should be:

- \leq -40 dB for a multimode UPC connection
- \leq -50 dB for a single-mode UPC connection
- \leq -60 dB for an APC connection
- \leq -60 dB for a fusion splice

ORL measurements should be better than:

- 20 dB for multimode
- 26 dB for single-mode

14.6.4.4 Optical fiber cabling field test instrument

14.6.4.4.1 Requirements

Optical fiber field test instruments for multimode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-1).

Optical fiber field test instruments for single-mode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-2).

14.6.4.4.2 Additional information

IEC 61280-4-1 has adopted the encircled flux metric for testing installed multimode optical fiber links. Field test instruments typically combine two wavelength sources through a single port. A single mandrel is typically placed on the launch cord to measure the two wavelengths, which reduces complexity and time. This two wavelength measurement procedure prevents alignment of each individual source wavelength to their separate encircled flux targets and requires a compromise alignment for each wavelength placement within the encircled flux template. Using a single mandrel, alignment performed for one wavelength to meet encircled flux (typically 850 nm) may result in the other wavelength (typically 1300 nm) to have some uncertainty. Additionally, the encircled flux limits do not account for enabling existing field test instruments that may meet outdated standards. The use of an external modal conditioner with existing field test instruments adds additional uncertainty. These cumulative uncertainties may cause variations outside the encircled flux limits, more so at one wavelength over another.

14.6.4.5 Optical fiber cabling field test interfaces, adapters, connectors and cords

14.6.4.5.1 Requirements

Test equipment interfaces, adapters, connectors, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these components. Test adapters, interfaces, connectors, and cords shall be replaced per manufacturer recommendations.

User cords are equipment cords, patch cords or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

Connector endfaces shall be inspected with a suitable microscope (minimum 100x magnification) and when necessary cleaned in accordance with manufacturers' instructions prior to mating.

NOTE: The use of temporary index matching materials (gels and/or fluids) in mated connectors under test is not recommended where the introduction of such materials may invalidate any measurement or test result.

14.6.4.6 Optical fiber cabling field test documentation**14.6.4.6.1 Requirements**

Documenting the test results provides the information that demonstrates the acceptability of the cabling system or support of specific networking technologies. A permanent record of all tests should be retained together with:

- Details of the measurement procedure.
- Details of the measurement type.
- Serial number of field test instruments used.
- Proof of calibration of the field test instruments used.
- Details of the test cords used.

14.7 Telecommunications cabling, pathways, and spaces administration**14.7.1 General****14.7.1.1 Introduction**

Documentation, labeling, and administration of data center components are critical to proper operation and maintenance of a data center. Administration systems may be manually operated or utilize an automated system. However, physical labeling of all items should be undertaken irrespective of the system being implemented. The following guidelines and recommendations contained in this section are for the administration of a data center.

14.7.1.2 Requirements

Data centers shall be provided with an identification/administration system following the hierarchical requirements of an approved standard (e.g., ANSI/TIA/EIA-606-A and ANSI/TIA/EIA-606-A Addendum 1). The administration system must include identification and labeling requirements for:

- Campus or site;
- Building;
- Indoor telecommunications space;
- Outdoor telecommunications spaces such as maintenance holes, handholes, joining chambers, pedestals, or outdoor cabinets;
- Cabinet, frame, or wall segment;
- Closure;
- Port or termination on closure;
- Backbone cable or cable between cabinets, frames, or wall sections;
- Pair/port within backbone cable or cable within distributor, telecommunications room, equipment room, or computer room;
- Splice - pair in splice on backbone cable or horizontal cable to outlets mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center;
- LDP - port in local distribution point in a data center;
- Horizontal cable to telecommunications outlet not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center;
- Telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center;
- Splice - pair in splice on horizontal link to telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center;
- CP - port in consolidation point on horizontal link;
- Patch cord or jumper;
- Outdoor pathway system;
- Campus or building entrance pathway system;
- Pathway system within a building;
- Fire stop in building pathway system;
- Data center pathway system;
- Bonding conductor for cabinet or frame;
- Cabinets, racks, and frames;
- Patch panels;
- Patch panel ports;
- Cables;
- Patch cords and equipment cords.

14.7.1.3 Recommendations

Supplies for labeling and administration should be part of an inventory system. Cable label makers, labels, markers, spare batteries and other supplies are often overlooked and should be readily available. This will help ensure proper marking.

14.7.2 Identification conventions for data center components

14.7.2.1 Spaces

14.7.2.1.1 Introduction

Spaces in the data center need to be identified and recorded to ensure operational efficiencies. Space identification is traditionally user specified. Additionally, architectural concerns could determine the labeling methods for spaces. Data center spaces are also defined in the various cabling standards.

14.7.2.1.2 Requirements

All spaces shall have a unique identifier.

All spaces shall be labeled.

14.7.2.1.3 Recommendations

A space summary report should be available listing all spaces, including their types and locations.

A space with access floor should track the computer room grid. Most computer rooms will use at least two letters and two numeric digits to identify every 600 mm × 600 mm (24 in × 24 in) floor tile. In such computer rooms, the letters will be AA, AB, AC ..., AZ, BA, BB, BC. and so on. For example, a floor tile located in the seventh row (AG) in the twelfth (12) column should be called AG12.

If the computer room is comprised of multiple spaces, the space identifier should be incorporated at the beginning of the floor space identifiers. Thus, the cabinet at AG05 in room 4DC should be named 4DC-AG05.

In general, space identifiers should be formatted as fs-XXYY, where:

- fs is the optional space identifier;
- XX is floor tile grid row;
- YY is floor tile grid column.

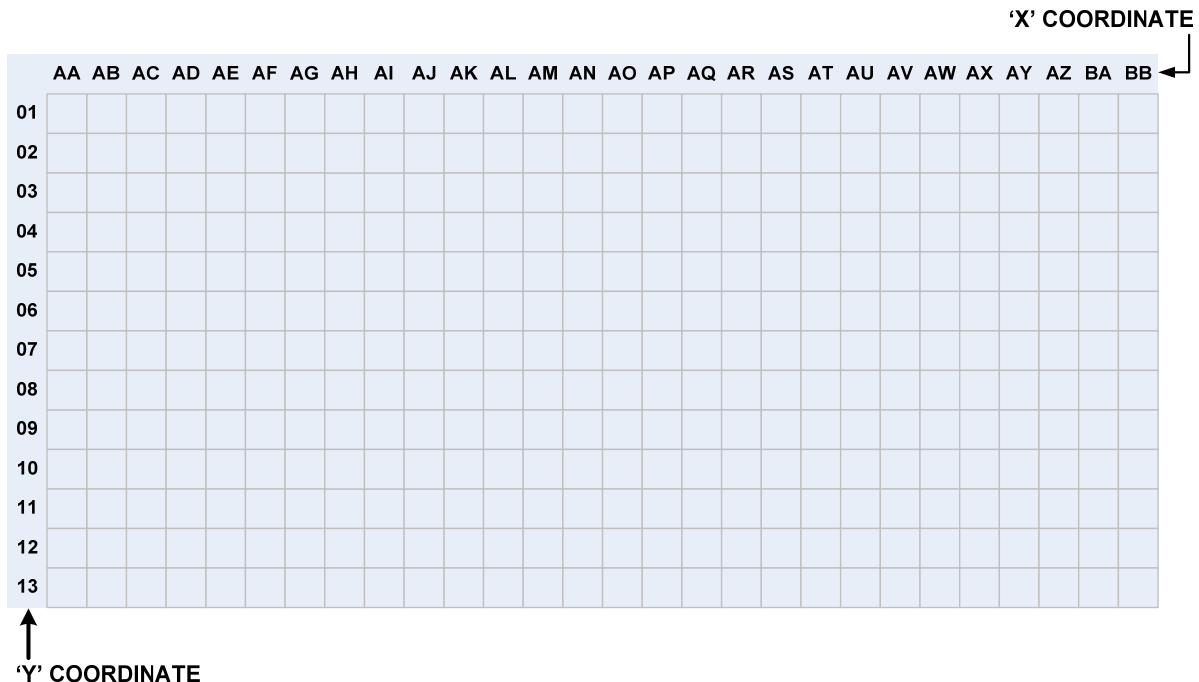


Figure 73: Room Grid Coordinate System Example

14.7.2.2 Pathways**14.7.2.2.1 Introduction**

Pathways include, conduit, tray systems or elements in the data center used to support and convey telecommunications cabling.

14.7.2.2.2 Requirements

All entrance pathways and pathways between rooms shall have a unique identifier per applicable standards (e.g., ANSI/TIA-606-A).

All entrance pathways and pathways between rooms shall be labeled at all endpoints.

14.7.2.2.3 Recommendations

Additional labeling should be provided at:

- intermediate points such as pull boxes and joined cable tray segments;
- regularly spaced intervals in closed loop pathways such as cable tray rings;
- partitioned pathways such as partition duct or innerduct. Unique identifiers shall be provided for each segment.

A pathways summary report should be available listing all pathways, including their types, origins, destinations, total capacities, and present fill conditions.

14.7.2.3 Records**14.7.2.3.1 Recommendations**

A rack, cabinet and frame summary report should be available listing all racks, cabinets and frames, including their types, locations, sizes, capacities, and current usage status.

A cabling summary report should be available listing all cabling, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, patching/cross-connection assignments, connected equipment, and unterminated or damaged pairs/strands.

It is also recommended that the database source for the cabling reports be able to provide end-to-end circuit trace connectivity reports from either end or from any intermediate point along the circuit.

A cross-connect summary report should be available listing all cross-connects, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, and connected equipment.

14.7.2.4 Active equipment**14.7.2.4.1 Introduction**

Active equipment includes switches, routers, hubs, firewalls, multiplexers, servers, external storage devices, and other equipment designed to support data center LANs, WANs, SANs, and computing infrastructure.

14.7.2.4.2 Requirements

All pieces of active and spare equipment shall have a unique identifier.

All active equipment shall be labeled on the front and back with their identifiers. These labels shall be machine generated and legible.

14.7.2.4.3 Recommendations

All pieces of active and spare equipment shall have a unique identifier associated with them keyed to the rack/cabinet/ frame in which they reside and the function they perform.

An active equipment summary report should be available listing all pieces of equipment, including their types, uses, location, connected backbone and/or horizontal cabling port/pair/strand assignments on termination hardware, other connected equipment.

14.7.2.4.4 Additional information

A two-digit counter or rack unit location can delineate the active equipment in each rack/cabinet/frame. The location of top of the equipment in rack units from the bottom of the usable space in the cabinet or rack is preferred.

An alternative to the rack unit designation is a counter. The counter should start at the top and proceed downward. On shelves with more than one piece of equipment, the counter should increase from left to right looking at the front elevation of the rack/cabinet/frame.

14.7.2.5 Bonding and grounding system**14.7.2.5.1 Requirements**

The bonding and grounding system and all components of the bonding and grounding system shall be labeled and identified on all “as built” documentation, in accordance with applicable cabling standards being followed and, if applicable, with manufacturer-recommended labeling systems.

14.7.2.5.2 Recommendations

Bonding and grounding system records should:

- Include next scheduled maintenance information. At a minimum maintenance should include an inspection and test all bonding and ground connections.
- All bonding and grounding system records should be available and kept on file. This should include the maintenance schedule.

14.7.2.6 Electronic documents**14.7.2.6.1 Recommendations**

Specifications for electronic documentation for the data center should be defined during the design phase and may be contingent on the size and type of the data center.

- Base building – Provide drawings in AutoCAD or similar electronic format.
- Data center – Provide drawings in AutoCAD or similar electronic format.
- Data center utilities – Provide all test results for the data center utilities, including but not limited to power, HVAC, and fire detection and suppression systems, in electronic format and keep on file.
- Balanced twisted-pair, coaxial, and optical fiber cabling – Provide all balanced twisted-pair, coaxial, and optical fiber cabling schedules and test results in electronic format and keep on file. Cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware.
- Power cabling – Provide all power cabling schedules in electronic format and keep on file. Power cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware.
- Rack and cabinet elevations – Provide drawings identifying rack layout and equipment placement in AutoCAD or similar electronic format.
- Active equipment inventory – Provide inventory list of all active equipment on drawings or approved electronic format.

14.7.2.7 Firestopping**14.7.2.7.1 Recommendations**

A firestopping system should be labeled and should include digital pictures.

Fire detection and suppression systems should be identified on all as-built documents.

Fire stop submittals, including manufacturer cutsheets and installation instructions, should be available and kept on file.

14.7.2.8 Alternate power systems**14.7.2.8.1 Recommendations**

The data center may contain various emergency power systems necessary for redundancy. These should be identified and be labeled.

All components of the alternate power system shall be labeled and identified on all as built documentation.

All alternate power systems records should be available and kept on file. This should include the maintenance schedule.

14.7.2.9 Change control**14.7.2.9.1 Introduction**

Access and change control policies and procedures are important elements to consider during the design.

Administration of the data center components is integral to the access and change control policies.

14.7.2.9.2 Requirements

Change control procedures shall be posted and be part of the access requirements. Work shall only be performed after proper approvals.

Change control process shall identify the proper work in progress practices.

Change control process shall include trouble ticket procedures and identify the proper site access as part of the resolution.

Change control procedures shall identify and include all required safety practices.

14.7.3 Intelligent infrastructure management**14.7.3.1 Introduction**

Intelligent infrastructure management features cabling records updating automatically upon changes of equipment cord or patch cord positions in a given intelligent patching field. The system may be implemented with the addition of an analyzer or scanner able to monitor all the cabling connections within a given distributor or patching field and update the system database.

The intelligent infrastructure management system is composed of patch panels, patch cords, analyzers or scanners, additional cables for connections between analyzers or scanners and the patch panels, and a management software usually installed in a dedicated server. Monitored patch panel ports are connected to the analyzer or scanner so when an equipment cord or patch cord is removed or inserted, the system will detect it and update the software database. Thus the network administrator will have access to the up-to-date information about the cabling system at any time.

Some benefits of intelligent infrastructure management:

- physical connections between switch ports and patch panel ports can be monitored in real-time;
- equipment cord and patch cord connections are stored in a software database;
- communication with network devices can be implemented through SNMP (Simple Network Management Protocol);
- if SNMP is implemented, several network management features can be implemented in the intelligent patching system as alarm configurations, messages through e-mail, in case of unauthorized access to the network and/or other actions according to prior configuration;
- permits planning of work orders (moves, additions, and changes).

Some potential disadvantages of intelligent infrastructure management:

- difficult or impossible to retrofit into an existing infrastructure;
- additional labor resources required for long-term system administration;
- significantly more expensive than an equivalent nonintelligent infrastructure
- intelligent patching may involve significant recurring costs;
- consumes additional rack units at locations wherever patching is managed;
- depending on the product selected, manufacturer specific equipment cords or patch cords may be required;
- SNMP may be considered by some users to be unacceptably intrusive, and consume an unacceptable degree of network bandwidth.

Intelligent infrastructure management systems may be implemented using two configurations:

- Interconnection;
- Cross-connection.

Interconnection configuration is implemented by using sensor strips installed on the Ethernet switch ports to provide them with a means for detection of equipment cord or patch cord connections. Figure 74 depicts the interconnection configuration.

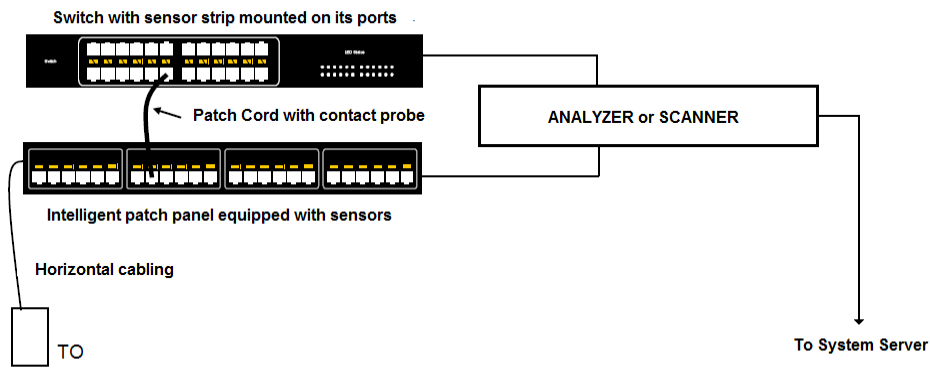


Figure 74: Intelligent Infrastructure Management Interconnection Configuration Example

Cross-connection configuration is implemented through a “mirror” patch panel between the Ethernet switch and the horizontal distribution. Switch ports are mirrored in the intelligent patch panel so connections will be made between patch panel ports only and not between switch ports and patch panel ports. This configuration is especially suitable for systems that operate with sensors or micro-switches for detection of equipment cord or patch cord connections. Figure 75 depicts the cross-connection configuration.

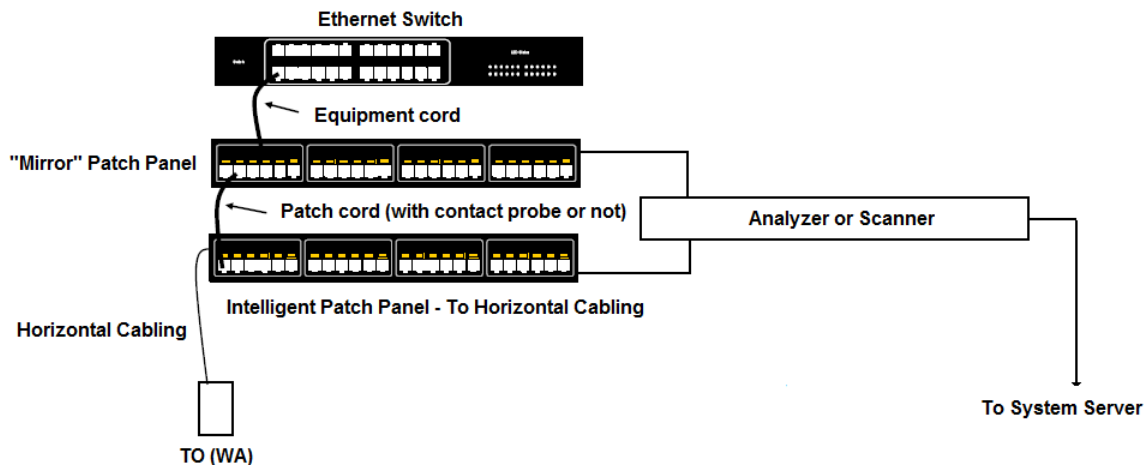


Figure 75: Intelligent Infrastructure Management Cross-Connection Configuration Example

14.8 Telecommunications Infrastructure Classes

14.8.1 Introduction

The reliability of the telecommunications infrastructure can be increased by providing redundant cross-connect areas and pathways that are physically separated. It is common for data centers to have multiple access providers, redundant routers, redundant core distribution and edge switches. Although this network topology provides a certain level of redundancy, the duplication in services and hardware alone does not ensure that single points of failure have been eliminated. The telecommunications topology Classes listed in this standard are consistent with the telecommunications infrastructure redundancy levels as defined in ANSI/TIA-942.

Figure 76 illustrates data center telecommunications cabling infrastructure redundancy at various Classes. Figure 77 provides an example of local area network and storage area network redundancy in Class F3 and Class F4 data centers.

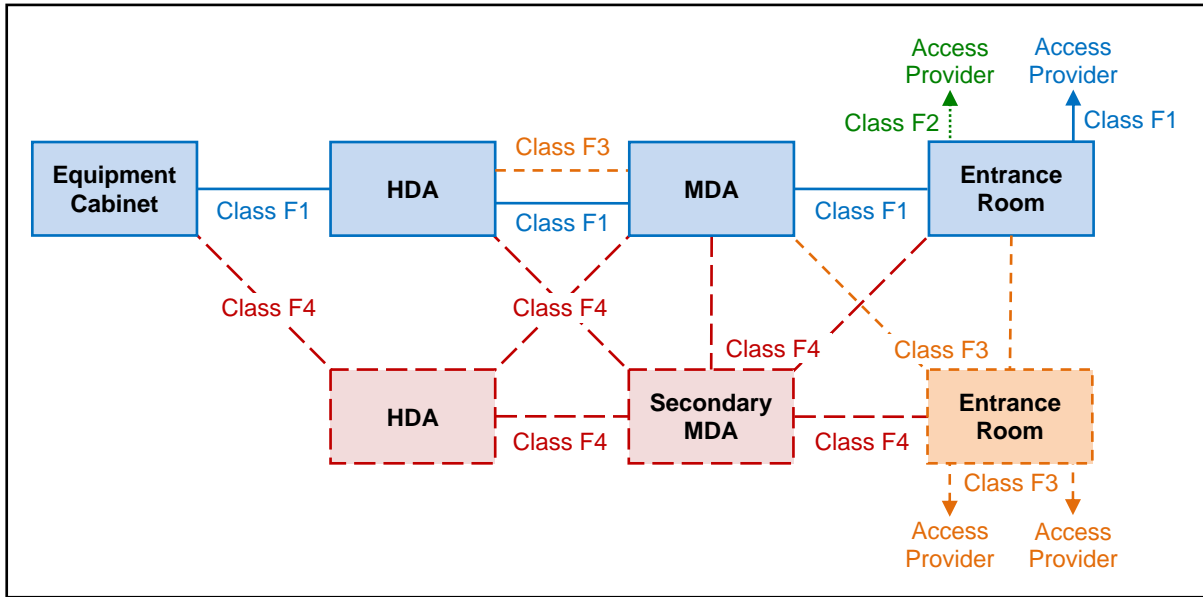


Figure 76: Telecommunications Cabling Infrastructure Classes

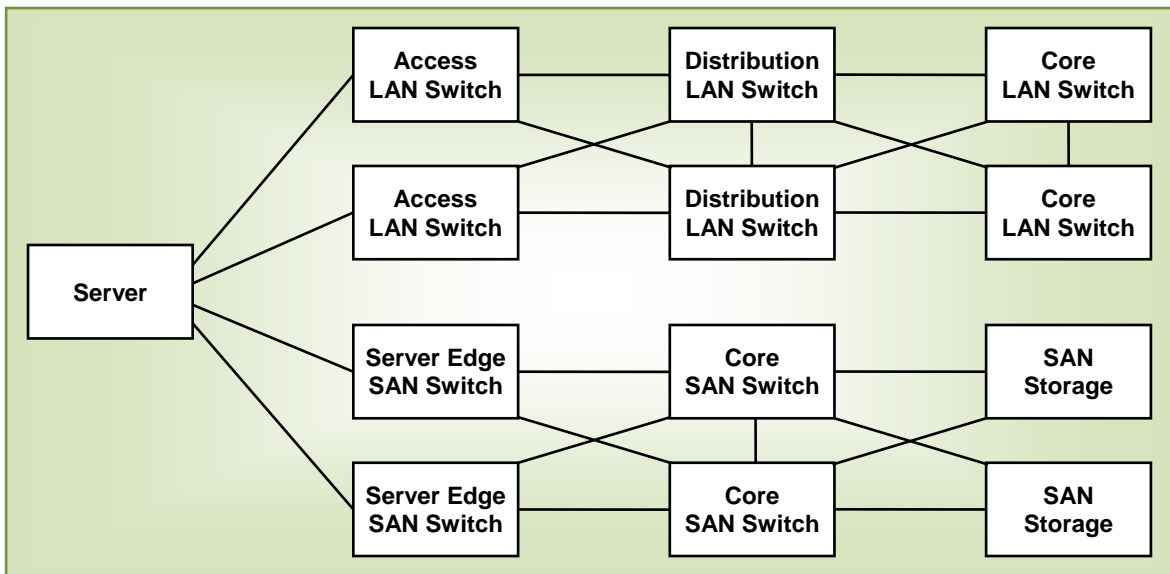


Figure 77: Example Of LAN And SAN Infrastructure At Class F3 And Class F4

14.8.2 Class F2 telecommunications infrastructure

14.8.2.1 Requirements

A Class F2 data center shall be served by at least two connections from the same or different access provider networks. Service shall be provided from two different points-of-presences at least 20 m (66 ft) apart. The physical path of the access provider connections shall be a minimum of 20 m (66 ft) along their entire routes. Class F2 data centers also provide component level redundancy for network equipment (e.g., redundant power supplies and processors for switches and routers).

14.8.3 Class F3 telecommunications infrastructure

14.8.3.1 Requirements

Class F3 must provide redundancy at system level (multiple routers and switches), redundant access providers, redundant entrance rooms, and redundant backbone cabling between HDAs, IDAs, and MDAs. The entrance rooms and pathways from the access provider offices to the entrance rooms shall be a minimum of 20 m (66 ft) along their entire routes.

14.8.3.2 Recommendations

Component level redundancy for routers and switches is not required for Class F3; however, the network should be configured in such a way that there is no interruption in service in the event of failure of any single network device or component.

14.8.4 Class F4 telecommunications infrastructure

14.8.4.1 Requirements

Class F4 adds a secondary MDA and requires that each equipment distribution area (e.g., equipment cabinet) be served by two HDAs. A Class F4 cabling infrastructure has no single-points of failure. Component level redundancy (e.g., redundant power supplies, processors or any modules within a device that requires business continuity) along with system level redundancy (multiple routers and switches) is required for Class F4. Class F4 can also be provided without redundancy at the component level, but for this purpose the system shall be configured as 2(N + N) instead of 2(N + 1). It is equivalent to two separate Class F3 networks.

14.8.4.2 Recommendations

The network should be configured in such a way that there is no interruption in service in the event of failure of any single network device or component. Care should be taken to ensure that resiliency is not affected by the failure of any device.

This page intentionally left blank

15 Information technology

15.1 Disaster recovery

15.1.1 Introduction

There are several considerations when developing a disaster recovery plan. Some of the considerations are:

- offsite data storage;
- collocation facility;
- onsite data storage;
- HVAC failure;
- power failure;
- distance between data centers.

15.1.2 Offsite data storage

15.1.2.1 Cold site (recovery ranging from 24 hours to 5 days)

A cold site is typically a leased or a company owned disaster recovery facility providing only the physical space for recovery operations. Clients provide their own hardware, software, and network. Depending on the level of services contracted, equipment is either ‘cold’ (stored at the site) or ‘cool’ (powered up but not in service). Clients transfer data on physical media like tape and optical media. The clients can also transfer data over point-to-point communication lines or via secure VPN tunnels directly to the site. Backup data may be transferred to a second off-site facility as well for remote storage of critical data. The ‘cold’ or ‘cool’ site method provides the replication machines, operating systems and applications required for disaster recovery at significantly less cost than having a full backup data center. However, recovery time may be unacceptable. The cool disaster recovery site should be tested regularly.

15.1.2.2 Warm site (recovery ranging from 30 minutes to 8 hours)

A warm site is a backup site having some, but not all of the components necessary to immediately restore all business functions. During a disaster, obtaining additional hardware and software will delay recovery to some degree. A warm site can function as a second production data center until needed for disaster recovery. Because the warm site must be able to assume the primary site workload, data must be replicated and transferred to the warm site periodically. Generally, the data replication routine can occur anywhere from once every 24 hours to once a week. The data transfer often takes place through a high-speed data connection. In the event of a disaster, the warm site would run on one day or older data unless real-time mirroring of production data occurs. Real-time mirroring is expensive and requires data synchronization management.

15.1.2.3 Hot site (recovery ranging from 1 minute to 20 minutes)

A hot site is a fully operational offsite data processing facility equipped with both the hardware and software systems that can very quickly assume the disaster recovery workload. A hot standby site can be used as an active/active data center for certain applications. This can be achieved by replicating the data in a synchronized fashion between the data centers in real time.

A hot standby site can also be used as an active/standby data center for certain applications. To achieve that the data should be saved in a synchronized fashion but not necessarily in real time.

15.1.3 Collocation facility

A collocation facility is a data center in which multiple clients lease small portions of the computer room for their computer and network equipment. Companies typically lease anywhere from one rack or cabinet to several racks or cabinets enclosed in a secured fence or by walls. The equipment may be for backup recovery, for remote storage, or even the primary data center for that client. The advantage to the client is having a secured and controlled computer room environment without having to build and maintain a data center. The collocation owner is typically responsible for moving equipment into the spaces (often called cages), setting up customer-provided racks or cabinets, configuring communications equipment, and creating physical security access lists.

The collocation facility owner provides power as required by the client, circuit delivery facilities, and various levels of support. Collocation facilities generally offer high security, including cameras, fire detection and extinguishing systems, multiple connection feeds, filtered power, backup power generators, and other items to ensure high availability, which is mandatory for all Web-based, virtual businesses.

15.1.4 Onsite data center redundancy

Redundant pathways are typically designed to eliminate or reduce single points of failure in the cabling infrastructure.

Network equipment redundancy includes redundant routers, core, distribution, service appliances and/or service modules, and/or access layer LAN/SAN switches, hot-swappable port cards, spare wireless antennas, and power supplies.

15.1.4.1 Requirements

Backup equipment cabinets, racks and associated hardware are required for recovery of campus area networks and metropolitan area networks, long-haul fiber optic emergency facilities are provisioned for high-bandwidth connectivity to critical sites during disasters.

15.1.4.2 Recommendations

Equipment should be in cabinets supported by branch circuits from different electrical panels or power distribution units. Equipment with multiple power supplies and power cords should be plugged into different branch circuits for power redundancy. For equipment with one power cord, consider plugging the equipment into a rack-mount switch or power strip that is fed from two different branch circuits.

15.1.5 HVAC failure

Refer to Sections on Electrical, Mechanical, and Building Automation Systems for coordination of Disaster Recovery procedures.

15.1.5.1 Recommendations

Every facility should have a portable HVAC unit and an adequate number of large fans in storage to provide temporary service to critical equipment. Special considerations must be made in advance to ensure that power is available with the correct type of power receptacle. Additional advanced consideration is required for hot air exhaust from portable air conditioning units and properly sized exhaust tubes, including correct lengths. Exhaust tubes and ceiling grid connectors are not necessarily included with portable unit purchases but may be purchased separately.

15.1.6 Power failure

In general, the power disaster recovery efforts should include a consideration for redundant external power sources, alternate power supply methods and dedicated UPS units per equipment, equipment rack, or cabinet. (See also Section 9)

15.1.6.1 Recommendations

Power strips within the equipment cabinets or racks should be IP capable to allow for SNMP monitoring and reactive reporting of power consumption, spikes, dips, and preaction alerts.

Communications devices should support multiple power supplies and be capable of continuous operation in the event that one supply fails, loses power, or requires hot swap.

Ensure that equipment that has dual power supplies is plugged into separate PDUs, supported by redundant UPS and generator systems. A process or procedure should be defined to avoid plugging dual power supplies into same circuit or PDU.

15.1.7 Mirroring

Mirroring is the copying of data from the host system to a second system in real time. Because the data is copied in real time, the information stored on the second system is the same as the information on the host system. Data mirroring is critical for the speedy recovery of critical data after a disaster. Data mirroring can be implemented locally or offsite at a remote data center or collocation facility. When copying data offsite, it is important to consider the form of transmission used, as bandwidth and delay affect the performance and capacity of the mirroring or replication. Transmission methods such as ISDN PRI, T-1, T-3, E-1, E-3, ATM, Gigabit Ethernet, SONET, SDH, and DWDM are commonly employed.

15.1.8 Location of real-time redundant storage device

The location of the redundant storage devices is critical. Possible locations include housing the equipment in the same room, the same building, on campus and/or off-site. Considerations include the need to have quick access to the backup equipment for maintenance, disaster recovery timelines and policies, and security levels of protection of the stored information. Other considerations include the financial and criticality aspects of maintaining a real time, redundant databases.

15.1.8.1 Recommendations

It is generally desirable for redundant storage to be located off-site in a location far away enough to avoid losing both copies during a single disaster. It should be noted, however, that many data replication methods have distance limitations.

15.1.9 Physical connectivity methods and devices

Physical connectivity can take many forms (e.g., conventional copper, optical, satellite). Conventional methods include copper connections between devices within the same cabinet, rack, row, or room. While this is the most economical, equipment must be located within a limited distance not to exceed constraints that may limit bandwidth. Other methods can increase the distance and speed of replication; however, there is an inherent increase in costs associated with these methods, which include but are not limited to long-haul Ethernet, carrier MPLS networks, ATM, SONET, and DWDM.

15.1.10 RAID

Short for redundant array of independent (or inexpensive) disks, a category of disk drives that employs two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but are not generally necessary for personal computers.

There are number of different RAID levels:

- Level 0: striped disk array without fault tolerance—provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy; this improves performance but does not deliver fault tolerance; if one drive fails then all data in the array is lost;
- Level 1: mirroring and duplexing—provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks;
- Level 2: error-correcting coding—not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level;
- Level 3: bit-interleaved parity—provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used;
- Level 4: dedicated parity drive—a commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk; if a data disk fails, the parity data is used to create a replacement disk; a disadvantage to Level 4 is that the parity disk can create write bottlenecks;
- Level 5: block interleaved distributed parity—provides data striping at the byte level and stripe error correction information; this results in excellent performance and good fault tolerance; Level 5 is one of the most popular implementations of RAID;
- Level 6: independent data disks with double parity—provides block-level striping with parity data distributed across all disks;
- Level 7: A trademark of Storage Computer Corporation that adds caching to Levels 3 or 4.
- Level 0 + 1: a mirror of stripes—not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them; used for both replicating and sharing data among disks;
- Level 10: a stripe of mirrors—not one of the original RAID levels, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.

15.1.11 Distance between data centers

The synchronous replication of data and accessing of that data by applications, between two or more data centers is dependent on the distance between the data centers. The latency increases as the distance increase. The latency should be in limits so that application or the data replication write functions can show acceptable performance.

15.2 Channel and console cabling

15.2.1 Introduction

System consoles should be networked over Private IP address space and accessible from the operations center. Providing this type of architecture enables a ‘lights-out’ operation in that personnel do not need to be in the computer room, except when human intervention is necessary.

15.2.2 Mainframe channel cabling

15.2.2.1 FICON

Fiber Connection (FICON) is a high-performance protocol. FICON channels enable 100-Mbps of bidirectional link rates at distances up to 20 km over optical fiber cables. In addition, an I/O interface for mainframes supports the characteristics of existing and evolving higher speed access and storage devices.

In summary, FICON products—from IBM—use a mapping layer that is based on the existing ANSI standard, Fibre Channel-Physical and Signaling Interface (FC-PH). FC-PH specifies the physical signaling, cabling and transmission speeds for Fibre Channel.

Each FICON channel is capable of supporting more than 4,000 I/O operations per second, which allows each channel to support the same capacity as up to eight Enterprise Systems Connection (ESCON) channels.

Disaster recovery functions, such as tape vaulting, remote disk copy and geographically dispersed parallel Sysplex, which are multiple mainframes strapped together as a single unit, benefit from the large distance supported by FICON channels. Although direct links between FICON devices of 10 kilometers are supported, 20-kilometer links are possible under certain conditions. The FICON protocol also permits additional end-to-end error checking above that provided by the FC-PH transport.

FICON is also designed to support a mixed workload: Small data transfers, typical for transactions, do not have to wait for large data transfers to complete.

Instead, they are multiplexed on the link with the long running operations. This helps to simplify configurations and removes one of the inhibitors to having a single database for transaction processing and business intelligence workloads.

15.2.2.2 ESCON

Enterprise System Connection (ESCON) is an IBM optical fiber channel connection technology that provides 17-MB/sec throughput. ESCON provides direct channel-to-channel connections between mainframe systems and peripherals over optical fiber links at distances up to 60 kilometers (36 miles). It also provides a way for communication controllers and other devices to share a single channel to a mainframe.

Compared to the copper-based parallel bus and tag channels, ESCON provides greater speeds and uses a serial interface. An ESCON Director is a hub-and-spoke coupling device that provides 8-16 ports (Model 1) or 28-60 ports (Model 2).

15.2.2.3 Small computer system interface (SCSI) channel cabling

The term "SCSI cable" usually refers to a complete cable, including the wire, connectors, and possibly a terminator as well. A number of different types of cables are available with various connector types to create specific cable implementations.

SCSI cables come in two distinct varieties: external and internal. External cables are used to connect SCSI devices that do not reside inside the PC, but rather have their own enclosures and power supplies; internal cables connect SCSI devices installed within the system enclosure. These cables are different in construction, primarily because the external environment represents much more of a risk to data corruption. This means external cables must be designed to protect the data traveling on the cable. Internal cables do not have this problem because the metal case of the cabinet shields the components inside from most of the electromagnetic and radio frequency noise and interference from the "outside world". Thus, internal cables can be made more simply and cheaply than external ones.

External cables are commonly called shielded cables because they are made specifically to protect the data they carry from outside interference. They have a very specific design in order to ensure that data traveling on the cable is secured, including the following properties:

- Twisted-pair wiring—All the wires in the cable are formed into pairs, consisting of a data signal paired with its complement; for single-ended signaling, each signal is paired with a signal return or ground wire; for differential signaling, each "positive" signal is paired with its corresponding negative signal; the two wires in each pair are then twisted together; this twisting improves signal integrity compared to running all the wires in parallel to each other; therefore, an external narrow cable with 50 wires actually contains 25 pairs; a 68-wire cable 34 pairs; this sort of wiring is also commonly used in other applications, such as network cabling, for the same reason.
- Shielding—The entire cable is wrapped with a metallic shield, such as aluminum or copper foil or braid, to block out noise and interference.
- Layered structure—The pairs of wires are arranged in layers; the core layer of the cable contains the pairs carrying the most important control signals—REQ and ACK (request and acknowledge); around that core, pairs of other control signals are arranged in a middle layer; the outer layer of the cable contains the data and other signals; the purpose of this three-layer structure is to further insulate the most important signals to improve data integrity.

External cables have a round cross-section, reflecting the circular layers mentioned just above. These cables are not simple to manufacture, and external SCSI cables are generally quite expensive. For internal cables, special steps are not required to protect the data in the wires from external interference. Therefore, instead of special shielded, multiple-layer construction, internal devices use unshielded cables, which are flat ribbon cables similar to those used for floppy drives and IDE/ATA devices. These are much cheaper than external cables to make.

Even with internal cables, there are differences in construction (beyond the width issue, 50 wires for narrow SCSI or 68 wires for wide SCSI). One issue is the thickness of the wires used; another is the insulation that goes over the

wires. Better cables generally use Teflon as a wire insulation material, while cheaper ones may use PVC (polyvinyl chloride; vinyl). Regular flat cables are typically used for single-ended SCSI applications.

For Ultra2 or faster internal cables using LVD signaling, the poor electrical characteristics of flat ribbon cables begin to become an issue in terms of signal integrity, even within the PC. Therefore, a new type of internal ribbon cable was created that combines some of the characteristics of regular internal and external cables. Pairs are twisted between the connectors on the cable as with external cables but the ribbon remains flat near the connectors for easier attachment. Ultra2 pair twisting improves performance for high-speed SCSI applications. While pair twisting increases cost, Ultra2 cables are not as expensive as external cables. This technology is sometimes called twist-n-flat cable, since it is partially flat and partially twisted pair.

There are several variations of the SCSI cable, each with its own limitations:

- Single-ended (SE) SCSI—Most SCSI devices use SE SCSI signaling. In SE SCSI, each signal is carried by a single wire. SE SCSI is very susceptible to noise and has a rather short distance limitation, a maximum of 6 m (20 ft).
- Differential SCSI (also called high-voltage differential [HVD] SCSI)—Differential SCSI is incompatible with SE SCSI above because it uses differential signaling rather than single-ended signaling. The benefit of using differential SCSI is that it works well in noisy areas and can reach up to 25 m (82 ft) in distance.
- Low-voltage differential (LVD) SCSI—LVD is the newest type of SCSI cabling, and LVD SCSI specifications offer distances up to 12 m (39 ft) and legacy support if LVD/SE which offer LVD mode or SE mode. Most LVD SCSI devices are LVD/SE; however, the link can only run in SE mode or LVD mode. If one device on the SCSI bus is SE, all devices will be limited to SE limitations. All devices must be set to LVD to achieve LVD distance and speed capabilities; note that LVD SCSI cabling requires twist and flat ribbon cable and an LVD/SE terminator or a twist and flat ribbon cable with built-in LVD termination.

15.2.2.4 Serial console cabling in the computer room and operations center

15.2.2.4.1 Recommendations

The following recommended maximum distances for serial console connections using EIA/TIA-232-F and EIA/TIA-561/562 are as follows:

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 20 kb/s are approximately:

- 23 m (76 ft) over Category 3/Class C balanced twisted-pair cabling;
- 27 m (90 ft) over category 5e/class D or category 6/class E balanced twisted-pair cabling.

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 64 kb/s are:

- 8 m (27 ft) over Category 3/Class C balanced twisted-pair cabling;
- 10 m (31 ft) over category 5e/class D, category 6/class E or higher balanced twisted-pair cabling.

15.2.2.5 KVM switches

15.2.2.5.1 Introduction

A keyboard, video, mouse (KVM) switch allows a single keyboard, video display monitor, and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time. The switch provides more table space in addition to saving the cost of multiple keyboards and monitors. KVM switches are commonly used at Web and other server locations with multiple computers but usually a single administrator or Webmaster.

IP protocols are also advancing into KVM switching systems that are used to access server consoles remotely. IP KVMs allow users to remotely control server screens via Web browsers. Wireless KVM solutions are also available. The systems encapsulate KVM signals into Ethernet packets for wireless transmission over the 802.11 wireless LANs. For large data centers, this means saving on KVM cabling and cable management, as well as more flexible server control. Security is provided through wireless LAN encryption and potentially by using proprietary protocols.

15.2.2.5.2 Recommendations

Consider using integrated KVM or console consolidation systems to avoid the need for keyboards, monitors, and mice for every system or rack. IP-based systems allow servers to be managed over the network, allowing support staff to be located away from the data center; however, these systems should incorporate security to ensure that only authorized personnel have console access to the servers.

15.3 Communications

15.3.1 Wired/wireless/hands-free voice communications

15.3.1.1 Introduction

Data center employees spend a lot of time during the day working on multiple systems within multiple cabinets or locations in the data center or adjoining facility. Efficient voice communications is a critical consideration when designing the data center. During critical down times, employees working to repair the system should not need to worry about where the nearest telephone is.

The communications industry provides several methods of technology to consider for this situation, including:

- **Wired:**
 - Desktop;
 - Wall mounted;
 - Rack mounted;
 - Intercom devices.
- **Wireless:**
 - Analog;
 - Cellular;
 - VoIP;
 - Hands free.

Advancements in wireless data technology and digital voice systems permit voice and data systems to share the same wireless system.

An intercom device can be designed in conjunction with overhead speakers and ceiling mounted microphones to provide hands free communication between the data center staff and support space. The intercom system can also be a very effective form of access control and can be integrated with video and the appropriate door release hardware.

Wireless equipment may not work well in a shielded computer room.

15.3.1.2 Recommendations

When using a wireless VoIP system, one of the more important tasks to perform prior to designing a wireless deployment is to conduct a wireless site survey. This survey will verify that wireless antenna coverage is adequate to provide appropriate Quality of Service (QoS) for voice and data applications.

The data center designer should refer to the most current version of the BICSI Wireless Design Reference Manual (WDRM) for further design considerations.

One note of caution when considering 2-way radios within the data center; some fire suppression systems contain blasting caps that are used to 'fire' the release pin on the suppression media tank in the event of a fire. Construction sites use similar explosive caps. Signs are often posted when approaching road construction that warns to turn off two-way radios and cell phones. These caps can be triggered by certain frequencies; therefore, it is advised that prior to using two-way radio communications in the data center, that the fire suppression provider be contacted. The manufacture or installation contractor will be able to specify if two-way radios can be used in or near the data center. It is further recommended that a NO RADIO ZONE be established of a size as determined by the manufacture if the data center is using a blasting cap type system (see Figure 78).

15.3.2 Wireless network for portable maintenance equipment

15.3.2.1 Recommendations

With the growing size and complexities of today's data centers, the designer should take advantage of the advancements in wireless technology to potentially provide a redundant maintenance network.

- personal digital assistant (PDA);
- tablets;
- scanners – asset tracking.

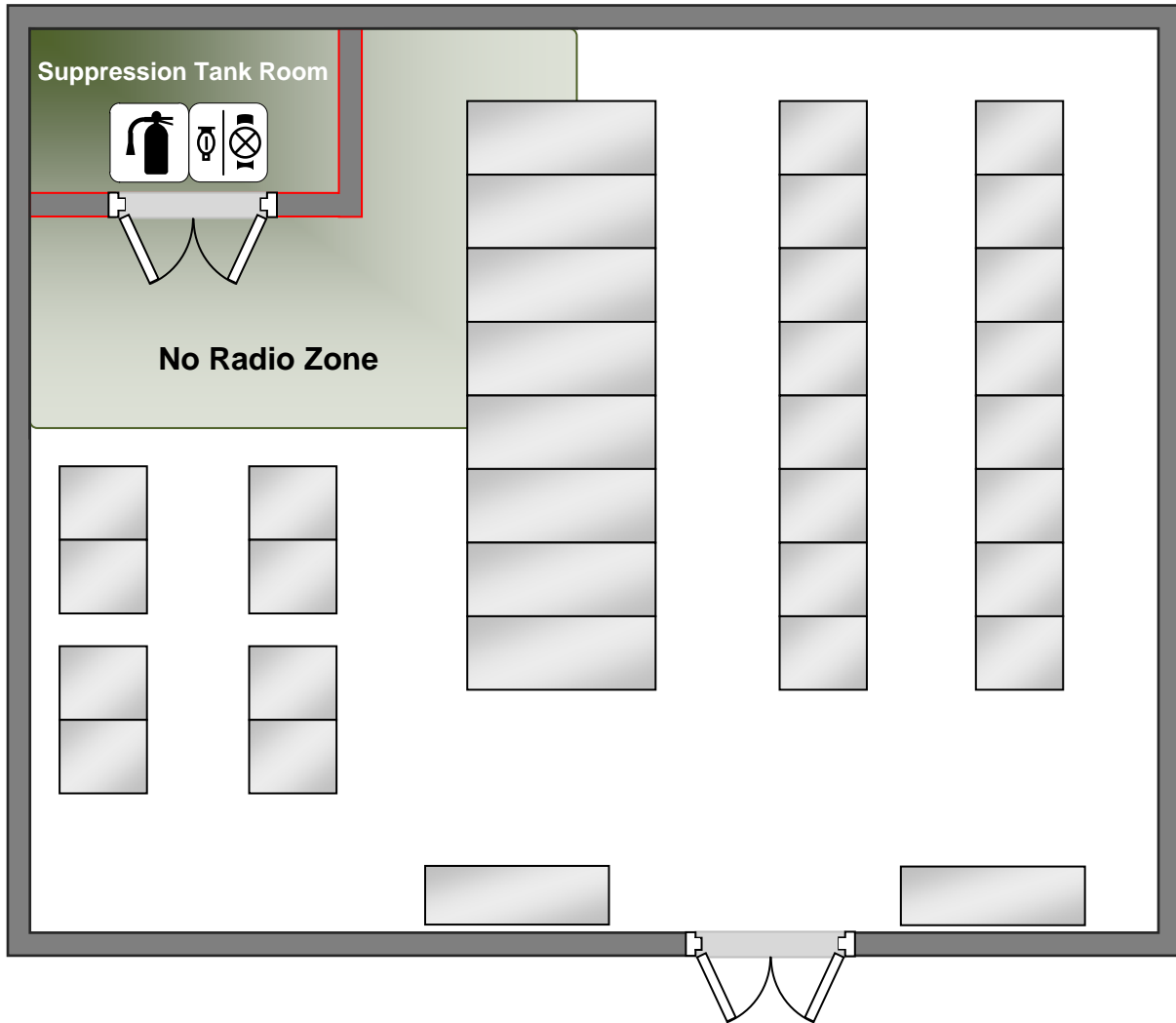


Figure 78: No Radio Zone Around Suppression Tank Room

15.3.3 Zone paging

15.3.3.1 Introduction

While overhead paging can be one of the more primitive forms of communication, it can still be very effective for regionalized voice contact in such areas as:

- control room;
- support space;
- computer room.

15.4 Computer room layout

15.4.1 Introduction

Computer room layout is affected by cable length restrictions for channel cabling, console cabling, LAN, SAN and WAN cabling.

15.4.2 Equipment line-ups for efficiency

15.4.2.1 Recommendations

- Hot and cold aisles:
Minimize the reintroduction of hot air into rack and equipment cold air intake vents by using blanking panels. Minimize the loss of the necessary static pressure under the access floor by means of dampers, brushes, or other means to seal cable cutouts and other openings in access floor tiles.
- Dedicated application rows;
- Dedicated equipment type areas:
 - The concept of same type equipment rows is a Best Practice method of both connectivity and airflow. From a connectivity perspective, some equipment is inherently fiber-connected, some copper connected, and some equipment uses proprietary cabling and share proprietary peripherals. By aligning same type equipment, the designer may be able to limit the use of proprietary cabling in cable pathways.
 - From an airflow perspective, having same type equipment cabinets or racks in same type rows helps keep a consistent airflow around equipment, allows for ease of hot/cold aisle design, and better prepares the computer room for portable cooling if necessary.
 - Consider separate areas of the computer room for rack-mounted and floor-standing systems to simplify cabling and rack/cabinet management.
 - Develop a small number of standard cabinet and rack cabling configurations for the computer room to simplify cable installation and administration.

15.4.3 Connectivity panel distribution

15.4.3.1 Introduction

Refer to the most recent version of the relevant standards and reference manuals (e.g., BICSI TDMM, ANSI/TIA-942, ISO/IEC 11801) for information on standards-based cabling distance limitations:

- copper and fiber panel distribution;
- dedicated network connectivity rack area;
- distributed connectivity racks:
 - standards-based rack;
 - standards-based cabinet;
 - underfloor.
- dedicated panels for each equipment cabinet or storage device.

15.4.3.2 Recommendations

Figure 18 is a representation of simple connection topography for a data center. The connections shown can be copper or optical fiber, so long as standards are not violated. Points to remember:

- Stay within recommended lengths.
- Check the AHJ on plenum issues for computer rooms.
- If running above the floor, watch for distance limitations from fire suppression elements (check with AHJ).
- If running under the floor, stay under aisle ways and do not run media under static equipment.
- Keep all runs at 90 degree turns (not violating bend radius); do not run media on an angle across the room.
- Map out all pathways and provide updated copies to computer room managers.
- If using underfloor cable tray, check with the floor and cable tray manufacturer for best practices regarding stanchion attachment.

The figure below is a basic representation of zone distribution. A zone distribution area can be housed above the floor in an equipment rack, or below the floor in an access box. Each method has both advantages and disadvantages. When housed above floor, the connections are easier to access for connection and maintenance. However, the above floor methods use floor space that would otherwise be available for equipment. Below floor methods provide better security and maximize above floor space. However installing zone boxes under the floor requires proper planning. The network team and the data center management need to agree on long-term commitments regarding placement of the remote distribution units as moving them is difficult in terms of the organization allowing for the necessary downtime. In addition, data center space planners need to understand that equipment cannot be placed on top of underfloor zone distribution areas.

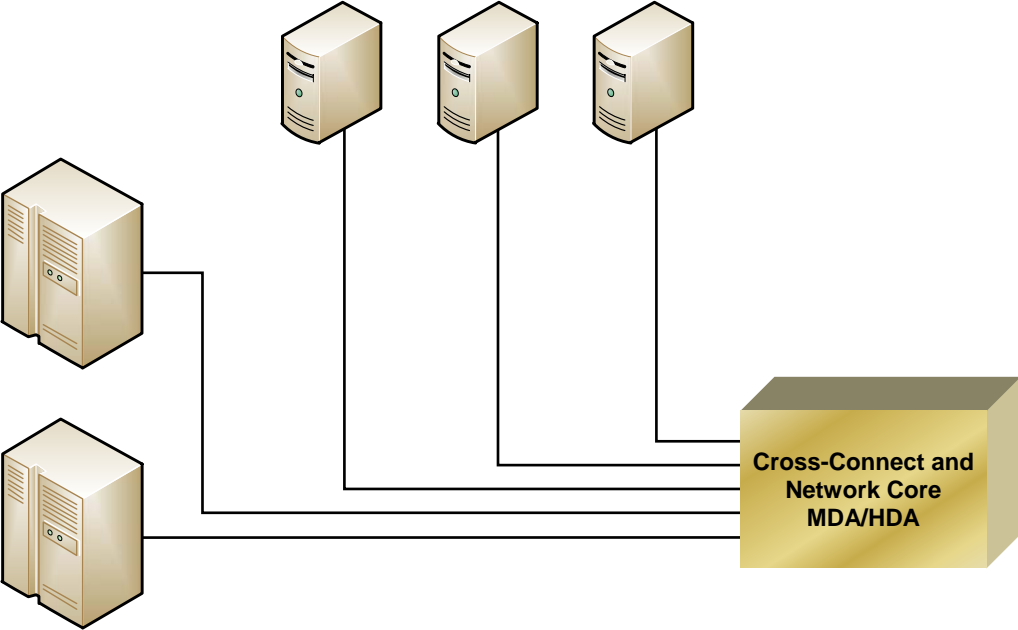


Figure 79: Simple Connection Topology

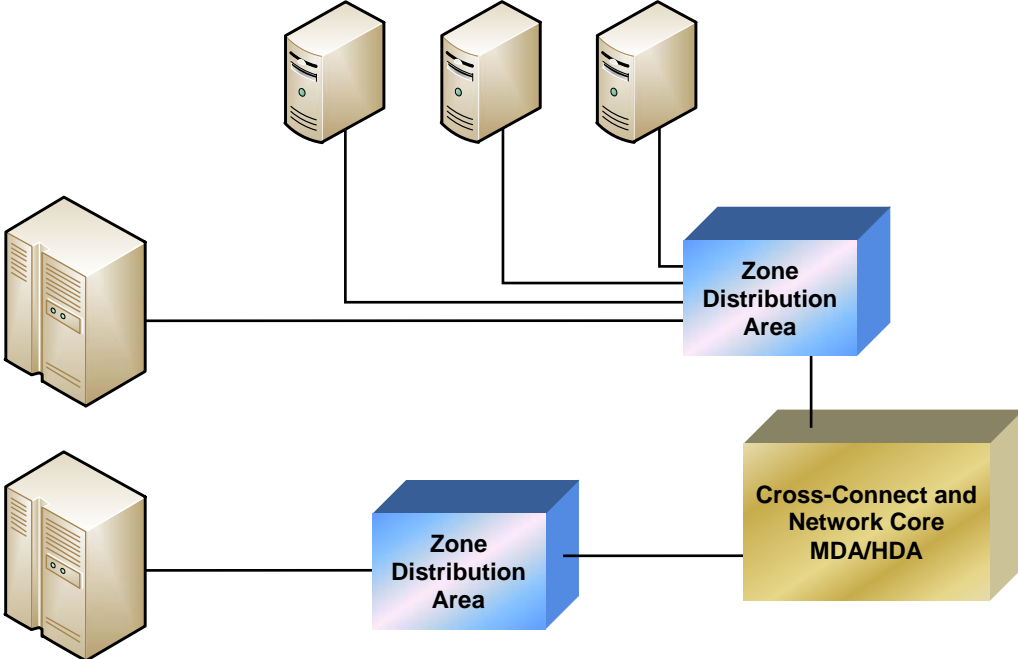


Figure 80: Sample Zone Distribution Topology

Figure 81 represents a redundant topology using redundant zone distribution areas. Notice that two totally separate pathways are used to keep maximum separation of the cabling from each ZDA.

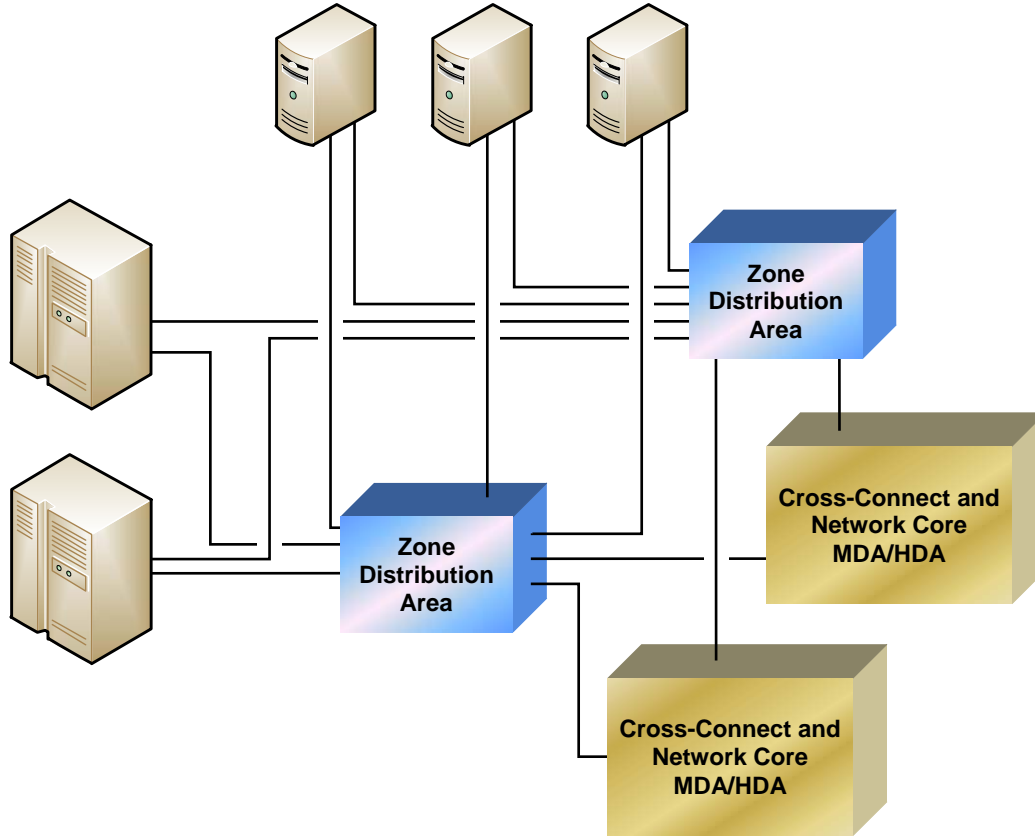


Figure 81: Sample Redundant Topology

15.4.4 Adequate material storage

15.4.4.1 Recommendations

The planner should account for enough storage for emergency parts and equipment to minimally maintain the data center in an event. Items could be stored in the following areas:

- control room;
- computer room;
- tape drives;
- hot swappable devices;
- patch cords;
- test equipment;
- in row;
- off-site or out of room staging area.

15.4.5 Aisle sizing and workflow analyses for proper walkways and egress pathways

15.4.5.1 Recommendations

It is suggested that the walk-ways be designed to accommodate the following requirements:

- cabinet portability;
- HVAC maintenance;
- accessibility and emergency egress—refer to Section 7: Architectural.

15.5 Operations center

15.5.1 Monitoring of building systems

15.5.1.1 Introduction

Refer to Section 10 and Section 13 for coordination. In general, the monitoring systems should be available within the Operations control center.

For more information about the monitoring of security cameras and access control devices, refer to Section 12.

15.5.2 Location

15.5.2.1 Recommendations

System consoles should be networked over Private IP address space and accessible from the operations center, so operations personnel do not have to be in the computer room except in cases when human intervention is necessary.

Operations center should be located adjacent to the computer room with a viewing window if possible to provide visual communications.

Center should be equipped with large screen displays for system/network tools (Plasma, Flat Panel, Touch Screen) such as power consumption, computer room humidity, and temperature.

This page intentionally left blank

16 Commissioning

16.1 General

16.1.1 Introduction

Commissioning is the process of ensuring systems are designed, installed, functionally tested, and capable of being operated and maintained according to the owner's design intent and operational needs.

Historically commissioning has been associated with the HVAC systems. Today commissioning has become an important quality control process that encompasses the entire building or data center.

Data centers' unique facilities requirements and systems should be commissioned according to industry guidelines and requirements.

16.1.2 Recommendations

The following systems should be considered for inclusion in the commissioning plan for a data center:

- electrical systems;
- HVAC systems;
- control systems (BAS);
- monitoring systems (BMS);
- fire protection and suppression systems;
- security systems;
- IT infrastructure components, including cabling and pathways;
- grounding systems;
- fuel oil pumping systems;
- inventory monitoring systems;
- lead detection systems;
- systems required by codes or local ordinance to be commissioned.

Commissioning should follow the sequence described in the next section.

16.2 Phases of commissioning process

16.2.1 Program phase

The program phase establishes the foundation for the other phases and determines the scope of work and systems to be commissioned. Objectives in the program phase include:

- crucial decisions are made;
- approvals are signed off;
- establishment of the design intent;
- funding and budgets are established;
- identify the team;
- determine the systems to be commissioned.

16.2.2 Design phase

During the design phase, the design of the data center components and systems is completed. Contract documents, specification documents and system documents are completed. The commissioning agent should review all documents to ensure compliance with the design intent. Objectives in the design phase include:

- architectural review of room or building;
- needs assessment/inventory of it requirements;
- design intent documentation submitted;
- IT, facilities, and architectural reviewed;
- review of scope of work for all participants, including contractors and vendors.

16.2.3 Construction phase

As the building or data center is constructed, the commissioning authority monitors the progress to ensure the design intent is being followed. Objectives in the construction phase include:

- milestone monitoring is performed;
- prefunctional testing is completed as required;
- field inspections and progress reports are submitted;
- change order process and approval authority are monitored;
- modification of the design intent is documented and approved.

16.2.4 Acceptance phase

During the acceptance phase, functional performance testing is performed on all the integrated systems. System calibration, manufacturers testing guidelines and other requirements established during the design intent are completed and documented. Nonperforming systems are identified and corrected prior to startup. Objectives in the acceptance phase include:

- functional performance testing;
- site audit;
- warranty audit;
- final documentation submittals and all test reports.

16.2.5 Post-acceptance phase

During the post-acceptance phase, operations and maintenance procedures are defined and monitored. As an extension of the acceptance phase the documentation of new systems, changes in the facility and a process for verification that the design intent is still being met should be clearly documented. Objectives in the post-acceptance phase include:

- O&M procedures established;
- documents storage and modifications to documents defined;
- training the personnel;
- moves, adds, and changes procedures established;
- change control procedures and policies implemented.

16.3 Types of commissioning

16.3.1 Introduction

Four types of commissioning can be employed depending on the project scope, client budgets and the design intent.

16.3.2 Continuous commissioning

- commissioning authority is engaged at the start of project;
- information gathering is on-going;
- ensure the design intent is maintained through project.

16.3.3 Milestone commissioning

- define design milestones procedures;
- perform testing, component validation, verification of design intent at agreed upon intervals.

16.3.4 Acceptance phase commissioning

- conduct required test on the integrated systems only;
- review all test and maintenance criteria prior to turnover;
- validate operational performance and correct deficiencies.

16.3.5 Network operability

- performance validation of IT systems before turnover;
- document observed performance to establish baseline criteria.

16.4 Testing

16.4.1 Introduction

As a quality assurance process, commissioning requires testing at various intervals and in conjunction with the design intent of the project. Functional performance testing is the basis for the commissioning process. The main

objective of functional performance tests is to ensure that all systems and equipment are operating efficiently and in accordance with the design intent.

16.4.2 Functional testing components

- equipment description;
- purpose of the test;
- required personnel, tools, and instruments needed to perform the tests;
- design information pertinent to the equipment or system under test;
- detailed sequence of operation, including any operating set points;
- scheduling requirements;
- special instructions or warnings;
- define expected results;
- sampling strategies.

16.4.3 Functional testing procedures

- inspection of equipment for manufacturing and installation defects;
- conditions of test;
- integrated systems test;
- what was done to the system to cause a response?;
- verification of response ;
- comparison actual response to acceptance criteria.

16.5 Commissioning documents

16.5.1 Introduction

Documentation is one of the primary differentiating aspects for implementation a commissioning process. Thorough documentation prevents random quality control and assurance that often lead to system inefficiencies.

16.5.2 Design documents

- design intent;
- building drawings;
- general equipment specifications;
- system submittals;
- architectural requirements ;
- change order;
- sequence of operation.

16.5.3 Process documents

- commissioning plan;
- reporting forms;
- schedules and timelines;
- meeting minutes and progress reporting;
- conflict and resolution records;
- startup and testing plans and schedule;
- training program.

16.5.4 Verification documents

- construction observation reports;
- deficiency logs and resolutions;
- test reports:
 - manufacturers;
 - contractor;
 - commissioning agent;
- Final commissioning report.

16.5.5 Operation and maintenance documents

- warranties;
- equipment operation and maintenance (O&M) manuals;
- as-builts;
- control drawings

16.6 Example of final commissioning report (informative)

The following is an outline of the information that should be included in the final commissioning report.¹

- project name;
- name, address, firm, and telephone number of commissioning authority;
- description of the building:
 - size;
 - location;
 - use;
 - construction.
- HVAC and other installed systems;
- list and description of commissioning tasks;
- commissioning plan;
- complete documents;
- completed design intent document;
- completed prefunctional test checklists;
- completed functional performance tests;
- all noncompliance forms;
- summary of commissioning findings;
- recommendations for system recommissioning;
- recommendations for monitoring the ongoing performance of the system;
- recommendations for system improvements.

16.7 Example of PDU testing (informative)

16.7.1 Purpose

To establish steps necessary to finish commissioning the PDUs and perform the Integrated Systems Test in customer room #1 while minimizing potential impact to critical customer equipment

16.7.2 Introduction

- connect temporary power jumper from M1BB tiebreaker to 1HUPSDP2;
- shift critical load to UPS 2B at the ASTS PDU level.
- transfer UPS system 1A to internal bypass from UPS mode;
- energize A side PDUs in customer room #1;
- transfer UPS system 1A from internal bypass to UPS mode;
- power up the B side of customer room #1 PDU/ASTSs using temporary power;
- perform ASTS Commissioning Procedure on STS 3B;
- leave A side PDUs in customer room #1 on the 1A UPS;
- shift critical load in Customer Room #3 and Network to UPS 1A at the ASTS PDU level;
- transfer UPS system 2B to internal bypass from UPS mode;
- energize B side PDUs in customer room #1;
- transfer UPS system 2B from internal bypass to UPS mode;
- restore power to normal power paths.

16.7.3 Systems impacted

The following systems may be impacted by this procedure: UPS system 1A, UPS system 2B and all STS PDUs.

16.7.4 Backout plan

If a problem occurs with a PDU or STS during testing, it will be isolated from the system until it is repaired.

¹ Source – Building Commissioning Guide Version 2.2 US General Services Administration

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
			Run temporary power jumpers from M1BB tie breaker to panel 1HUPSDP 2, 4, 6		
		N/A	Site check-in		
			Enable contractor badges for access to proper work areas.		
			Notify monitoring company of impending work. Disable ALC page out function.		
		30 min	Project meeting—introductions, review of project, safety, and tool inventory		
1			At the MSDA, select source 1 (UPS 1A) as the Master Source.		
2			Record the load on UPS System 1A at the SCC control panel: kVA _____ KW _____ Phase A amps _____ Phase B amps _____ Phase C amps _____		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
3			Record the load on UPS System 2B at the SCC control panel: kVA _____ KW _____ Phase A Amps _____ Phase B Amps _____ Phase C Amps _____		
4			Verify that all STS's are programmed with UPS 2B as Preferred source. If the STS is programmed with UPS 1A as the preferred source, transfer to UPS 2B as the preferred source using the following procedure: 3STS1A Time _____ 3STS2A Time _____ 3STS3A Time _____ 3STS4A Time _____ 3STS5A Time _____ 3STS6A Time _____		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
4c			3STS7A Time _____ 3STS8A Time _____ 3STS9A Time _____ STSNETA Time _____ 1) At the STS, select Monitor Mimic screen and verify that no alarms are present. 2) Select Source Transfer screen and verify: <ol style="list-style-type: none"> Source 2 voltage available; ON Source 1; Source 1 Preferred; OK to transfer; synchronization within 15°. 3) Simultaneously press Alarm Reset and Down buttons. 4) Verify transfer by checking ON Source Message : <ol style="list-style-type: none"> ON Source 2; Source 2 Preferred. 		
5			Verify load increase on UPS 2B. It should be approximately the same as recorded in step 1.		
6			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass is not inhibited.		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
7			Transfer UPS 1A from UPS mode to Internal Bypass by: 1) Verifying at UPS User Interface Panel: a. OK to transfer; b. Static Switch connected; c. no alarms present. 2) Review Load Transfer Procedures on the UPS User Interface Panel. 3) Using the Push to Turn Voltage Adjust Pot , set UPS output voltage 2 to 4 V above bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display).		
7c			1) If OK to Transfer is highlighted, simultaneously press Control/Enable and Bypass buttons. 2) Press Horn Off to silence alarm. 3) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker closed b. UPS Output Breaker open.		
8			Energize A PDUs on normal UPS Source: 1) In CR1 at Panel 1HUPSDP 1, 3, 5 open and lock out breaker being fed by temporary power from M1BB. 2) At UPS 1A SCC distribution in room XXX, close Feeder to 1HUPSDP 1, 3, 5 3) In CR1 at Panel 1HUPSDP 1, 3, 5 close Breaker Main – DP (Fed From UPS1A) 4) Close the Main Input breaker then the Subfeed 1 and Subfeed 2 breakers at: a. 1PDU1A b. 1PDU2A c. 1PDU3A d. 1PDU4A		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
9			Transfer UPS 1A from internal bypass to UPS mode by: 1) Verify at UPS SCC Monitor Mimic Panel. a. UPS on Internal Bypass b. UPS Modules are on line 2) Review Load Transfer Procedures on the UPS User Interface Panel. 3) Using the Push to Turn Voltage Adjust Pot, set UPS output voltage 2 to 4 V above Bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display). 5) If OK to Transfer is highlighted, simultaneously press Control/Enable and UPS buttons.		
9c			1) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker open b. UPS Output Breaker closed 2) Reset the UPS system output voltage to 488 V.		
10			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass in not inhibited.		
11			In customer room #1 open and lock out feed from UPS 2B to panel 1HUPSDP2, 4, 6.		
12			Close tie breaker in M1BB		
13			In customer room #1: 1) Close breaker 1HUPSDP2, 4, 6 2) Close tie breakers among 1HUPSDP2, 1HUPSDP4, and 1HUPSDP6 3) Energize B side PDUs		
15			Perform ASTS Commissioning Procedure on STS 3B: 1) Ensure that the ASTS is in normal operating mode, and that no alarms are present. NOTE: During the performance of the tests, verify proper normal and alarm indications are present. Verify remote alarm indications.		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
15c			<ol style="list-style-type: none"> 1) Apply 100% load to the output of the ASTS. 2) Perform calibration checks for source 1 and record in the appropriate table. 3) Infrared scan the source 1 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 1 PDU. 4) Perform a maintenance isolation to source 1 maintenance bypass. 5) Infrared scan the source 1 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 6) Perform a restoration to normal operation. 7) Perform a manual transfer to source 2. 8) Perform calibration checks for source 2 and record in the appropriate table. 9) Infrared scan the source 2 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 2 PDU. 10) Perform a maintenance isolation to source 2 maintenance bypass. 11) Infrared scan the source 2 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 12) Infrared scan the output breaker distribution section. 13) Perform a restoration to normal operations. 14) Perform a manual transfer to source 1. 		

16.8 Example of PDU and diesel generator testing (informative)

NOTE: Checkboxes (☑) have been incorporated into the following procedure to ensure full compliance to all steps contained herein.

16.8.1 Purpose

- to demonstrate that the new UPS module and diesel generator associated with the data center client facility will function in accordance with the manufacturer's specifications
- to ensure that these new critical power components will function accordingly in their parallel configuration

16.8.2 Scope

Testing to be performed as part of this procedure will be done as follows:

- 1) UPS 4 (600 kW required):
 - input and output THD measurements;
 - voltage regulation measurements;
 - step load transient response;
 - bypass transfer transient tests;
 - transfer to battery transient response;
 - rectifier ramp in measurement.
- 2) parallel UPS (1800 kW required):
 - voltage regulation measurements;
 - module output load sharing measurements;
 - step load transient response;
 - bypass transfer transient tests;
 - module fault off and restore transient response.
- 3) DG 3 (2000 kW required):
 - 4 hour burn in;
 - output THD measurements;
 - voltage regulation measurements;
 - step load transient response;
 - 100 % block load transient response;
- 4) parallel DG system (2000 kW required):
 - load sharing measurements;
 - voltage regulation measurements;
 - DG fault off and restore transient response.

16.8.3 Vendor's responsibility

The technicians from each vendor have the responsibility of operating their equipment, and guiding all attending personnel through this procedure.

Vendors are also responsible to provide copies of all startup paperwork, and all equipment specifications for review and inclusion into the final commissioning report.

A copy of all vendor paperwork must be available at the beginning of the commissioning to ensure that applicable equipment startup checks have been performed.

16.8.4 General contractor's responsibility

The technicians from each vendor have the responsibility of operating their equipment and guiding all attending personnel through this procedure.

Vendors are also responsible for providing copies of all startup paperwork and all equipment specifications for review and inclusion in the final commissioning report.

A copy of all vendor paperwork must be available at the beginning of the commissioning to ensure that applicable equipment startup checks have been performed.

They are responsible for ensuring that the following are available as needed during the performance of this procedure:

- technician(s) from the UPS vendor;
- technician(s) from the diesel engine vendor;

- a minimum of two site familiar electricians to assist as necessary in the performance of this test procedure (e.g., to operate electrical distribution breakers, and or assist with load banks as needed); Additional electricians may be required in the event that the commissioning process will otherwise be delayed;
- an Infrared camera and operator (must be an infrared camera with the ability to take sample thermograms to establish a baseline recording of all major electrical equipment);
- to provide the necessary air-cooled load banks and cables (please be sure that the cables provided are sufficient in length and ampacity for the amount of load); load bank positioning should be determined before cables are ordered; resistive load equal to the full load rating of each system to be tested shall be available:
 - 1) for UPS module load testing, the load banks should be connected directly to the output switchgear of each UPS module (this will require 480V load banks with external fan power capability):
 - 2) for UPS module testing 1200 kW required. The external fan power for the load banks must be connected to a source, which will not be interrupted during the commissioning process.
 - 3) for diesel generator testing, the load banks should be connected directly to the output of the paralleling cabinet. (This will require 480V load banks with external fan power capability):
 - for diesel generator testing, a minimum of twelve, ideal of twenty-four 2000 kW resistive load bank must be available.
 - The necessary diesel fuel oil.
- to ensure that all parties are aware of their individual responsibilities as they pertain to this procedure;
- to ensure that all testing prerequisites are met before the commencement of the commissioning procedure (this includes the load bank hookup and placement for each day of commissioning);
- to inform all applicable subcontractors that there will be no other work permitted in the spaces where commissioning is being performed. Failure to adhere to this requirement can result in personnel injury and/or equipment damage.

16.8.5 Testing agent's responsibility

The testing agent shall provide the necessary engineering personnel to complete the proposed testing, and will furnish the following test equipment or its equivalent:

- 2 each reliable power meters (RPM) power analysis recorder;
- 1 each Astromed Dash 10 Chart Recorder;
- 2 each Fluke Model 87 digital multimeters;
- 1 each Fluke 600A clamp-on current probe.

16.8.6 Requirements

- The diesel generator system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- Each diesel generator (single unit) shall be capable of accepting a 100% block load, and fully recovering (voltage and frequency) within 15 seconds.
- The diesel generator switchgear shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- The diesel generators shall be capable of paralleling, and load sharing to within 5% of each other from 25% to 100% system load.
- The UPS system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to this equipment.
- Resistive load equal to the full load rating of each system to be tested shall be available.
- During the performance of this procedure, no other work will be permitted in the spaces in which equipment is being tested (e.g., while UPS module testing is being performed, no other work will be permitted in the UPS room, or in the area through which load bank cables are run). No other work will be permitted on equipment feeding the equipment, directly or indirectly controlling power to devices being commissioned.

NOTE: This precaution must be adhered to since the proposed work will require testing on exposed and energized electrical equipment—other work in the area jeopardizes the safety of the testing engineers, and the individuals doing the work.

16.8.7 Emergency generator system testing

The purpose of this test is to record the operating parameters and compare them to the manufactures specifications. The results of this testing will also be used as a baseline for future testing.

NOTE: If at any time during the diesel generator testing should a call for emergency occur from any ATS the load bank shall be turned off, the load bank breaker shall be opened and the DG system returned to automatic operation.

16.8.7.1 Diesel generator

16.8.7.1.1 Diesel heat run

This step shall be performed by the diesel vendor and paperwork should be presented to the testing agent's engineer:

- Place this diesel generator on line and load to 2000 kW;
- Heat run at full load for four (4) hours;
- Take readings of voltage, current, frequency, RPM and all engine data available from the DG display panel (e.g., exhaust temperature, battery voltage, oil pressure, coolant temperature) every 15 minutes. Take a note of any RPM instability.

16.8.7.1.2 Infrared scan

- Infrared scan the engines once full load has been applied for a minimum of 1 hour.
- Infrared each cylinder head. Values shall be at the same aim point for each head and within 2.5 °C (4.5 °F) of each other.
- Infrared scan the four turbos and ensure uniform temperatures for all four.
- Conduct an infrared scan of all power terminal connections, Circuit Breakers, between the generator and load bank, and record temperature following a minimum of 15 minutes operation at 100% load. Terminal temperature shall not exceed 75 °C Maximum.
- Conduct an infrared scan of the generator bearing housing and record the generator bearing housing temperature. Bearing Housing Temperature shall not exceed 50 °C maximum.
- Repeat the steps in this section after 3 hours of full load operation for each diesel generator being tested. Any abnormalities should be brought to the engineer's attention.

16.8.7.1.3 Steady state tests

- Start the engine. Apply 100% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM at 100% load. Record data from the RPM meter and Engine Generator Panel on the attached data sheet.
- Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM meter at 50% load. Record data from RPM and Engine Generator Panel on the attached data sheet.
- Remove all load. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM meter at no load. Record data from the RPM meter and Engine Generator Panel on the attached data sheet.

16.8.7.1.4 Transient response tests

- With generator output at no-load (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the event recording as "0 to 50% Transient".
- With generator output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the event recording as, "50% to 100% Transient".
- With generator output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the event recording as, "100% to 50% Transient".
- With generator output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the event recording as. "50% to 0% Transient".

16.8.7.1.5 Block load test

The purpose of this test is to establish the load that this engine generator combination can accept and recover to rated voltage and frequency within 15 seconds.

With generator output at no-load, apply 100% rated kW load in one step. Make sure that the load does not exceed 100% capacity. For instance, if the generator is rated for 2000 kW, applying 2050 kW will cause the generator to respond out of specification. In this case, lowering the load by 100 kW is still acceptable as 100% block load. Record output voltage, current, and frequency with the RPM meter in **Monitor** mode. Annotate the event recording as, “0% to 100% Transient.”

NOTE: If the engine is unable to recover to rated voltage and frequency within 15 seconds, reduce the block load amount to 75% and repeat the test. Annotate the file accordingly.

16.8.7.2 Diesel generator parallel testing

NOTE: For parallel diesel generator testing, full system load for these tests is 2000 kW.

16.8.7.2.1 Steady state tests

- Place all engine generators on line. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM meter at no load. Annotate the RPM recording as, “0% Load”. Record data from the RPM meter and engine generator parallel panel meter on the attached data sheet.
- With no load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.
- Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM at 50% load. Annotate the RPM recording as “50% Load”. Record data from the RPM meter and Engine Generator Parallel Panel meter on the attached Data Sheet.
- With 50% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.
- Apply 100% load to the system. Take a snapshot of output voltage, current, frequency and harmonic content with the RPM at 100% load. Annotate the RPM recording as, “100% Load”. Record data from the RPM meter and Engine Generator Parallel Panel meter on attached Data Sheet.
- With 100% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.

16.8.7.2.2 Transient response tests

- With system output at no-load, (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the recording as, “0 to 50% Transient”.
- With system output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the recording as, “50% to 100% Transient”.
- With system output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the recording as, “100% to 50% Transient”.
- With system output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the recording as, “50% to 0% Transient”.
- With system output at no-load, apply 100% rated kW load in one step. Record output voltage, current and frequency with the RPM meter in **Monitor** mode. Annotate the recording as, “0% to 100% Transient.”

16.8.7.2.3 Generator fault testing

- Connect the RPM Power recorder to monitor three phase output voltage and current on the diesel generator parallel bus. Setup the RPM power recorder for 15 minute monitoring period, Create the new RPM **Site Information** directory and annotate it as, “DG Fault Offs”; Create new **Location Information** directories for each DG and annotate them accordingly.
- Place all diesel generators in parallel.
- Apply 100% load to the system.
- Link to the RPM power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory as, “Fault off and Restore DG 1”, and start recording.
- Open the output breaker for DG 1 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Restore DG 1 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Stop the RPM recording and download the data.
- Link to the RPM power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 2**, and start recording.
- Open the output breaker for DG 2 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Restore DG 2 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Stop the RPM recording and download the data.
- Link to the RPM power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 3**, and start recording.
- Open the output breaker for DG 3 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Restore DG 3 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- Stop the RPM recording and download the data.

16.8.8 UPS testing**16.8.8.1 Critical load isolation**

- Start the diesel generators using the test online position on the parallel switchgear.
- Ensure that the three circuit breakers (UPS-Input SWGR, UPS-Maint. Bypass A, and UPS-Maint. Bypass A) on the DG parallel switchgear are all closed.
- Transfer Switchboard UPS-Input to emergency.
- Transfer the UPS system to bypass.
- Transfer the Maintenance Bypass Switch A to Generator bypass.
- Transfer the Maintenance Bypass Switch B to Generator bypass.
- Open the output breakers on the UPS Parallel Switchgear.
- Shutdown the UPS system and connect the load banks.

16.8.8.2 UPS module # 1

UPS Data

Make: _____ Model: _____

Serial #: _____ kVA: _____ kW: _____

Battery Data

Make: _____ Model: _____

of Strings: _____ Jars/string: _____ Cells/Jar: _____ Float/Cell: _____

16.8.8.2.1 Steady-state load tests

- Connect the RPM meter to the input of the UPS module to be tested.
- Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:
 - 1) 100% load;
 - 2) 50% load;
 - 3) no load (0% load).
- Connect the RPM meter to the output of the UPS module to be tested.
- Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:
 - 1) 100% load;
 - 2) 50% load;
 - 3) no load (0% load).
- While 100% load is applied to the unit record the following on the attached data pages:
 - 1) 3-phase current into the input filter;
 - 2) 3-phase current into the output filter;
 - 3) 3-phase current into the rectifier(s).

16.8.8.2.2 Transient load tests

- Connect the waveform recorder to the output of the UPS module to measure three phases of output voltage, and one phase of output current.
- Record the following load step transients with the waveform recorder:
 - 1) 0%–50%–0%;
 - 2) 50%–100%–50%;
 - 3) 25%–75%–25%.
- Connect the Waveform recorder to measure three phases of system output voltage.
- Place the CT on one phase of the system SS bypass and record the following transfer transients with the waveform recorder:
 - 1) normal transfer to bypass with 100% load applied;
 - 2) module failure to bypass with 100% load applied.
- Place the CT on one phase of the UPS module's output and record the following transfer transient with the waveform recorder:
 - Transfer from bypass to UPS with 100% load applied.

16.8.8.2.3 Infrared scan

- Infrared scan the entire UPS module after 100% load has been applied for a minimum of 15 minutes.
- Infrared scan the upstream and downstream breakers of the UPS module after 100% load has been applied for a minimum of 15 minutes.

16.8.8.2.4 Battery discharge transient test

- Verify that the waveform recorder is set to measure three phases of output voltage and one phase of input current.
- Verify that 100% load is applied to the UPS module.
- Send the UPS module to battery. Record the following:
 - the initial transfer to battery with the waveform recorder.
- Restore the UPS input.
 - Record the utility restoration and rectifier ramp with the waveform recorder.

16.8.8.3 Parallel UPS system testing

Parallel System Control Cabinet Data:

Model #: _____ Serial #: _____

SCC Rating: _____ SCC Breaker Rating: _____ Amps.

16.8.8.3.1 Steady-state load tests

- Connect the RPM meter to the output of the parallel system cabinet.
- Apply 100% load to the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the RPM meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.
- Apply 50% load to the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the RPM meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.
- Remove the entire load from the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the RPM meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.

16.8.8.3.2 Transient load tests

- Connect the waveform recorder to the output of the parallel system cabinet to measure three phases of output voltage, and one phase of output current.
- Record the following load step transients with the waveform recorder:
 - 1) 0%–50%–0%;
 - 2) 50%–100%–50%;
 - 3) 25%–75%–25%.
- Connect the waveform recorder to measure three phases of output voltage, and one phase of the bypass current.
- Place four UPS modules on line, apply 100% system level load, and record the following transfer transients with the waveform recorder:
 - 1) Normal Transfer to bypass;
 - 2) Transfer from bypass to UPS.

16.8.8.3.3 Infrared scan

- Place all UPS modules in parallel.
- Place full system level load on the UPS System.
- Infrared scan the UPS side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.
- Transfer the UPS system to Static bypass and increase the load to full static bypass current.
- Infrared scan the Static Switch Bypass side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.
- Transfer the UPS system to Maintenance bypass and infrared scan the MBP side and distribution of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.

16.8.8.4 Parallel UPS module fault testing

- Connect the waveform recorder to monitor three phases of output voltage on the UPS parallel bus.
- Place all UPS Modules in parallel.
- Apply 100% load to the system.
- Place a waveform recorder CT on the output of UPS Module 1, and connect to the waveform recorder.
- Open the output breaker for UPS 1 to remove it from the bus. Record the transient with the waveform recorder.
- Restore UPS 1 to the parallel bus. Record the transient with the waveform recorder.
- Place a waveform recorder CT on the output of UPS Module 2, and connect to the waveform recorder.
- Open the output breaker for UPS 2 to remove it from the bus. Record the transient with the waveform recorder.
- Restore UPS 2 to the parallel bus. Record the transient with the waveform recorder.
- Place a waveform recorder CT on the output of UPS Module 3, and connect to the waveform recorder.
- Open the output breaker for UPS 3 to remove it from the bus. Record the transient with the waveform recorder.
- Restore UPS 3 to the parallel bus. Record the transient with the waveform recorder.
- Place a waveform recorder CT on the output of UPS Module 4, and connect to the waveform recorder.
- Open the output breaker for UPS 4 to remove it from the bus. Record the transient with the waveform recorder.
- Restore UPS 4 to the parallel bus. Record the transient with the waveform recorder.

16.8.8.5 Critical load restoration

- Shut down the UPS system and disconnect the load banks.
- Close the output breakers on the UPS Parallel Switchgear.
- Transfer the UPS system to bypass.
- Transfer the Maintenance Bypass Switch B to UPS.
- Transfer the Maintenance Bypass Switch A to UPS.
- Start the UPS system and transfer from bypass to UPS.
- Transfer Switchboard UPS-Input to normal.
- Shutdown the Diesel Generators by returning the DG parallel switchgear to Automatic.

16.8.9 Data tables

DIESEL HEAT RUN TEST DATA SHEET UNIT #: _____

DATA COLLECTED BY: _____ TEST DATE: _____

DIESEL MANUFACTURER: _____ RATING: _____

MODEL NO. _____ SERIAL NO _____

	<i>Time</i>	<i>0:00</i>	<i>0:15</i>	<i>0:30</i>	<i>0:45</i>	<i>1:00</i>	<i>1:15</i>	<i>1:30</i>	<i>1:45</i>	<i>2:00</i>
<i>Engine Data</i>	<i>Exhaust temp left (°F)</i>									
	<i>Exhaust temp right (°F)</i>									
	<i>Battery voltage (VDC)</i>									
	<i>Engine RPM</i>									
	<i>Oil pressure (PSI)</i>									
	<i>Fuel pressure (PSI)</i>									
	<i>Coolant temp (°F)</i>									
<i>Output</i>	<i>Phase A-B VAC</i>									
	<i>Phase B-C VAC</i>									
	<i>Phase C-A VAC</i>									
	<i>Phase A current</i>									
	<i>Phase B current</i>									
	<i>Phase C current</i>									
	<i>Frequency (Hz)</i>									
	<i>kW</i>									

DIESEL HEAT RUN TEST DATA SHEET UNIT #: _____

	<i>Time</i>	<i>2:15</i>	<i>2:30</i>	<i>2:45</i>	<i>3:00</i>	<i>3:15</i>	<i>3:30</i>	<i>3:45</i>	<i>4:00</i>	
<i>Engine Data</i>	<i>Exhaust temp left (°F)</i>									
	<i>Exhaust temp right (°F)</i>									
	<i>Battery voltage (VDC)</i>									
	<i>Engine RPM</i>									
	<i>Oil pressure (PSI)</i>									
	<i>Fuel pressure (psi)</i>									
	<i>Coolant temp (°F)</i>									
<i>Output</i>	<i>Phase A-B VAC</i>									
	<i>Phase B-C VAC</i>									
	<i>Phase C-A VAC</i>									
	<i>Phase A current</i>									
	<i>Phase B current</i>									
	<i>Phase C current</i>									
	<i>Frequency (Hz)</i>									
<i>kW</i>										

DIESEL GENERATOR TEST DATA SHEET

UNIT NO: _____ TEST DATE: _____

MANUFACTURER: _____

MODEL NO. GENERATOR _____ SERIAL NO. _____

ENGINE _____ SERIAL NO. _____

<i>Engine Data</i>						
	<i>No load</i>		<i>50% load</i>		<i>100% load</i>	
<i>Exhaust temp left (°F)</i>						
<i>Exhaust temp right (°F)</i>						
<i>Battery voltage (VDC)</i>						
<i>Engine RPM</i>						
<i>Oil pressure (PSI)</i>						
<i>Coolant temp (°F)</i>						
<i>Generator data</i>						
	<i>No load</i>		<i>50% load</i>		<i>100% load</i>	
	<i>Panel mtr</i>	<i>Test inst.</i>	<i>Panel mtr</i>	<i>Test inst.</i>	<i>Panel mtr</i>	<i>Test inst.</i>
<i>Phase A-B voltage</i>						
<i>Phase B-C voltage</i>						
<i>Phase C-A voltage</i>						
<i>Phase A current</i>						
<i>Phase B current</i>						
<i>Phase C current</i>						
<i>Frequency (Hz)</i>						
<i>L-L THD (%)</i>						

Paralleling Switchgear, 3 Generators in Parallel

		System output voltage			System output current			System additional readings		
		A - B	B - C	C - A	A	B	C			
No load	Panel meter									
No load	Test instr									
50% load	Panel meter									
50% load	Test instr									
100% load	Panel meter									
100% load	Test instr									

Parallel Load Sharing, All 3 Generators

	GEN 1			GEN 2			GEN 3		
Mtrs:	θA	θB	θC	θA	θB	θC	θA	θB	θC
0% GEN									
0% Swgr									
50% GEN									
50% Swgr									
100% GEN									
100% Swgr									

UPS MODULE #__

Load Test and Meter Calibration Data

		Input voltage			Input current			Output voltage			Output current		
		A-B	B-C	C-A	A	B	C	A-B	B-C	C-A	A	B	C
0%	Panel meter												
	Test inst												
	THD												
50%	Panel meter												
	Test inst												
	THD												
100%	Panel meter												
	Test inst												
	THD												

Input Harmonic Filter Current Balance

	AØ	BØ	CØ	AØ-N	BØ-N	CØ-N
AMPS						

Output Harmonic Filter Current Balance

	AØ	BØ	CØ	AØ-N	BØ-N	CØ-N
AMPS						

Rectifier Current Balance

	ΔA	ΔB	ΔC	YA	YB	YC
AMPS						

UPS System Cabinet Readings

		System output voltage			System output current			Bypass voltage		
		A-B	B-C	C-A	A	B	C	A-B	B-C	C-A
0%	Panel meter									
	Test instr									
	THD									
50%	Panel meter									
	Test instr									
	THD									
100%	Panel meter									
	Test instr									
	THD									

Parallel Load Sharing, UPS Modules 1, 2, 3, and 4

	UPS 1			UPS 2			UPS 3			UPS 4		
Mtrs:	θA	θB	θC	θA	θB	θC	θA	θB	θC	θA	θB	θC
0% UPS meter												
0% parallel meter												
50% UPS meter												
50% parallel meter												
100% UPS meter												
100% parallel meter												

Attendees:

Telecommunications Contractor: _____

Owner: _____

General Contractor: _____

Electricians: _____

UPS Vendor: _____

Infrared: _____

Diesel Vendor: _____

Diesel Switchgear: _____

17 Data center maintenance

17.1 Maintenance considerations

The purpose of this section is to provide general guidelines for all types of maintenance considerations within a data center. With the exception of power and cabling systems, very little vendor-neutral information is available regarding systems maintenance issues in data centers.

Electrical Systems and Structured Cabling Systems are governed by national and local codes and standards, over the installation that addresses maintenance issues for these systems. NFPA 70 (*NEC*), NFPA 70B, NFPA 70E, NFPA 75, NFPA 76, and ANSI/TIA/EIA-568-B are some of the codes/standards that are typically adhered to for the aforementioned systems.

IT systems, HVAC systems, Telecommunications systems and Access flooring systems generally have manufacturer and model specific maintenance requirements that are furnished by the manufacturer. When systems are selected and installed, most often the manufacturer, manufacturer's representative, or installation technician will provide maintenance specifications for the particular system being installed. Manufacturers or their representatives frequently offer maintenance contracts.

17.1.1 Introduction

All systems within and supporting the data center will require maintenance. Activities can include emergency maintenance, preventive maintenance, remedial maintenance, and maintenance actions required to upgrade systems. Therefore it is very important to keep in mind these maintenance requirements during the design, planning and operational stages of the data center.

Insufficient maintenance and/or maintenance spaces within the data center can result in extended downtime and potential damage to the supported systems. The "benchmark" number for systems availability within the data center is 99.999% availability. Systems Maintenance or lack thereof can positively or negatively affect the achievement of this critical systems availability number. Anecdotal evidence consistently shows that more data center interruptions occur during maintenance activities than at any other time. Therefore, all maintenance activities must be carefully planned and performed by personnel familiar with the entire system and all inter-dependencies. As part of the operational maintenance strategy a plan should be drafted determining order and sequence of all annual maintenance and testing procedures. It is especially important not plan works on primary and secondary components of the same system or mirrored components simultaneously.

Availability is a function of both meantime between failure (MTBF) and meantime to repair (MTTR). The latter impacts availability and not reliability. The formula below shows:

- as MTBF goes up, availability also goes up;
- as MTTR goes up, availability goes down.

$$\text{Availability} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})} \quad (13)$$

To achieve the high "nines of reliability," all of the elements of a system must be designed for high reliability and allow for minimum downtime for service, whether it is preventive or remedial.

The terms "predictive maintenance" and "just-in-time" maintenance come from a philosophy that is gaining popularity. It suggests that, because human intervention is as often causative as it is preventive, anything that can be done to minimize human error increases availability.

Systems maintenance also includes periodic testing of the systems to ensure that they are operating properly.

All electrical and mechanical equipment should be initially tested after installation and then periodically throughout the life of the equipment. Testing should be performed on the equipment individually and as an integrated system to ensure compatibility and proper interaction between equipment in accordance with the design intent. Frequency of testing shall conform to manufacturer's recommendation as a minimum. Equipment or devices susceptible to significant wear resulting from testing, such as (but not limited to) batteries, should not be subjected to more testing than is recommended by the manufacturer. Testing of equipment or devices performed at high risk should be limited to the recommendation of the manufacturer.

Backup system testing should be scheduled during off hours, even if the electrical systems are designed to keep all critical loads running when one or more electrical service feeds are shut down as the testing may uncover a defect that causes a system outage.

17.1.2 Requirements

The number one maintenance requirement that will apply to all the various systems is to always adhere to the manufacturer's maintenance specifications and/or the AHJ over the installation, (e.g., local code, *NEC*, OSHA). The AHJ typically evaluates an installation in compliance with applicable codes and regulations (e.g., NFPA 70, OSHA).

17.2 Systems requiring maintenance

17.2.1 Cabling systems

17.2.1.1 Introduction

Cabling systems once installed, will normally require very little maintenance, provided the structured cabling system is designed and installed to comply with appropriate codes and standards of the data center location. Properly built cabling systems do not generally break under normal usage without some external force causing breakage. Cable pathways and spaces are designed and built in compliance with applicable standards and follow the recommended cable fill ratios. There should be sufficient space for moves, adds, and changes that will normally occur as changes and reconfigurations take place in the data center. This is particularly important in a new data center where growth is expected. Cable access is the single most important factor for maintenance of structured cabling systems in the data center.

Cabling systems should be inspected periodically for cable degradation, cracks, abrasions, heat, deformation, brittleness, movement, corrosion, or other indications of abuse and/or age.

17.2.1.2 Recommendations

Only qualified personnel should be performing moves, adds, and changes.

Personnel performing changes should be trained in the data center standards and policies for:

- rack, cabinet, equipment, cable, patch cable, power strip, and power receptacle labeling;
- cable and patch cord color scheme (if used);
- routing and dressing of cables and patch cords;
- proper equipment installation (air intakes in the front, exhaust out back, preferably not on rail, labeling, routing of cables);
- connecting equipment to the proper power strips and receptacles to provide the desired redundancy.

Annual inspection or during move, adds, and changes performed by cabling technicians:

- inspect/repair/replace worn, cut, pinched cabling entering cabinets and at stress points in the cable management systems;
- inspect/repair secure mounting of all cable management systems;
- inspect/repair cable congestion points with in telecommunications switches and or servers;
- inspect/repair floor, wall, and ceiling cable penetrations for correct fire stop and or cable damage;
- inspect/repair any loose cable that could be snagged, cut or tripped over;
- remove any/all unused/abandoned cable whenever possible. (especially important at cross connections);
- ensure any unused terminated optical fiber is capped to prevent dust contamination or scratches on fiber ends;
- ensure that cabinets, racks, and raceways are properly grounded and that bonding conductors are secure. grounding connections should be inspected regularly (annually at minimum) to ensure that they have not been damaged, corroded, or come loose;
- ensure that all cabinets, racks, patch panels, cables, and patch cables are properly labeled.

17.2.2 Electrical systems

17.2.2.1 Introduction

Many electrical systems are required to support a working data center. Some of these systems will require more maintenance than others. Generators, batteries and UPS systems will require periodic maintenance at manufacturer-specified or industry standard intervals.

Safe performance of electrical maintenance and testing should conform to the manufacturers' procedures. Technicians must also follow applicable safety codes and standards such as NFPA 70B, NFPA 70E, NFPA 110, NFPA 111, IEEE stationary battery standards, and applicable local and federal guidelines.

The most important factor regarding electrical systems maintenance is safety. Consequently, all electrical work shall be performed by fully qualified, licensed/bonded/insured electricians/technicians who have been trained (and certified when such certification is available) on the specific type of equipment. All electrical work shall be accomplished in accordance with all applicable codes and regulations as mandated by the AHJ. Certain maintenance

functions, such as replacement of hot swappable elements, shall be permitted to be performed by trained operators when the equipment has been so designed and procedures have been specified.

NFPA 70B, Section 25.3.8, recommends routine maintenance on a semiannual basis for UPS systems. It also suggests what should be inspected, measured, and possibly tested.

NFPA 70B, Section 4, illustrates the importance of Effective Electrical Preventive Maintenance (EPM), its economic benefits as well as increased availability.

17.2.2.2 Recommendations

Perform inspections as required by the AHJ:

- all power connections secure;
- IR thermography scanning is recommended once per year to identify loose or poor connections and unbalanced electrical loads, all characterized by increased resistance or temperature rise;
- all receptacles and power strips properly labeled;
- all safety features in place and operational;
- doors and cover plates on panelboards and power distribution units in place and operating properly;
- UPS and power generation systems periodic maintenance inspections performed in accordance with manufacturer's specifications and or AHJ;
- consider battery monitoring in UPS systems;
- lighting systems checked and bulbs replaced as required;
- emergency lighting operational check as required by AHJ;
- BAS and fire alarm systems operational check as required by AHJ;
- ensure complete compliance with all mandated safety regulations (e.g., OSHA, NEC, local code, AHJ).

Perform inspections as specified by the equipment manufacturers.

The following is an example of one manufacturer's specified service intervals for electrical systems and components:

- 3-phase UPS—2 preventive maintenances (PMs) per year;
- VRLA batteries associated with 3-phase UPS—4 PMs per year;
- wet cell batteries associated with 3-phase UPS—12 PMs per year;
- 1-phase UPS—1 PM per year;
- VRLA batteries associated with 1-phase UPS—1 PM per year;
- Power distribution units (PDU)—1 PM per year;
- Static transfer switches—2 PMs year;
- dc power plants—2 PMs per year;
- VRLA batteries associated with dc power pants—4 PMs per year;
- Wet cell batteries associated with dc power plants—4 PMs per year;
- Remote monitoring systems—1 PM per year;
- TVSS—surge suppression devices—condition item only—no PM;
- IR thermography scanning—1 per year.

Perform inspections on batteries as recommended by IEEE standards – see the following sections.

17.2.2.2.1 VRLA battery recommendations

IEEE 1188 provides details for maintenance, testing, and replacement of stationary valve-regulated lead-acid (VRLA) batteries, including:

- monthly:
 - visually inspect for evidence of corrosion, container distortion, and dirt;
 - check overall battery float voltages at regular intervals (at least monthly if performed manually; continuous monitoring is recommended).
- quarterly:
 - measure and record cell/unit internal ohmic value, temperature, and voltage;

- annually:
 - measure and record cell-to-cell and terminal connection resistance and measure ac ripple current;
 - compare measurements to base line data, monitor trends, and identify units that fall outside of predicted range (per manufacturer’s recommendation);
 - replace battery units or strings as necessary;
 - if UPS is designed with continuously monitored modular battery cartridges, replace when notified by alarm.

17.2.2.2.2 Vented (flooded) lead acid battery recommendations

IEEE 450 details the recommended maintenance, testing, and replacement practices for vented, stationary, and lead acid batteries:

- monthly:
 - visually inspect for evidence of corrosion, container distortion or damage, and dirt;
 - check overall battery float voltages and charger float current;
 - inspect electrolyte levels; add water as required;
 - check pilot cell voltage and electrolyte temperature;
 - check for unintentional grounds.
- quarterly:
 - measure and record cell/unit voltage;
 - measure and record specific gravity and temperature of 10% of cells.
- annually:
 - measure and record cell-to-cell and terminal connection resistance;
 - measure and record specific gravity and temperature of each cell;
 - inspect structural integrity of battery rack or cabinet;
 - compare measurements to base line data, monitor trends, and identify units that fall outside of predicted range (per manufacturer’s recommendation);
 - replace battery units or strings as necessary.

17.2.2.2.3 Vented nickel-cadmium (Ni-Cd) battery recommendations

IEEE 1106 provides details for maintenance, testing, and replacement of stationary vented Ni-Cd batteries, including:

- monthly:
 - visually inspect for evidence of corrosion, container distortion, dirt;
 - check overall battery float voltages at regular intervals;
 - measure charger output current and voltage;
 - visually inspect electrolyte levels; replenish as required;
- quarterly:
 - measure and record pilot-cell electrolyte temperature.
- semiannually:
 - measure and record voltage of each cell.
- annually:
 - measure intercell connection torque;
 - yearly measure and record cell-to-cell and terminal connection resistance;
 - YEARLY inspect structural integrity of battery rack or cabinet;
 - check fuel quality for generators annually.

Reference IEEE 1184-2006, Annex G, “Maintenance and Testing Intervals”

17.2.2.2.4 Generator testing recommendations

Regular testing is required to maintain the generator per manufacturers’ instructions and code requirements. See NFPA 110 regarding recommendations for maintenance.

Testing under a load bank will prevent the potential of jeopardizing the critical load. However, local code may require testing under live load. Class F1 and F2 generator systems should have an extra breaker with lugs for connection of a portable Load Bank. Class F3 and F4 should have a permanent load bank for regular testing

17.2.3 HVAC systems

17.2.3.1 Introduction

HVAC systems in data centers are a critical component in the operation of the center. All IT and Telecommunications system operating within the data center have temperature and relative humidity operating ranges that must be maintained to prevent overheating and damage to critical system components.

Numerous commercially available environmental monitoring tools run on LANs and provide computer room environment reporting to the operations center. Operations personnel can then take preventative measures if computer room conditions begin to approach threshold temperatures.

It is very important that HVAC systems operate at optimal performance. To do so these systems must be maintained according to manufacturer's specifications.

Data center HVAC systems should always be maintained by qualified HVAC technicians that are available for service twenty-four hours a day, seven days a week

17.2.3.2 Recommendations

Recommended preventive maintenance for computer room air conditioning (CRAC) systems:

- monthly:
 - environment:
 - verify that each module is maintaining temperature and humidity set points;
 - record room temperature and humidity near the return vent of each module;
 - inspect for visible damage to module (dents, scratches);
 - inspect for environmental damage (dirt, dust, debris, liquid stains) around the module installation area;
 - inspect belts (if applicable) for wear and tightness;
 - record past month's alarm history – cause and response.
 - cleanliness:
 - check condition of return air filters; replace if necessary;
 - check condition of drain pan and remove any accumulation of debris.
 - mechanical:
 - ensure that all components of the blower and its motor are moving freely, with no signs of binding or damage;
 - inspect the set-screws on fan blades and bushings to make sure that they are tight;
 - verify that condensate line is flowing freely;
 - verify that the humidification system does not have leaks at the fill and drain valves and that these modes of operation are functional;
 - ensure that there are no kinks in the steam delivery system (where applicable) from the cylinder top to the steam distributor;
 - check for build-up in cleanable cylinders (where applicable) and clean as required;
 - replace disposable humidifier cylinders if necessary (where applicable);
 - verify chilled water supply temperature (where applicable).
 - electrical:
 - confirm that the incoming main power is within tolerance listed on the module's nameplate;
 - verify that the control voltage is within manufacturer's recommended tolerance.
- quarterly:
 - mechanical:
 - check water lines for leaks;
 - verify tightness of blower and its motor hardware.
 - electrical:
 - conduct an infrared (IR) scan of electrical panels and connection points. if hot spots are identified, schedule shutdown, deenergize the equipment, and tighten any loose connections;
 - record amperages for critical components (such as cooling coil fan motors, reheater, and humidifier).

- semiannually:
 - cleanliness:
 - check cleanliness of chilled water coil.
 - electrical:
 - verify that contactors and relays are operating correctly;
 - check the main power wiring for critical components such as reheat elements, evaporator motors, and humidifiers.
 - functional tests:
 - verify operation of the coil fluid (water regulating) valves and record pressure;
 - check the operation of all system alarms.

17.2.4 IT and telecommunications systems

17.2.4.1 Introduction

IT systems for data centers come in many configurations from small servers that fit in a single rack unit or blade server chassis module to very large multiple processor systems that consume several cabinets and can require a footprint of 1.7 m² (18 ft²) or more. The one thing all servers and associated peripherals have in common is that they all will require maintenance at some time.

All IT systems manufacturers should provide the necessary maintenance documentation and or Web-based technical support for their particular systems. Most will offer maintenance programs ranging from defective component mail in replacement to on-site maintenance technicians.

The key to IT systems maintenance is to provide sufficient space for qualified technicians to perform the required maintenance actions.

Telecommunications systems have advanced as rapidly as today's new generation of servers and are just as sophisticated. Systems can be ordered with redundant "Hot Swappable" components that make it possible to run virtually forever without taking a system offline for hardware maintenance.

Maintenance spaces are very important for Telecommunications systems due to cable congestion that often happens with large configurations installed in cabinets or racks.

Like IT systems, Telecommunications system manufacturers should provide the necessary maintenance documentation and or web based technical support for their particular systems. Most will offer maintenance programs ranging from defective component mail in replacement to on-site maintenance technicians. The key to Telecommunications Systems maintenance is to provide sufficient space for qualified technicians to perform the required maintenance actions.

Ethernet switches, commonly used to provide network connectivity to servers with in the data center, range in size from one rack space unit for a small office Ethernet distribution switch with eight, to forty eight connectivity ports (see Figure 82), to large enterprise class distribution switches that will take up nearly half (or more) of a standard 42U cabinet or rack and can contain four hundred or more connectivity ports.

Maintenance on a small switch usually consists of whole unit removal and replacement when failure is detected. In contrast, a large enterprise class switch will consist of a chassis with multiple "blades" and redundant power supplies. Maintenance on a large switch like this requires removal and replacement of the individual defective "blade" or power supply.

Some devices require front access for maintenance and others will require rear access for maintenance. It is wise to plan for both front and rear maintenance access. Some specialty peripheral equipment such as robotic tape storage systems can require front, rear and side maintenance access due to the complexity and size of the internal subsystems and components.

All equipment and systems proposed for installation in the data center will have manufacturer recommended installation specifications that must be reviewed in advance by planners, configuration managers and or facilities managers to help determine the maintenance space required for each respective system installed in the data center.

Planning for and allocating adequate maintenance space ensures expedient and safe maintenance activities on installed IT and Telecommunications systems.

17.2.4.2 Recommendations

Some IT systems must be maintained by factory authorized service technicians because of their proprietary nature and/or complexity, and some IT systems can be maintained by competent onsite personnel. Most checks would be performed during periodic maintenance inspections monthly, quarterly or annually.

- cleaning of cooling fans in all equipment;
- check/replace inoperative or noisy cooling fans in all equipment;
- cleaning or replacement of air filters where applicable;
- checking for failing/failed power supplies in equipment fitted with redundant power supplies;
- checking exposed cabling (power or data) for possible damage;
- confirm all computer and telecommunications equipment is properly labeled.

Whether maintenance activities are performed by factory-authorized technicians or trained competent on-site personnel, it is critical to adhere to the manufacturer's recommended maintenance plan for proper operation of IT and Telecommunications Systems.



Figure 82: One Rack Space Unit (1U) 24 Port Ethernet Switch

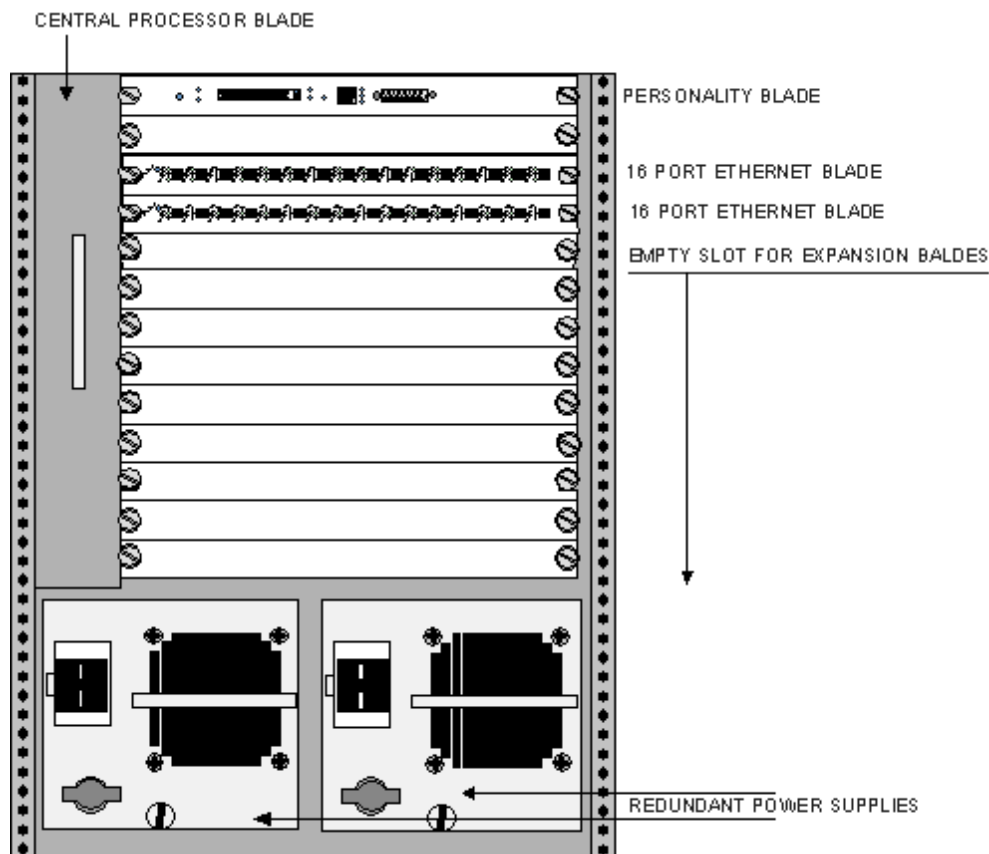


Figure 83: Enterprise Class Network Switch (Connectivity And Maintenance Access View)

The figures above are generic representations of switches that may be found in use in a data center. Network hardware and configurations are as varied as automobiles; the one consistency is that they are all designed to mount in standard cabinet/rack spaces.

Manufacturer specifications for maintenance space should always be followed as a minimum requirement. When manufacturer specifications are not available, one meter maintenance access space in front and rear is sufficient in most cases.

NOTE: High port density switches such as the one pictured above require careful and neat cable management in order to avoid patch cable congestion that will make maintenance (component removal or changes) difficult to perform without affecting connected users, particularly when the switch is installed in an enclosed cabinet.

Server cabinets can be configured with left side hinges in front and right side hinges in the rear or vice versa or doors that are split in the middle and therefore hinged on both sides in front and rear. Some manufacturers offer cabinets with removable side skins that allow like cabinets to be fastened together. Not all cabinets will be offered with an anti tip rail in the bottom but this is an important safety feature to look for in tall cabinets with a full complement of slide-out servers if the cabinet is not secured to the floor, however it is recommended that such cabinets be secured to the floor.

Liquid-cooled cabinets will require special procedures for access and maintenance due the high heat loads being generated in these cabinets. Any door open time will need careful planning to reduce the impact of cooling loss on the equipment contained in them.

Removing cabinet front and rear doors is not recommended for:

- cabinets that rely on ventilation fans installed in the doors or the presence of these doors for proper air circulation;
- data centers that rely on locked cabinet doors are lockable to prevent untrained/unauthorized personnel from accessing cabinet contents;
- data centers that are used as a ‘showcase’, where without doors present a poor aesthetic when tours are conducted.

NOTE: It is common in high-density server cabinets, to have multiple network connections required per server. Therefore it is imperative that careful and neat power and network cable routing and management is critical in these cabinets to prevent cable damage when servers are extended for maintenance service, as well as observing power and data cable separation requirements.

17.2.5 Access floor systems

17.2.5.1 Introduction

Access floor systems require maintenance as described in this section.

As IT, telecommunications, structured cable and power distribution systems are installed in, and moved around the data center, wear and tear of the access floor system will occur. Over time, dust and debris will accumulate in the sub floor presenting the potential for dirt infiltration into systems receiving conditioned air from under the access floor. Consequently maintenance inspections/actions and cleaning will be necessary to maintain the integrity/cleanliness of the floor system. The failure or collapse of an access floor system will result in extended down time. An unstable floor system is dangerous and can lead to serious injuries or equipment damage. Failure to maintain the access floor system may result in violation of AHJ codes or standards.

17.2.5.2 Recommendations

There are two categories of maintenance concerns for access floor systems: Structural and Environmental.

17.2.5.2.1 Access floor structural maintenance

17.2.5.2.1.1 Lateral instability

Lateral instability occurs when the floor system becomes loose and unstable. There are gaps between panels. Panels shift laterally when weight is applied.

Causes are:

- missing edge trim;
- lateral braces loose or untied;
- user abuse;
- incorrect cutouts;
- leaving panels out;
- poor installation;
- drastic temperature changes;
- multiphase installations.

Consequences are:

- structural damage to other floor components;
- equipment subject to shifting;
- personnel hazard;
- allows debris to drop on stringers causing vertical instability;
- reduction in plenum pressure from air conditioning;
- allows water/chemicals used in cleaning to corrode understructure;
- safety hazard.

17.2.5.2.1.2 Vertical instability

Vertical instability occurs when floor panels do not rest securely on the pedestal head or grid system, allowing the floor panels to rock; panels move up and down when weight is applied.

Causes are:

- missing gaskets;
- missing stringers;
- missing pedestal pads;
- dirt/debris on pedestal/grid caused by lateral instability;
- subfloor dirt/particulates forced on grid by air conditioning;
- removing stringers, not replacing properly;
- removing panels, not replacing properly;
- swollen wood core panels;
- warped panels;
- moving equipment on floor too soon after installation;
- tipped pedestal.

Consequences are:

- reduction in plenum pressure from air conditioning;
- tripping hazard for personnel;
- edge trim is exposed, subject to breaking (if edge trim is broken, laminate surface is exposed to chipping);
- dirt/debris drops into subfloor;
- permanent panel damage.

17.2.5.2.1.3 Missing edge trim

Missing edge means that edge trim has been removed, misplaced, or broken from panel edge.

Causes are:

- neglectfully not reinstalling after underfloor access;
- user abuse;
- vertical instability;
- lateral instability.

Consequences are:

- chipping of high-pressure laminate;
- carpet fraying;
- panel surface detachment;
- safety hazard (tripping);
- lateral instability;
- reduction of plenum pressure;
- collection of dirt/dust on grid and subfloor;
- allows cleaning chemicals to reach steel components;
- rapid aging of floor system.

17.2.5.2.1.4 Overloaded panels

Overloaded panels subject to weights exceeding load rating of floor system.

Causes are:

- heavy permanent loads (equipment, racks);
- heavy loads repetitively rolled over the floor panels.

Consequences are:

- floor system failure;
- permanent panel damage;
- rapid aging of floor system.

17.2.5.2.1.5 Perimeter tipping

Perimeter tipping occurs when the outside edge of floor is not level or in accordance with access floor specification.

Causes are:

- improper interface between perimeter panel and pedestal head;
- stringers not cut and bolted to the perimeter pedestal head;
- improper reinstallation (after removal for underfloor access);
- missing understructure.

Consequences are:

- safety hazard to personnel;
- lateral instability;
- dangerous to rolling equipment.

17.2.5.2.1.6 Panel surface detachment

Panel surface detachment occurs when panel surface (e.g., carpet, laminate, vinyl) becomes loose or detached.

Causes are:

- breakdown of glue from using improper cleaning chemicals;
- improper maintenance (flooding the floor);
- missing edge trim (if vertical instability is present);
- freezing (0 °C [32 °F]);
- rapid increase or decrease in temperature.

Consequences are:

- irreversible panel surface damage;
- tripping hazard;
- absence of surface leaves steel surface exposed to cleaning chemicals/water followed by rust.

17.2.5.2.1.7 Deformed panel surface

Panel surface deformations are individual or multiple indentations in the panel surface.

Causes are:

- dropping heavy objects on floor;
- rolling heavy loads with small caster wheels.

Consequences are:

- loss of static dissipative qualities of surface;
- rapid aging of floor system;
- unsightly appearance.

17.2.5.2.1.8 Chipped laminate

Laminate surrounding the outer edge of panel may become chipped or cracked.

Causes are:

- missing edge trim that causes exposure with vertical instability;
- unsealed cutouts;
- scratching.

Consequences are:

- irreversible surface damages.

17.2.5.2.1.9 Brittle edge trim

Edge trim surrounding the panel may become brittle and unstable.

Causes are:

- repeated uses of acrylic/polymer chemicals (wax).

Consequences are:

- breaking of edge trim leaves laminate surface open to chemicals that can detach surface covering;
- leaves laminate surface exposed to chipping;
- lateral instability;
- allows water/chemicals used in cleaning to corrode understructure;
- safety hazard from personnel tripping.

17.2.5.2.1.10 Missing components

Components may be removed or broken when panels are removed or replaced.

Causes are:

- not installing components properly after underfloor access;
- improper reinstallation of components.

Consequences are:

- improper access floor performance;
- structural damage;
- safety hazard;
- system failure.

17.2.5.2.1.11 Improper grounding

Floor system may fail to provide proper electrical ground.

Causes are:

- grounding clips are removed or not reinstalled properly.

Consequences are:

- loss of floor system conductivity;
- damage to equipment;
- injury to personnel.

17.2.5.2.1.12 Plenum leaking

Plenum pressure may be reduced when subfloor is used as an air plenum.

Causes are:

- missing edge trim;
- lateral instability;
- vertical instability;
- improper sealing the cutouts;
- using stringers without gaskets;
- not using cove base at perimeter and column locations to seal floor.

Consequences are:

- reduction in static pressure;
- improper balance of air delivery around sensitive equipment.

17.2.5.2.1.13 Subfloor particulate—rust

Causes are:

- excessive moisture in area;
- deterioration of pedestals;
- high humidity;
- leak under floor;
- flooding of floor system during cleaning.

Consequences are:

- component damage;
- component failure;
- unwanted rust flake particulate.

17.2.5.2.1.14 Uneven wear

Panels may not wear evenly due to excessive foot or equipment traffic.

Causes are:

- high traffic in certain areas;
- improper maintenance;
- not rotating panels periodically;
- equipment caster;
- chair caster of facility personnel.

Consequences are:

- loss of static dissipative qualities of panels;
- uneven panel wear;
- life of panels reduced;
- rapid aging of floor system.

17.2.5.2.1.15 Untrimmed cutouts

Panel cutouts may be without the proper edge molding.

Causes are:

- proper molding not installed when cutouts were made.

Consequences are:

- damage to cables;
- electrical hazard;
- employee injury;
- panel surface detachment (laminated surface exposed on sides to cleaning chemicals and water).

17.2.5.2.1.16 Warped panels

A warped panel is a panel whose structural framework has been altered.

Causes are:

- repeated heavy rolling loads with wide caster wheels;
- over wetting wood core panels causing panels to swell.

Consequences are:

- panel failure;
- rapid aging of floor system;
- vertical instability;
- unsightly appearance.

17.2.5.2.1.17 Miscellaneous problems

Some of other problems are:

- fascia needing repair;
- loose cutout trim (needing repair);
- bent stair nosing (creating safety hazard);
- ramp rubber torn (creating safety hazard);
- cover base loose/falling off (safety hazard);
- exposed grommet holes (tripping hazard).

Most of these problems can result in personal injury and structural damage to the floor system.

17.2.5.2.2 Access floor environmental maintenance

17.2.5.2.2.1 Underfloor conditions—subfloor debris

Causes are:

- unsealed cutouts;
- lateral instability;
- debris left over from construction;
- interim construction;
- improper maintenance of subfloor;
- using the cutouts in the floor system as a trashcan.

Consequences are:

- vertical instability;
- structural damage possible to other components;
- particulates harmful to computer equipment;
- unhealthy environment for employees;
- fire hazard;
- debris littering subfloor can block equipment-cooling fans.

17.2.5.2.2.2 Underfloor conditions—debris on grid and pedestal

Causes are:

- lateral instability;
- air forcing dirt and debris on grid system;
- unsealed cutouts;
- missing edge trim;
- improper maintenance of subfloor;
- flooding of floor surface causes build-up of residual water and chemicals on stingers and pedestals.

Consequences are:

- vertical instability;
- structural damage to other components.

17.2.5.2.2.3 Panel surface—improper maintenance

Causes are:

- uneducated maintenance personnel;
- improper cleaning chemicals;
- improper cleaning methods;
- flooding of the floor system;
- neglect.

Consequences are:

- permanent damage to floor system;
- structural damage to other components;
- unsightly appearance;
- loss of static dissipative qualities.

17.2.5.2.2.4 Panel surface—residual wax buildup

When access floor panels have been cleaned regularly, but they appear yellow, dingy, and dirty looking, more than likely residual wax has built up on the surface. This is a common problem with floor systems. Residual wax rapidly ages a floor system and should be removed. Careful, though, commercial wax removers will cause access panels to delaminate (panel surface becomes detached) and create a larger problem.

Causes are:

- cleaning crews using a mop in other areas of a building and using the same mop on the access floor;
- uneducated workers;
- wrong cleaning chemicals;
- improper cleaning methods.

Consequences are:

- affects static dissipating properties of surface;
- introduces unwanted contaminants into closed area;
- causes edge trim to become brittle;
- permanent damage to floor system;
- structural damage to other components;
- creates poor aesthetic quality of panel surface.

17.2.5.2.2.5 Panel surface—scuffs

Scuffs are markings on the floor area caused by foot traffic and caster wheels.

Causes are:

- heel marks;
- black casters;
- dragging equipment across panel surface.

Consequences:

- permanent damage to surface;
- unsightly appearance;
- rapid aging of floor system.

17.2.5.2.2.6 Panel surface—ink stains

Staining of panel surface caused by ink.

Causes are:

- ink spill.

Consequences are:

- permanent staining of panel surface (especially if panel surface is scratched, ink will dye laminate).

17.2.5.2.2.7 Panel surface—scratching

Marking on the panel surface caused by a variety of objects.

Causes are:

- objects moved over floor surface;
- not protecting floor when moving equipment;
- high traffic areas;
- sand.

Consequences are:

- permanent surface damage;
- poor aesthetic appearance;
- loss of static dissipative properties of surface;
- introduces contaminants into area.

17.2.5.2.2.8 Subfloor particulate—cement dust

Causes are:

- unsealed concrete subfloor;
- construction debris remaining from initial project;
- interim construction.

Consequences are:

- abrasive to panel surface;
- damage to sensitive equipment;
- continual scratching will remove design on floor panel;
- loss of static dissipative properties of surface.

17.2.5.2.2.9 Subfloor particulate—carbon

A specific type of dust usually found by the printers. It is electrically conductive and hazardous to sensitive electronic equipment. It is a flying sticky particulate that can create serious problems. All attempts should be made to eliminate excess carbon in a closed room.

Causes are:

- toner spills;
- toner used for printers.

Consequences are:

- creates abrasive film on floor surface;
- failure to computer related circuit boards;
- poor indoor air quality.

17.2.5.2.2.10 Subfloor particulate—sand

Causes are:

- brought into area by foot traffic;
- left from original construction.

Consequences:

- highly abrasive to high-pressure laminates;
- permanent surface damage;
- equipment damage;
- degrades static dissipative properties of surface.

17.2.5.2.2.11 Subfloor particulate—rust

Causes are:

- excessive moisture in area;
- deterioration of pedestals;
- high humidity;
- leak under floor;
- flooding of floor system during cleaning.

Consequences:

- component damage;
- component failure;
- unwanted rust flake particulate.

17.2.5.2.2.12 Subfloor particulate—sheetrock dust

Causes are:

- subfloor and access floor not properly cleaned after construction or renovation;
- original construction debris not cleared under floor;
- interim construction (cutting holes in walls).

Consequences are:

- damage to sensitive equipment;
- creation of high flying particulate.

17.2.5.2.2.13 Additional access floor maintenance recommendations

- develop and implement good daily/ weekly housekeeping procedures;
- use care when handling floor panels to avoid damaging panels;
- know the floor loading capacities and do not exceed them;
- depending on activities on the access floor, implement monthly, quarterly and annual floor inspections;
- depending on conditions (such as construction), implement quarterly or annual subfloor cleaning;
- refer to a guide such as *The Guide to Access Floor Maintenance* by Carol Blake for comprehensive access floor maintenance details.

17.2.6 Fire protection and suppression systems maintenance

Fire protection and suppression systems are a necessary system in a data center and are usually required by local fire codes.

NFPA 2001 Section 6 outlines inspection, maintenance, testing and training for fire suppression systems, and is probably the best guidance available for maintenance of these systems.

17.2.6.1 Recommendations

NFPA 2001 Section 6 should be adhered to as a guide for maintenance of fire suppression systems unless the local AHJ specifies otherwise.

Section 6 includes:

- 6.1 Inspection and tests;
- 6.2 Container tests;
- 6.3 Hose tests;
- 6.4 Enclosure inspection;
- 6.5 Maintenance;
- 6.6 Training;
- 6.7 Approval of installation;
- 6.8 Safety.

All fire suppression systems should only be maintained by properly trained/certified/authorized persons.

17.2.7 Security systems maintenance

Security Systems are often required by data center owners to control access into and protect assets within the data center.

Security systems can include but are not limited to:

- magnetic strip card readers (for entry control);
- motion detectors;
- CCTV with recorders;
- retina scanners;
- fingerprint readers.

Security systems can be very basic to extremely elaborate depending on local site security policy.

17.2.7.1 Recommendations

Depending on the complexity of the security system(s) in use and local security policy, maintenance will be performed by on site personnel and/or local security systems contractors.

Where fingerprint or other scanners are used to identify personnel the maintenance regime should provide for regular cleaning of the contact surfaces and anti-bacterial hand cleaner or wipes to avoid cross contamination of personnel from surface borne pathogens.

Very little preventive maintenance is necessary with most modern systems and is often performed in conjunction with remedial maintenance. Maintenance actions should be performed only by persons certified/authorized to service the installed systems.

Maintenance activities can include but are not limited to:

- camera adjustments;
- motion detector sensitivity and location adjustments;
- automatic door lock/closure adjustments;
- video recording system server updates;
- video tape rotation and storage.

All maintenance is dependent upon the type of security systems in place and due to the variety of systems available and criticality of the security systems maintenance should only be performed by the appropriate system specialists.

17.2.8 Monitoring and management systems maintenance

Monitoring and management systems are frequently used in data centers for monitoring and management of everything from environmental systems (HVAC), power generation and distribution, security systems, IT and Telecommunications systems.

Many newer systems will utilize SNMP software agents connected to the LAN to report systems status to a central server running a monitoring and management software application that collects all the details and provides a graphic display of monitored systems status to operations personnel in the central operations center.

Less sophisticated systems may have monitors, gauges, and dials that are directly connected to the device they are monitoring IE HVAC systems.

Like security systems, monitoring and management systems could be relatively simple to extremely complex and can consist of numerous individual specialized devices.

17.2.8.1 Recommendations

For SNMP based systems, it may be necessary to periodically check for agent software updates from the manufacturer that enhance functionality of the monitoring system.

Calibration of the device at manufacturers specified intervals.

Visual inspection of device at least annually.

For systems with direct connected monitoring devices such as gauges, dials, and LCD status displays. Periodic maintenance should include visual inspection of device at least annually.

Calibration of the device at manufacturers specified intervals.

Repair/replacement of failing displays as required.

The best practice is to follow the manufacturer/vendor/integrator maintenance recommendations for the system(s) installed.

Only allow maintenance activities to be performed by trained/authorized personnel.

17.3 Maintenance recordkeeping

17.3.1 Recommendations

Although maintenance recordkeeping is not mandatory, it is a valuable tool to establish maintenance histories, baselines and data trending.

Record keeping can be as simple as maintaining a paper maintenance log for each device/system under maintenance. However, a maintenance database is a much more efficient way of tracking maintenance information.

Some commercial industrial maintenance software products can be tailored for specific applications such as maintenance tracking or facilities management in the data center.

By using software to track maintenance actions, histories, baselines and data trending can be established to determine the life cycle of components/systems under maintenance. Histories, baselines and data trending can help to determine if a particular component(s) or systems are prone to premature failure. Histories, baselines, and data trending aid maintenance personnel in being proactive in maintaining failure prone systems and knowing which parts/components should be on hand and when they can anticipate needing them.

This page intentionally left blank

Annex A: Design Process (informative)

This annex is informative and not part of this standard.

A.1 Introduction

Communication and documentation are critical in the planning of space, power, and cooling requirements of data centers. Gaps commonly occur due to incomplete communication between disciplines. For example: “watts/m² or watts/ft²” specifications may not be adequate; more specific planning and communication of kW per cabinets of various types, along with the anticipated “end-state” deployment, may lead to higher level of success

A.1.1 Traditional A/E design process

The architectural/engineering (A/E) design process for traditional commercial space involves space programming that identifies the various spaces required. This task is typically performed by the architect or interior designer by interviewing the end users of each of the space and surveying the existing spaces occupied by the end user.

Once the “people” space and “people” flow have been identified, the architect or interior designer will work with the various engineering disciplines to determine the appropriate space for the supporting infrastructure (e.g., electrical and mechanical equipment spaces).

When all of the space programming has been completed, the process will then move into the design phases: planning, schematic design, design development and construction documents.

All of these design efforts are often done without input from IT. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

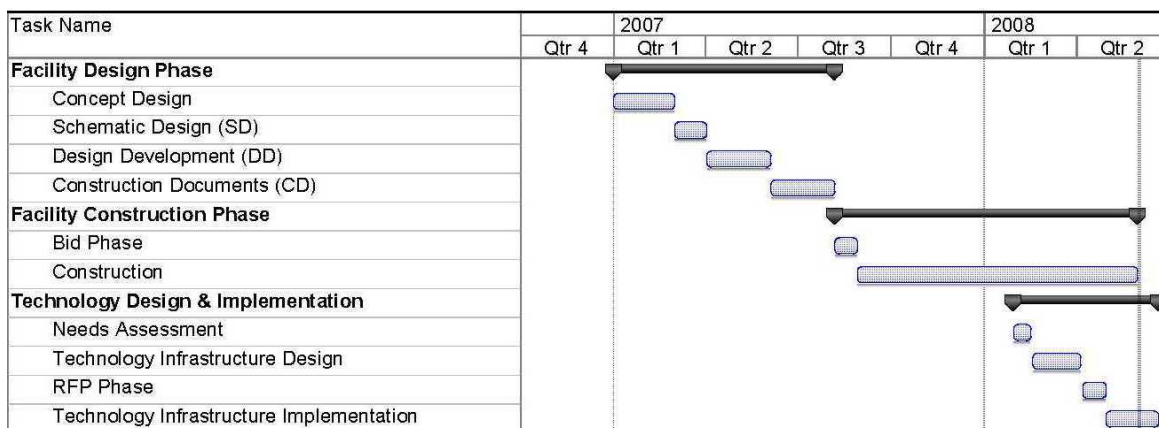


Figure A1: Traditional A/E Design Process

A.1.2 Traditional technology design process

The technology design process for traditional commercial space often starts after the physical design of the facility has been completed, often weeks afterward.

The technology process includes a needs assessment that identifies the specific technology requirements of each stakeholder.

When the needs assessment has been completed the technology design moves into the detailed design and RFP development.

Technology design efforts are sometimes done with little or no coordination with the architectural and engineering design teams. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

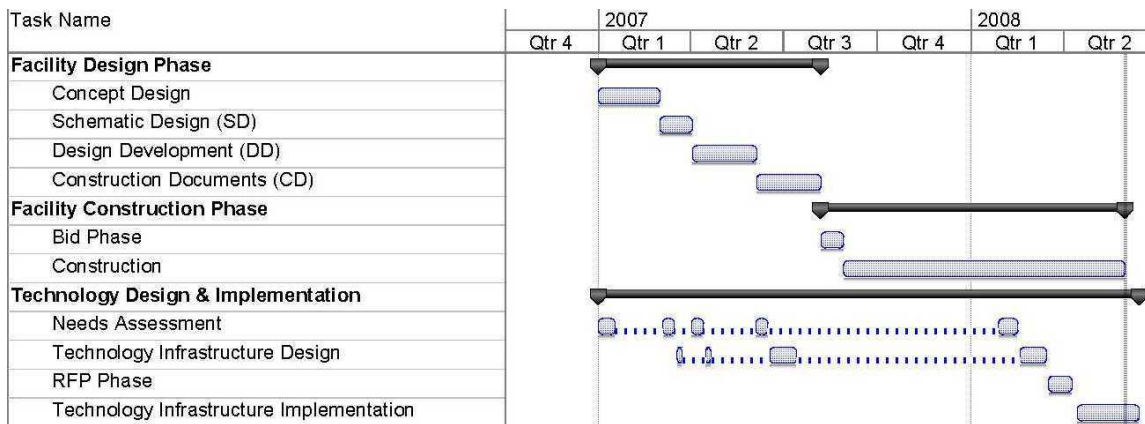


Figure A2: Data Center A/E Design Process

A.1.3 Data center design process requirements

A data center is an engineering and technologically complex facility that cannot be approached in a similar manner as traditional commercial space.

The design process must start with a thorough understanding of the technology (network, servers, connectivity) requirements and engineering requirements (power and cooling). The design process for a data center is not focused so much on the “people” space and flow but on the network and computer equipment space and flow. This drives the process to start with the engineering effort before the architectural design effort.

User or application requirements: both user and application requirements tend to drive the reliability of the data center. The design process must gather data regarding the availability requirements of the people and applications supported by the data center and design the space accordingly (see Annex B for guidance in calculating availability).

A.2 Project delivery methods

A.2.1 Design-bid-build

The design-bid-build process is a method of project delivery that separates the architectural and engineering design services from construction services.

The end user or owner may hold separate contracts for the design and construction services. The A/E design services and the construction services can both be negotiated or competitively bid in an open or selected market with the responses evaluated with respect to cost, experience, schedule and any other end user requirement.

The design-bid-build process consists of the entire facility design being completed by the architect/engineering team with the deliverables consisting of a set of constructible documents and specifications.

These construction documents (CD’s) are then issued to contractors for negotiated or competitive pricing. In a bid environment, the contractors that are allowed to bid are either:

- invited by the end user; or
- selected through a qualification process prior to the issuance of bid documents.

The bid documents, prepared based on the user’s needs and budget as previously defined, are issued to all contractors interested in bidding.

The architectural/engineering design team will usually be involved in construction administration, which includes periodic site surveys to assess the work progress and compliance with bid documents and specifications.

A.2.2 Design-build

The design-build process is a method of project delivery in which one entity, the design-builder, provides the architectural, engineering and construction services all under one contract.

The design-build process starts with a consultant developing the program for the facility to develop the general scope of the project. The general contractor is then selected through either negotiation or competitive bid to complete the design and construction services.

The single entity in the design-build process can be a general contractor, construction management firm, or consulting firm. Each project will result in varying amounts of the scope of work being performed by the single entity. It will be the single entity’s responsibility to bring together a team that has the experience to complete the project as required by the end user.

The design-build project delivery method has often been used when the schedule is a primary driver for a successful project. It is also acceptable when schedule is not an issue.

Further information can be obtained from the Design-Build Institute of America website (www.dbia.org).

A.2.3 Construction management

The construction management (CM) project delivery model can be a fee-based service or at-risk based service. The construction manager is responsible to, and under contract exclusively with, the owner. The construction manager represents the owners interest's throughout the various phases of the project.

The CM model is similar to the design-bid-build model in that there is a separation of the architectural and engineering design services from the construction services. It is also similar to the Design Build model in that the CM represents the constructor's perspective throughout the design process, but the CM is solely responsible to the owner and does not have any financial incentive by value engineering during the construction phase.

To obtain the greatest advantage of the CM delivery model, the owner should engage the CM very early in the project at the concept development design phase.

The CM delivery model provides flexibility to the owner in procuring the construction services.

- the owner can procure the construction services, managed by the CM, with a single contract where the general contractor and subtrades are all under contract through one prime contractor;
- the owner can also procure the construction services with multiple contracts where the general contractor and significant subtrades (electrical and mechanical) are under separate contracts directly with the owner; the multiple contracts with the owner would be managed by the CM.

The fee based CM model is where the CM is under contract to the owner for a fixed fee and all construction contracts are negotiated between the owner and the contractors.

The "at-risk" based CM model is where the CM commits to the owner the delivery of the construction project with a Guaranteed Maximum Price (GMP). This model is similar to the CM acting as a construction consultant to the owner during the design phase and as a prime general contractor during the construction phase.

Further information can be obtained from the Construction Management Association of America (<http://cmaanet.org>).

A.3 Facility design phases

A.3.1 Planning and concept development

The following tasks are commonly included within the planning phase:

- data center IT and telecommunications infrastructure requirements documents
- facility programming;
- space relationships/flow diagrams;
- project development scheduling;
- project budgeting;
- life cycle cost studies;
- economic feasibility studies;
- agency consulting/review/approval;
- site selection/analysis utilization;
- environmental studies as well as city/county and permit requirements;
- power requirements and availability;
- energy studies;
- existing facilities surveys;
- client-supplied data coordination;
- services related to project management;
- presentations;
- marketing studies;
- project financing;
- special studies;
- rezoning assistance;
- project promotion;
- legal survey;
- geotechnical analysis.

A.3.2 Schematic design (SD)

The following tasks are commonly included within the schematic design phase:

- client-supplied data coordination;
- program and budget evaluation;
- review of alternative design approaches;
- architectural schematic design;
- schematic design drawings and documents;
- statement of probable construction costs;
- client consultation;
- interior design concepts;
- special studies (e.g., future facilities, environmental impact);
- special submissions or promotional presentations;
- special models, perspectives, or computer presentations;
- project management;
- agency consultation;
- IT and telecommunications infrastructure conceptual design documents;
- structural design concepts;
- mechanical design concepts;
- electrical design concepts;
- civil design concepts;
- landscape concepts;
- statements of probable costs.

A.3.3 Design development (DD)

The following tasks are commonly included within the design development phase:

- client-supplied data coordination;
- design coordination;
- architectural design development;
- design development drawings and documents;
- client consultation;
- interior design development;
- special studies/reports (e.g., planning tenant or rental spaces);
- promotional presentations;
- models, perspectives or computer presentations;
- project management;
- agency consultation;
- IT and telecommunications infrastructure detailed design documents;
- structural design development;
- mechanical design development;
- electrical design development;
- civil engineering design development;
- landscape development;
- detailed construction cost estimates or quantity surveys;
- cost estimate reconciliation with budget.

Further information can be obtained from the Design-Build Institute of America website (www.dbia.org).

A.3.4 Prepurchase

- define list of long lead items;
- prepare specifications for prepurchase items;
- bid or procure items ahead of issuance of facility construction documents due to possible long lead material cost increases.

A.3.5 Construction documents (CD)

The following tasks are commonly included within the construction documents phase:

- client-supplied data coordination;
- project coordination;
- architectural construction documents (working drawings, form of construction contract and specifications);
- document checking and coordination;
- client consultation;
- interior construction documents;
- alternative bid details and special bid documents;
- project management;
- agency consultation;
- low-voltage/telecommunications cabling system bid documents;
- structural construction documents;
- mechanical construction documents;
- electrical construction documents;
- statements of probable costs;
- civil engineering construction documents;
- landscape documents;
- detailed construction cost estimates or quantity surveys;
- cost estimate reconciliation with budget.

A.4 Technology design phases

A.4.1 Needs assessment

The following tasks are commonly included within the needs assessment phase:

- develop a project plan that will outline the tasks, timeframes and responsibilities for completing the technology project;
- conduct information gathering sessions identifying and documenting the technology and business needs;
- review the existing technology systems;
- interview IT and facilities personnel and determine the group(s) that will be responsible for each portion of the data center infrastructure when the project is complete;
- review anticipated growth and new technologies;
- review timeframes, capital and operational budgets;
- develop data center IT/Telecommunications infrastructure requirements document;
- develop a business case for recommendations made during needs assessment analysis.

A.4.2 Design analysis

The following tasks are included within the design analysis phase:

- review, evaluate and prioritize all of the information received and documented during the needs assessments phase;
- validate vendor qualification criteria, technology applications, required infrastructure, industry standards and best practices, budgets and other pertinent information with project stakeholders;
- develop conceptual design for data center IT and telecommunications infrastructure.

A.4.3 Acquisition

The following tasks are included within the acquisition phase:

- develop detailed IT and telecommunications infrastructure design;
- draft the RFP for the technology vendor services, including detailed specifications and drawings; the RFP should also include the project organization, expected milestone schedule, current construction schedule, and responsibility matrix;
- analyze and evaluate all bid responses for accuracy and completeness, and financial, technical and service qualifications;
- assist in the selection process and final contract review and negotiations.

A.4.4 Implementation

The following tasks are included within the Implementation phase:

- provide project management services to facilitate the implementation of the technology vendor's service contract;
- facilitate regularly scheduled status meetings to review procedures and processes, maintenance records and documentation submitted by vendor to ensure that end user is receiving the service and support as outlined in the service contract;
- assist end user in measuring and benchmarking services provided by the technology vendor.

A.5 Commissioning

The following tasks are included within the commissioning phase:

- request design intent document from A/E of record that is reflective of original basis of design identified in concept documents;
- request sequence of operation for electrical and mechanical components;
- validate alignment between sequence of operations and controls methodology; review SCADA and building automation system topology and sensor locations;
- prepare system readiness checklists to be signed off by contractors prior to startup of individual components;
- prepare verification test procedures for each component in each system and record anomalies encountered;
- conclude commissioning testing with integrated system test for normal, failure, and maintenance modes; apply simulated loads such as server simulator load banks to fully test the entire data center load carrying components;
- conclude commissioning phase with a lessons learned report that serves to benchmark the operation of electrical and mechanical systems; the corrective action report would also be prepared during this phase.

A.6 Data center documentation

A.6.1 Recommendations

Data center documentation should include:

- construction and implementation:
 - contract documents:
 - request for bid/quote;
 - project schedule;
 - specifications;
 - floor plan drawings;
 - outside plant drawings;
 - connectivity riser diagrams;
 - equipment layout drawing and details;
 - rack and cabinet elevations;
 - cable pathway details;
 - construction change orders
 - as-built drawings;
 - construction administration reports;
 - test reports;
 - punch-list reports;
 - operations and maintenance (O&M) manuals;
 - close-out, sign-off and acceptance certificates;
 - certificate of occupancy.
- ongoing change management documentation, including system inventories and configuration databases—these may also be used as a starting point for relocation planning documentation.
- relocation planning documentation such as equipment, system, and application inventories, including system and application dependencies.

Annex B: Reliability and Availability (informative)

This annex is informative and not part of this standard.

B.1 Introduction

This section is intended to provide a framework for understanding the process for determining criticality and aligning project objectives and budgets with appropriate performance levels.

People have come to expect ready access to information 24 hours a day, every day. The Internet as well as more traditional enterprises—both business and governmental—now operate 7 days a week, 24 hours a day. Typical 24/7 operations include banking systems, credit card companies, 911 emergency centers, telecommunications networks, hospital systems, overnight delivery operations, large multinational concerns, and other international organizations.

The burgeoning demand for mission-critical/data processing facilities (essentially server warehouses) requires fresh thinking given the radical differences in conventional building types. Consider some mission-critical facility norms:

- The power supplied to a typical office building is about 110 W/m² (10 W/ft²), but between 650 W/m² (60 W/ft²) and 2200 W/m² (200 W/ft²) or more in a mission-critical facility. Mission-critical power requirements far exceed any conventional building type.
- The mechanical/electrical/service space ratio to usable space averages 1:3 or 1:4 in typical buildings and is close to 1:1 in data centers.
- The cost of mission-critical facilities can run up to four times the cost of more traditional building types. Power and cooling requirements drive cost and design.

These numbers are revealing. Mission-critical power and cooling systems evolved from a philosophy dubbed "system + system", meaning that, for every critical electrical and HVAC system, a duplicate system is in place to provide service while the other is repaired, maintained, or tested off-line. Additionally, the risk of natural and provoked disasters and possible IT downtime dictates a hardened building shell as well as sufficient power and electrical capacity on site.

Continuous operation implies that building systems need a measured approach to incorporating reliability, with redundant building systems the usual tactic. After all, shutdown can cripple the revenue generating continuity of a business, ruin customer confidence, and possibly threaten its existence if extensive. Disruption to the IT systems underpinning today's industrialized societies may cause loss of life and endanger communities, depending upon the nature and location of the service.

Mission-critical facilities requiring 7 day at 24 hours/day operations need a comprehensive strategy to sustain their vital activities. Many small businesses have at least a 5 day at 12 hour/day high-availability operating requirement—less rigorous standards, yet still substantial. Mission-critical design variations will stem from each facility's requirements. Starting with site selection criteria and working forward through each layer of architectural, engineering and operational design, downtime risk reduction and reliability must be the prime focus, weighed and coordinated throughout the process.

Mission-critical facilities have not traditionally been high-profile projects, yet their design issues are increasingly complex and critical. With an emerging design terminology and vocabulary, their rapid evolution calls for an exceptional degree of building system coordination and integration. The facilities are not merely warehouses for servers, but instead rival operating or "clean rooms" with their precise environmental controls and power requirements. Intense, sustained work shifts with employees monitoring computer screens mean that workplace design issues must also be addressed.

Important design considerations also extend well beyond the context of the mission-critical facility itself. Electric deregulation is causing uncertainty. Increasing power demands challenge reliability of the power supply itself. Some utilities even question their capacity to power mission-critical facilities. Because IT plants are highly sensitive to temperature and power fluctuations, these concerns are attracting increased attention. It is not an issue addressed simply through the purchase of UPS systems.

B.2 Additional information

B.2.1 Goals and objectives

There is a process for designing new and upgrading existing mission-critical IT facilities. To achieve maximum benefit, defining the required performance levels of availability and reliability and then designing, procuring, and maintaining mission-critical IT facilities can and should be formalized. Lack of a formal process yields higher construction and operational costs as well as inconsistent and unpredictable performance.

An objective of this standard is to present an industry-wide process for planning mission-critical IT facilities, with the following strategic goals:

- Establish a consistent, cost-effective process.
- Develop optimum design and implementation solutions.
- Reduce the need to educate vendors and professional service providers.
- Develop a common enterprise-wide design vocabulary.
- Establish performance criteria used to generate or evaluate mission-critical facilities.

B.2.2 Creating mission-critical facilities

There are four steps in the process of designing a new mission-critical IT facility or upgrading an existing one. These are represented in Figure B1 and described afterward.

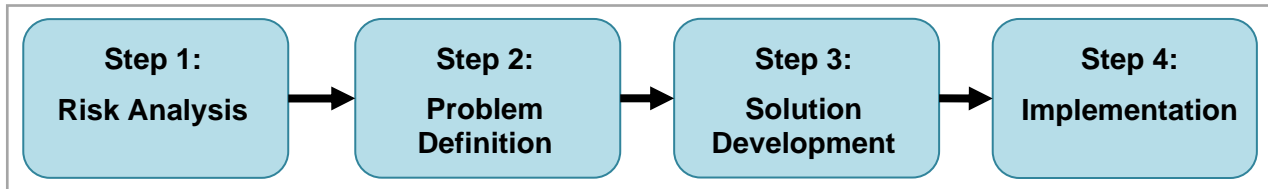


Figure B1: Planning Process For A Mission-Critical Facility

- Step 1: Risk analysis: As explained in the remainder of this section, risk analysis is a linear process. Three key characteristics are defined to arrive at an expression of the criticality of a mission-critical facility:
 - identify operational requirements—the opportunity to suspend operations for scheduled maintenance;
 - identify availability requirements—the targeted uptime of the system during operations, and the ability to endure unplanned interruption of operations;
 - define the impact of downtime—the consequences of unplanned disruptions on the mission.

The process of analyzing and mitigating risk is described in the next section. The other parts of this section form an important reference source during the remaining three process phases in creating a mission-critical facility.

- Step 2: Problem definition—After completing the risk analysis process, characterize the facility in terms of space, IT asset density (which has several components, including density of computing, data communications, and telephony), and anticipated availability requirements. The resulting information is usually documented in the facility program.
- Step 3: Solution development—Translate the facility program into one or more design solutions to solve the specific design problem and meet the objectives of the targeted availability Class.
- Step 4: Implementation—Construct the chosen solution, incorporating implementation tactics consistent with the targeted availability Class. This will include appropriate maintenance and operations procedures to ensure a sustainable level of availability.

B.2.3 Risk analysis

B.2.3.1 Introduction

It is impossible to eliminate the risk of downtime, but risk reduction is an important planning element. In an increasingly competitive world, it is critical to address downtime in business decisions. The design of systems supporting critical IT functions depends on the interaction between the criticality of the function and its operational profile.

Criticality is defined as the relative importance of a function or process as measured by the consequences of its failure or inability to function. The operational profile expresses the time intervals over which the function or process must operate. The following process is designed to integrate these and define the appropriate risk management strategy.

To provide optimal design solutions for a mission-critical facility, consider several key factors. NFPA 75 identifies six considerations for protection of the environment, equipment, function, programming, records and supplies in a data center. These include:

- 1) What are the life safety aspects of the function? For example, if the system failed unexpectedly, would lives be put at risk? Examples of such applications include some process controls, air traffic control, and emergency call centers.
- 2) What is the threat to occupants or exposed property from natural, man-made, or technology-caused catastrophic events? For example, is the building equipped with fire suppression? ...in a flood zone? ...seismically structured? ... in a tornado or hurricane corridor? ...etc.
- 3) What would be the economic loss to the organization from the loss of function or loss of records?
- 4) What would be the economic loss from damaged or destroyed equipment?
- 5) What would be the regulatory or contractual impact, if any? For example, if unplanned downtime resulted in loss of telephone service or electrical service to the community, would there be penalties from the government?
- 6) What would be the impact of disrupted service to the organization's reputation? For example, would subscribers switch to a competitors' service?

First, identify facility operational requirements. Next, assess the downtime risk to determine the impact of downtime. Finally, combine this information to arrive at a concise statement of criticality and the appropriate risk management strategy as expressed in the facility Availability Class. Paying careful attention to these factors determines an appropriate Availability Class that matches the mission-critical facility cost with the functions it is intended to support.

Figure B2 shows the overall flow of the risk management process; each step is explained afterward.

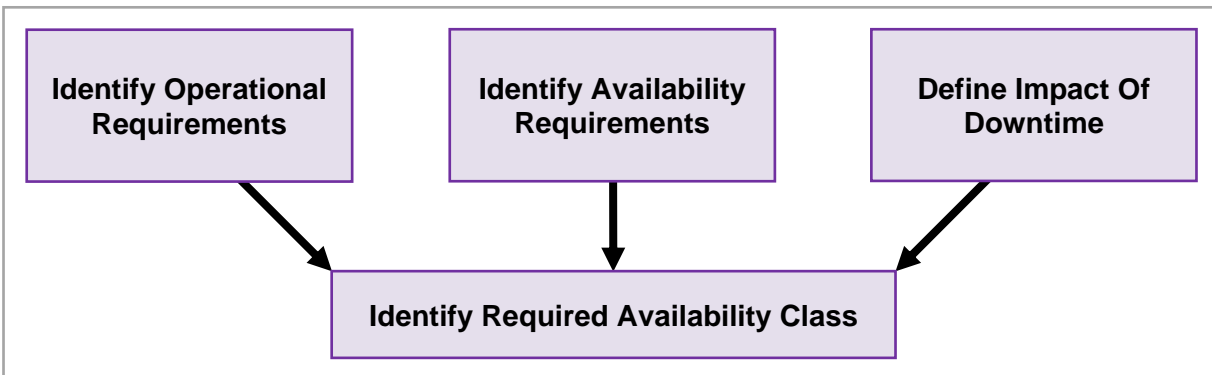


Figure B2: Risk Analysis Process

B.2.3.2 Identify operational requirements

The first step in defining the risk level associated with a mission-critical IT facility is to define the facility's intended operational requirements. Sufficient resources must be available to achieve an acceptable level of quality over a given time period. IT functions that have a high-quality expectation over a longer time period are by definition more critical than those requiring less resources, lower quality, and/or are needed over a shorter time period. The key element to consider here is time, which is quantified as "windows of opportunity" for testing and maintenance. Thus, to define the operational requirements for a critical IT facility, assign one of five facility operational levels, as defined in Table B1.

Note that the term "shutdown" means that operation has ceased; the equipment is not able to perform its mission during that time. Shutdown does *not* refer to the loss of system components if they do not disrupt the ability of the system to continue its mission.

Table B1: Defining Mission-Critical Risk Level Step 1 – Identify Operational Requirements: Time Available For Planned Maintenance Shutdown

<i>Operational level</i>	<i>Annual allowable planned maintenance hours</i>	<i>Description</i>
0	> 400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance “down” time is available during working hours and off hours.
1	100-400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance “down” time is available during working hours and off-hours.
2	50-99	Functions are operational up to 24 hours a day, up to 7 days a week, and up to 50 weeks per year – scheduled maintenance “down” time is available during working hours and off hours.
3	0-49	Functions are operational 24 hours a day, 7 days a week for 50 weeks or more . No scheduled maintenance “down” time is available during working hours.
4	0	Functions are operational 24 hours a day, 7 days a week for 52 weeks each year. No scheduled maintenance “down” time is available.

B.2.3.3 Determine availability requirements

The second step in the risk management process is to identify the facility’s operational availability requirements; i.e., the total uptime that the facility must support without disruption. Operational availability refers only to scheduled uptime—that is, the time during which the IT functions are actually expected to run.

The objective is to identify the intersection between the intended maximum annual downtime and the intended operational level. A function or process that has a high availability requirement with a low operational profile has less risk associated with it than a similar function with a higher operational profile. We use this step to adjust the overall availability to reflect the true functional requirement. This step will result in one of five Availability Rankings to be used in Step 3.

Availability is sometimes expressed as a percentage, or “nines of availability.” Thus, “five nines of availability” means that the system is full operable 99.999% of the time throughout a year. Table B2 shows what that means in terms of actual minutes of downtime. A general rule of thumb is that the cost of an installation increases by at least fifty percent for every incremental “nine” that is added. The cost of downtime must be weighed against the cost of uptime.

Table B2: Defining Mission-Critical Risk Level Step 2 – Identify Operational Levels: Tolerance For Unscheduled Shutdown

<i>Allowable maximum annual downtime (minutes)</i>	<i>Targeted uptime (percent)</i>
>5000	< 99.0
500 – 5000	99 to 99.9
50 – 500	99.9 to 99.99
5 – 50	99.99 to 99.999
0.5 – 5.0	99.999 to 99.9999

B.2.3.4 Determine impact of downtime

The third step in the risk management process is to identify the impact or consequences of downtime. This is an essential component of risk management because not all downtime has the same impact on mission critical facilities. Identifying the impact of downtime on mission-critical functions helps determine the tactics that we to deploy to mitigate downtime risk. As shown in Table B3, there are five impact classifications, each associated with a specific impact scope.

Table B3: Defining Mission-Critical Risk Level Step 3 – Classify The Impact Of Downtime On The Mission

<i>Classification</i>	<i>Description – impact of downtime</i>
Enterprise-wide	Affecting the quality of service delivery across the entire enterprise, or resulting in a significant disruption or delay in achieving key organizational objectives.
Multiregional	Multiregional in scope, affecting a major portion of the enterprise (although not in its entirety) or resulting in a major disruption or delay in achieving key organizational objectives.
Regional	Regional in scope, affecting a portion of the enterprise (although not in its entirety) or resulting in a moderate disruption or delay in achieving key organizational objectives.
Local	Local in scope, affecting only a single site, or resulting in a minor disruption or delay in achieving key organizational objectives.
Sub-local	Local in scope, affecting only a single function or operation, resulting in a minor disruption or delay in achieving non-critical organizational objectives.

B.2.3.5 Identify the data center facility availability class

The final step in the process defined in this section is to combine the three previously identified factors to arrive at a usable expression of availability. This expression of availability is used as a guide to determine the architectural and engineering features needed to appropriately support critical IT functions. Since operational level is subsumed within the availability ranking (as explained previously in this subsection), the task at hand is to matrix the availability ranking against the impact of downtime and arrive at an appropriate Availability Class. Table B4 shows how this is done:

Table B4: Determining Facility Availability Class

<i>Impact of Downtime (From Table B3)</i>	<i>Operational Level (From Table B1)</i>				
	<i>0</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Enterprise-wide	Class F1	Class F2	Class F3	Class F4	Class F4
Multiregional	Class F1	Class F2	Class F3	Class F3	Class F4
Regional	Class F1	Class F2	Class F2	Class F3	Class F3
Local	Class F0	Class F1	Class F2	Class F3	Class F3
Sub-local	Class F0	Class F0	Class F1	Class F2	Class F2

B.2.4 Reliability aspects of availability planning

Achieving an optimum Class of availability for a mission-critical facility requires strategic planning to determine the risks, design features and potential improvement measures that will lead to fewer facility related failures.

B.2.4.1 Reliability engineering principles and calculating reliability

Reliability is simply the probability that a given system will perform as intended over a given time period. It is expressed as a percentage – the *probability* that a system will fail at some point. (Compare this to *availability*, which is essentially the amount of time [expressed either as hours per year or as percentage of hours per year] that a system can continue its mission, despite system or subsystem failures). Over the last 30 years, data has been collected and analyzed for a wide variety of mechanical and electrical components and their failure characteristics. This has led to broad-based industry standards for the analysis and design of reliable power and cooling systems (e.g., IEEE Standard 493-2007 (Gold Book)—*IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*).

The reliability of a given system can be calculated from the published MTBF (mean time between failures) data for given components of that system. This calculation can then be combined to yield an overall expression of system reliability through the analysis of all series and parallel subsystems. The calculations are as follows:

$$R = e^{(-\lambda T)} \quad (B1)$$

where:

R = reliability (percent probability of success)

e = exponential function

λ = failure rate (the reciprocal of MTBF)

T = time period (same units as failure rate)

Example: A UPS module has a published MTBF of 17,520 hours (one failure every two years). Its failure rate would then be 0.00005708 failures per hour. What is its one-year reliability, or the probability of not failing in one year (8,760 hours)?

$$R = e^{(-0.00005708 \times 8,760)}$$

$$R = 0.6065 \text{ or } 60.65\%$$

To obtain the reliability of a given system, the individual reliability of each component must be calculated, then the reliability of parallel subsystems, and then the series reliability of all subsystems, as follows and as illustrated in Figure B3.

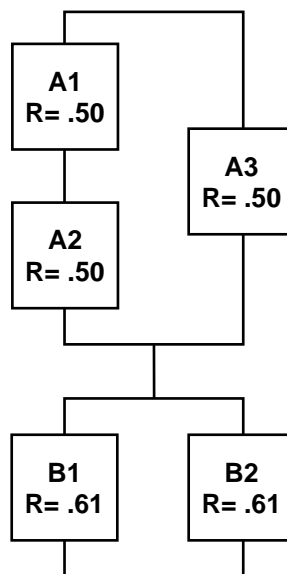


Figure B3: Sample reliability calculation

The reliability of a series system is equal to the product of all component reliabilities. The reliability of a parallel system is equal to the complement of the product of all component complements. Thus, the reliability for the system in Figure B3 would be calculated as follows:

$$R_{A1A2} = R_{A1} \times R_{A2} = 0.5 \times 0.5 = 0.25$$

$$R_A = 1 - [(1 - R_{A1A2}) \times (1 - R_{A3})] = 1 - [(1 - 0.25) \times (1 - 0.5)] = 0.625$$

$$R_B = 1 - [(1 - R_{B1}) \times (1 - R_{B2})] = 1 - [(1 - 0.61) \times (1 - 0.61)] = 0.848$$

$$R_{TOTAL} = R_A \times R_B = 0.625 \times 0.848 = 0.53 \text{ (53\%)}$$

B.2.4.2 Trends affecting reliability of critical IT facilities

As more and more clients require service level guarantees, service providers and facility managers must determine what facility performance is required to provide the agreed-to or sufficient end user availability (see Table B2). Availability levels of 99.99% (50 minutes of downtime per year) allow practically no facility downtime for maintenance or other planned or unplanned events. Therefore, migrating to high-reliability facilities is imperative.

As computers have become more reliable, the overall percentage of downtime events caused by facility failures has grown. Although the occurrence of such facility outages remains small, the total availability is dramatically affected because repair times for facility outages are lengthy.

B.2.4.3 Financial models

Over the last 30 years, the cost of facilities has not grown proportionately with the increasing cost of the computer hardware housed within those facilities. This has created a situation where favoring hardware over facility improvements in budget priorities has led to inadequate end-to-end performance.

The most appropriate way to ensure a balanced deployment of available capital funds is to prepare a business case that includes the costs associated with downtime risk. This cost is a function of both the consequences of an unplanned service outage and the probability that an outage will occur. For example, the costs associated with the different Classes of availability can be calculated as shown in Table B5 if the following hypothetical assumptions are used:

- The cost to the business for an outage is \$1 million per hour.
- The cost to build a data center with a design reliability target of 99% is \$200/ft².
- The cost to build a data center with a design reliability target of 99.9% is \$300/ft².
- The cost to build a data center with a design reliability target of 99.99% is \$400/ft².

Table B5: Sample Cost And Benefit Of Varying Degrees Of Reliability

<i>Design reliability</i>	<i>Cost/ft² size</i>	<i>Total first costs</i>	<i>Annual downtime</i>	<i>Cost of downtime</i>	<i>ROI</i>
99%	\$200/ft ² 50,000 ft ²	\$10 million	5000 min.	\$87.6 million	NA
99.9%	\$300/ft ² 50,000 ft ²	\$15 million	500 min.	\$8.76 million	1,576%
99.99%	\$400/ft ² 50,000 ft ²	\$20 million	50 min.	\$876,000	867%

As shown in the previous table, substantial cost reductions can be achieved by avoiding facility failure through investment in reliability improvements. In addition, by selecting the optimum availability Class, the investment return can be maximized.

B.2.4.4 Planning process

A proactive, strategic planning approach to mission-critical facility design and management requires a five-step process:

- 1) analyze your current facility;
- 2) identify and prioritize risks and vulnerabilities;
- 3) provide solutions to minimize risks;
- 4) develop an implementation strategy;
- 5) measure performance and verify improvement.

This should be done continuously, typically in an annual cycle. In this process, plans can be refined and modified as objectives are met or new technology is deployed.

B.2.4.5 Defining Data Center Facility Availability Class

Identifying the Availability Class for a facility is the final step in risk management, the first of these four phases. The latter three phases are Problem Definition, Solution Development and Implementation.

To a great degree, design decisions are guided by the identified Availability Class. Thus, it is essential to fully understand the meaning of each Availability Class. Each Availability Class is defined in terms of four areas of concern:

- 1) Component redundancy increases reliability by providing redundancy for critical high-risk, low-reliability components within systems.
- 2) System redundancy increases reliability even more by providing redundancy at the system level.
- 3) Quality ensures that high quality is designed and implemented in the facility, thus reducing the risk of downtime due to failure during initial installation and/or premature wear. Since MTBF is a major factor in the determination of system reliability, it stands to reason that higher quality components with lower failure rates will result in systems that are more reliable.
- 4) Survivability refers to reducing the risk of downtime by protecting against external events such as physical forces, security breaches, and natural disasters.

The following subsections provide more detail on how each of these four factors is defined for each of the five Availability Classes. Each Class is also illustrated by the application of the appropriate tactics to the critical power distribution system (see Section 9).

B.2.4.6 Availability Class F0

The objective of Class F0 is to support the basic environmental and energy requirements of the IT functions without supplementary equipment. Capital cost avoidance is the major driver. There is a high risk of downtime due to planned and unplanned events. However, in F0 facilities maintenance can be performed during non-scheduled hours, and downtime of several hours or even days has minimum impact on the mission.

B.2.4.6.1 Tactics for Class F0

Component redundancy:	none
System redundancy:	none
Quality control:	standard commercial quality
Survivability:	none

Application: A critical power distribution system separate from the general use power systems would not exist. There would be no back-up generator system. The system might deploy power conditioning or surge protective devices to allow the specific equipment to function adequately (utility grade power does not meet the basic requirements of critical equipment). No redundancy of any kind would be used for power or air conditioning for a similar reason.

B.2.4.6.2 Typical facility performance characteristics for Class F0

Annual maintenance windows:	> 400 hours
Targeted availability:	<99.0%
Scope of impact:	local data center

B.2.4.7 Availability Class F1

The objective of Class F1 is to support the basic environmental and energy requirements of the IT functions. There is a high risk of downtime due to planned and unplanned events. However, in Class F1 facilities, maintenance can be performed during nonscheduled hours, and the impact of downtime is relatively low.

B.2.4.7.1 Tactics for Class F1

Component redundancy:	none
System redundancy:	none
Quality control:	standard commercial quality
Survivability:	none

Application: The critical power distribution system would deploy a power conditioning device to allow the critical equipment to function adequately (utility grade power does not meet the basic requirements of critical equipment). No redundancy of any kind would be used for power or air conditioning for a similar reason.

B.2.4.7.2 Typical facility performance characteristics for Class F1

Annual maintenance windows:	100-400 hours
Targeted availability:	99.0%
Scope of impact:	local or regional data centers

B.2.4.8 Availability Class F2

The objective of Class 2 is to provide a level of reliability higher than that defined in Class 1 to reduce the risk of downtime due to component failure. In Class 2 facilities, there is a moderate risk of downtime due to planned and unplanned events. Maintenance activities can typically be performed during unscheduled hours.

B.2.4.8.1 Tactics for Class F2

Component redundancy:	redundancy is provided for critical components
System redundancy:	none
Quality control:	premium quality for critical components
Survivability:	moderate hardening for physical security and structural integrity

Application: In this Class, the critical power system would need redundancy in those parts of the electrical distribution system that are most likely to fail. These would include any products that have a high parts count or moving parts, such as UPS, controls, air conditioning, generators or ATS. In addition, it may be appropriate to specify premium quality devices that provide longer life or better reliability.

B.2.4.8.2 Typical facility performance characteristics for Class F2

Annual maintenance windows:	50 to 99 hours
Targeted availability:	99.9%
Scope of impact:	local, regional, or multiregional data centers

B.2.4.9 Availability Class F3

The objective of Class F3 is to provide additional reliability and maintainability to reduce the risk of downtime due to natural disasters, human-driven disasters, planned maintenance, and repair activities. Maintenance and repair activities will typically need to be performed during full production time with no opportunity for curtailed operations.

B.2.4.9.1 Tactics for Availability Class F3

Component redundancy:	redundancy is provided for critical and noncritical components; also provided to increase maintainability; not provided where the component is part of a redundant system
System redundancy:	redundancy may be provided without component redundancy
Quality control:	premium quality for all components
Survivability:	significant hardening for physical security and structural integrity

Application: The critical power system in a Class 3 facility must provide for reliable, continuous power even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, the power system must be able to sustain operations while a dependent component or subsystem is out of service.

B.2.4.9.2 Typical facility performance characteristics for Class F3

Annual maintenance windows:	0 to 49 hours
Targeted availability:	99.99%
Scope of impact:	all data centers, even some local data centers with high availability requirements and low maintenance windows, may need to be Class F3

B.2.4.10 Availability Class F4

The objective of Class F4 is to eliminate downtime through the application of all tactics to provide continuous operation regardless of planned or unplanned activities. All recognizable single points of failure from the points of connection at the utility to the points of connection at the critical loads are eliminated. Systems are typically automated to reduce the chances for human error and are staffed 24x7. Rigorous training is provided for the staff to handle any contingency. Compartmentalization and fault tolerance are prime requirements for a Class F4 facility.

B.2.4.10.1 Tactics for Availability Class F4

Component redundancy:	redundancy is provided for all critical components and to increase maintainability; also provided for noncritical components
System redundancy:	system redundancy is provided with component redundancy so that overall reliability is maintained even during maintenance activities
Quality control:	quality for all components
Survivability:	all building systems are self-supporting in any event and are protected against the highest levels of natural forces

Application: The critical power system in a Class F4 facility must provide for reliable, continuous power even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, the power system must be able to sustain operations while a dependent component or subsystem is out of service.

B.2.4.10.2 Typical facility performance characteristics for Class F4

Annual maintenance windows:	0 hours
Targeted availability:	99.999%
Scope of impact:	multiregional or enterprise wide data centers

B.2.5 Reliability planning worksheet

Use the following planning guide starting on the next page to determine the critical IT facility requirements.

B.2.6 Other factors

The process by which mission-critical Availability Classes are defined is not a perfect science. As projects are built, there will be unexpected outcomes and learned lessons. The following are just a few factors that may alter the selected Availability Class. Other factors will be added over time.

B.2.6.1 Intangible consequences of downtime

On occasion, a new product rollout, technical initiative, or other major endeavor will be announced. With heightened press exposure or internal performance pressures, there will be an incalculable and unpredictable cost of unplanned downtime. Avoiding these types of circumstances may dictate a higher Availability Class than is otherwise indicated.

B.2.6.2 Scheduled deployment

If a critical IT function must be deployed quickly, it may dictate different risk management strategies, outside that normally considered.

B.2.6.3 Unusual budget constraints

If the established budget for a critical IT facility will not support the required Availability Class, then a less reliable facility will need to be built unless additional funding is provided.

Project name: _____

Project number: _____

Project description: _____

Project location: _____

STEP 1: Determine operational requirements

- 1) Does this IT function support a production operation? Yes ___ No ___
If yes, proceed to the next line; otherwise your Availability Class can be F0 or F1
Note: Production Operation is considered to be any IT operation, the loss of which would negatively impact achievement of the organization's mission
- 2) How many hours of operation must be supported during a production week? _____
- 3) How many scheduled production weeks are there? _____
- 4) Multiply line 2 by line 3 and enter here. This is annual production hours: _____
- 5) Subtract line 4 from 8,760 and enter the result (allowable annual maintenance hours) here: _____
- 6) If line 5 is greater than 400, the Operational Level is 0; otherwise proceed to the next line.
- 7) If line 2 is less than 168, and line 5 is greater 100, the Operational Level is 1; otherwise proceed to the next line.
- 8) If line 5 is between 50 and 99, the Operational Level is 2; otherwise proceed to the next line.
- 9) If line 5 is between 1 and 49, the Operational Level is 3; otherwise, the Operational Level is 4.

STEP 2: Define Mission-critical Risk Level (see Table B3)

Downtime will reduce or negatively impact operations (select one):

- Enterprise-wide (across the entire enterprise) _____
- Multi-regional (across a wide area of the entire enterprise) _____
- Regional (across a single region) _____
- Local (at a single site) _____
- Sub-local (a single non-critical function) _____

STEP 3: Determine from the table below

- 1) Select the column from the Operational Level in Step 1
- 2) Select the row from the Risk Level in Step 2
- 3) Your Facility Availability Class is where the two intersect _____

Facility Availability Class

Impact of Downtime	Operational Level				
	0	1	2	3	4
Enterprise-wide	Class F1	Class F2	Class F3	Class F4	Class F4
Multiregional	Class F1	Class F2	Class F3	Class F3	Class F4
Regional	Class F1	Class F2	Class F2	Class F3	Class F3
Local	Class F0	Class F1	Class F2	Class F3	Class F3
Sub-local	Class F0	Class F0	Class F1	Class F2	Class F2

B.2.7 Other reliability alternatives

While systems in a Class F3 data center may only expect to stay up as long as the facilities stay up, that is for 99.99% of the time (see B.2.4.9), designs with clustered systems having nodes spread across multiple Class F3 data centers can provide better uptime (see the math in B.2.4.1 and Figure B3), potentially matching or exceeding the uptime of a single Class F4 data center.

In such a design the first failover is to the local node (synchronous), the second failover is to a nearby data center (~16 km [10 miles], and still synchronous) and the third is to a remote data center (but asynchronous).

Such a design does increase the facilities overhead and therefore the cost. However, it offers a way for designers to avoid many of the costs associated with Class F4 data centers, whether owned, leased or collocated.

Annex C: Referenced Documents (informative)

This annex is informative only and is not part of this standard.

The following standards and documents are related to or have been referenced within the text of this standard and provide additional information, which may be of use to the reader.

American Society for Testing and Materials (ASTM International)

- ASTM B539-02(2008), *Measuring Contact Resistance of Electrical Connections (Static Contacts)*;
- ASTM E136-09, *Test Method for Behavior of Materials in a Vertical Tube Furnace at 750 Degrees C* (2009);
- ASTM E814-09, *Methods of Fire Tests of Through-penetration Fire Stop*
- ASTM F1233-08, *Standard Test Method for Security Glazing Materials And Systems*

American Society of Heating, Refrigerating, and Air-Conditioning Engineer (ASHRAE)

- 2008 *ASHRAE Environmental Guidelines for Datacom Equipment—Expanding the Recommended Environmental Envelope*
- ASHRAE 52.2-2007, *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*;
- ANSI/ASHRAE/IESNA 90.1-2007, *Energy Standard for Buildings Except Low-Rise Residential Buildings*;
- *ASHRAE Handbook – Fundamentals* (2009)
- *ASHRAE Handbook – HVAC Applications* (2007)
- *ASHRAE Handbook – HVAC Systems and Equipment* (2008)
- Herrlin, M. K. 2005. *Rack Cooling Effectiveness in Data Centers and Telecommunications Central Offices: The Rack Cooling Index (RCI)*. ASHRAE Transactions, Volume 111, Part 2
- Herrlin, M. K. and Belady, C. 2006. *Gravity-Assisted Air Mixing in Data Centers and How it Affects the Rack Cooling Effectiveness*. ITherm 2006, San Diego, CA, May 30–June 2, 2006

Builders Hardware Manufacturers Association (BHMA)

- ANSI/BHMA A156.13-2002, *American National Standard for Mortise Locks and Latches Series 1000*

Building Services Research and Information Association (BSRIA)

- BG 5/2003, *Cooling solutions for IT - A guide to planning, design and operation*

Factory Mutual

- *FM Global Property Loss Prevention Data Sheets 1-28*;

Illuminating Engineering Society (IES)

- *IESNA Lighting Handbook*;
- ANSI/IESNA RP-1-04 *American National Standard Practice for Office Lighting*

Institute of Electrical and Electronics Engineers (IEEE)

- ANSI/IEEE C2-2007, *National Electrical Safety Code (NESC)*;
- IEEE C62.72-2007, *IEEE Guide for the Application of Surge-Protective Devices for Low-Voltage (1000 V or Less) AC Power Circuits*;
- IEEE 446-1995 (Revision 2000) (The IEEE Orange Book), *Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*;
- IEEE 485-1997, *IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stationary Applications*;
- IEEE 902-1998 (The IEEE Yellow Book), *Guide for Maintenance, Operation and Safety of Industrial and Commercial Power Systems*;
- IEEE 1013-2007, *IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stand-Alone Photovoltaic (PV) Systems*;
- IEEE 1145-1999, *IEEE Recommended Practice for Installation and Maintenance of Nickel-Cadmium Batteries for Photovoltaic (PV) Systems* (withdrawn standard);
- IEEE 1375-1998, *IEEE Guide for the Protection of Stationary Batteries*;
- IEEE/ASHRAE 1635/200, *Guide for the Ventilation and Thermal Management of Stationary Battery Installations* (under development)

Insulated Cable Engineers Association

- ICEA S-83-596-2001, *Optical Fiber Premises Distribution Cable*;
- ICEA S-87-640-2006, *Standard for Optical Fiber Outside Plant Communications Cable*;
- ICEA S-104-696-2001, *Standard for Indoor-Outdoor Optical Fiber Cable*;
- ICEA S-110-717-2003, *Optical Drop Cables*;

International Electrotechnical Commission (IEC)

- IEC 60603-7, *Connectors for electronic equipment (multiple document series)*;
- IEC 61300-3-6:2008, *Basic Fibre Optic Test Procedures – Part 3: Examination and measurement—Section 6: Return loss*;
- IEC 61300-3-34:2009, *Basic Fibre Optic Test Procedures – Part 3: Examination and measurement—Section 34: Attenuation of random mated connectors*;
- IEC 61754-20:2002, *Fibre Optic Connector Interfaces – Part 20: Type LC Connector Family*;

International Organization for Standardization (ISO)

- ISO/IEC TR 29106:2007, *Information technology – Generic cabling – Introduction to the MICE environmental classification*

Laser Institute of America (ASC Z136)

- ANSI Z136.2, *American National Standard for Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources* (1997)

National Electrical Contractors Association (NECA)

- ANSI/NECA/BICSI 568-2006, *Standard for Installing Commercial Building Telecommunications Cabling*;

National Electrical Manufacturers Association

- ANSI C80.3-2005, *American National Standard For Steel Electrical Metallic Tubing (EMT)*;
- NEMA VE 1-2009, *Cable Tray Systems*;
- NEMA VE 2-2006, *Metal Cable Tray Installation Guidelines*;

National Fire Protection Association (NFPA)

- NFPA 90A-2009, *Standard for the Installation of Air-conditioning and Ventilating Systems*;
- NFPA 101-2009, *Life Safety Code*;
- NFPA 110-2010; *Standard for Emergency and Standby Power Systems*;
- NFPA 111-2010; *Standard on Stored Electrical Energy Emergency and Standby Power Systems*;
- NFPA 258-2001, *Recommended Practice for Determining Smoke Generation of Solid Materials*;
- NFPA 5000-2009, *Building Construction and Safety Code*
- *NFPA Fire Protection System for Special Hazards*, 2004;

Telecommunication Industry Association (TIA)

- ANSI/TIA-455-57-B, *FOTP-57, Preparation and Examination of Optical Fiber Endface for Testing Purposes* (1994);
- ANSI/TIA-455-133-A, *FOTP-133-IEC-60793-1-22, Optical Fibres-Part 1-22: Measurement Methods and Test Procedures-Length Measurement* (2003);
- ANSI/TIA-526-7, *OFSTP-7, Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant* (2002);
- ANSI/TIA-568-C.0, *Generic Telecommunications Cabling for Customer Premises* (2009);
- ANSI/TIA-568-C.1, *Commercial Building Telecommunications Cabling Standard* (2009);
- ANSI/TIA-568-C.2, *Balanced Twisted-Pair Telecommunications Cabling and Components Standard* (2009);
- ANSI/TIA-568-C.3, *Optical Fiber Cabling Components Standard* (2009);
- ANSI/TIA-758-A, *Customer Owned Outside Plant Telecommunications Infrastructure Standard* (2004);
- ANSI/TIA-942-1, *Data Center Coaxial Cabling Specifications and Application Distances* (2008)
- ANSI/TIA/EIA-455-95-A, *FOTP-95, Absolute Optical Power Test for Optical Fibers and Cables* (2000);
- ANSI/TIA/EIA-4720000-B, *Generic Specification for Optical Waveguide Fibers* (2002);
- ANSI/TIA/EIA-472D000-B, *Sectional Specification (Adopted ANSI/ICEA S-87-640-2006) Standard for Optical Fiber Outside Plant Communications Cable* (2006);
- ANSI/TIA/EIA-485-A, *Electrical Characteristics Of Generators And Receivers For Use In Balanced Digital Multipoint Systems* (2003)

The Green Grid

- Haas, Pierce & Schutter, "Data Center 2.0 Design Guide Program Overview," The Green Grid, 2009;

Underwriters Laboratories (UL)

- ANSI/UL 1479-2003, *Standard for Fire Tests of Through-Penetration Firestops*;
- ANSI/UL 797-2007, *Standard for Electrical Metallic Tubing – Steel*;
- ANSI/UL 972, *Burglary-Resisting Glazing Material*

Other Standards and Documents

- Rural Utilities Services (RUS), Bulletin 345-63, *RUS Specifications for Acceptance Tests and Measurements of Telephone Plant* (1995).
- *International Fire Code (IFC)*, 2009;
- Federal Communications Commission (FCC) Part 15 and Part 68;