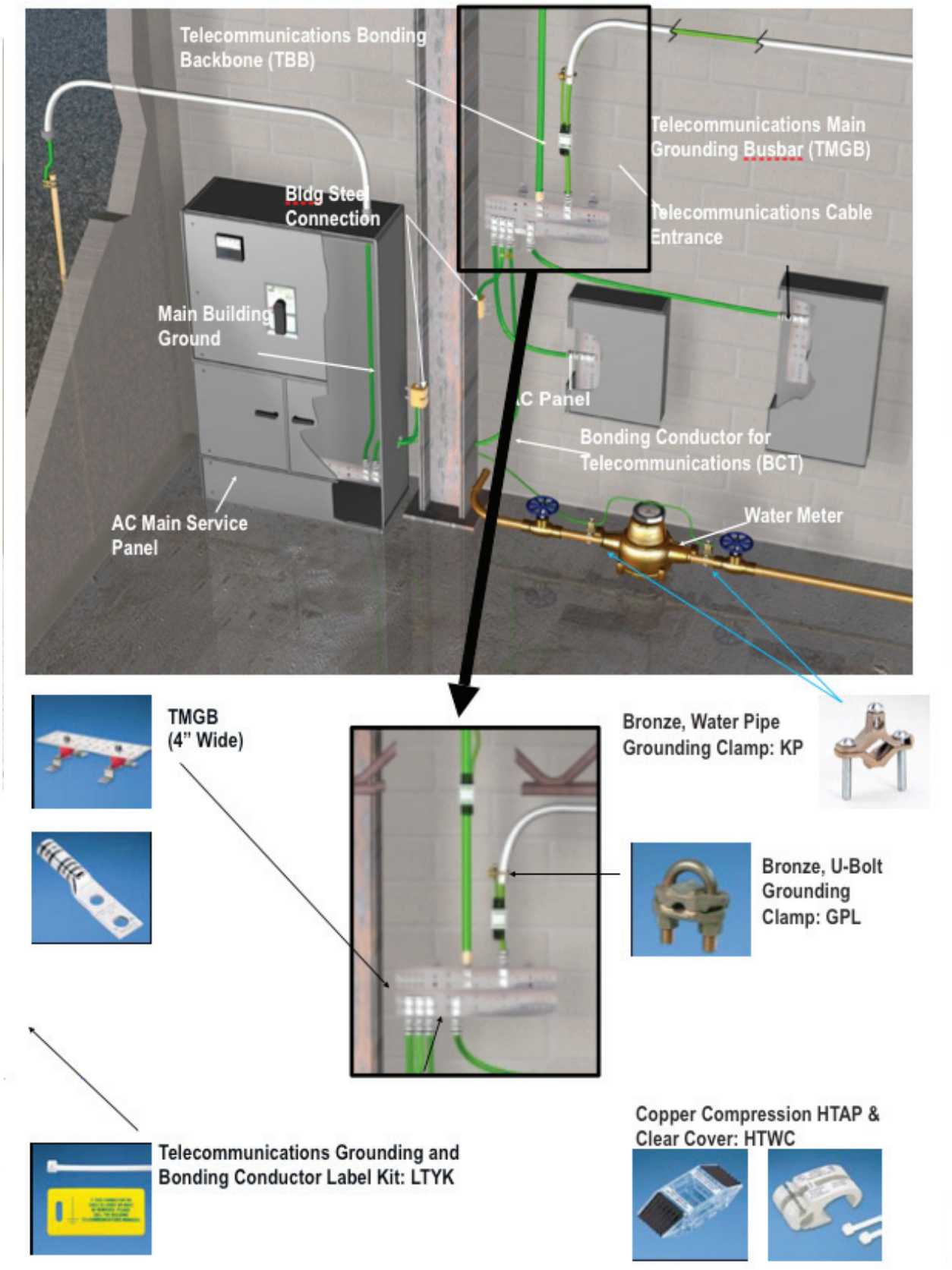


Figure 4.3-6. Data Center Grounding

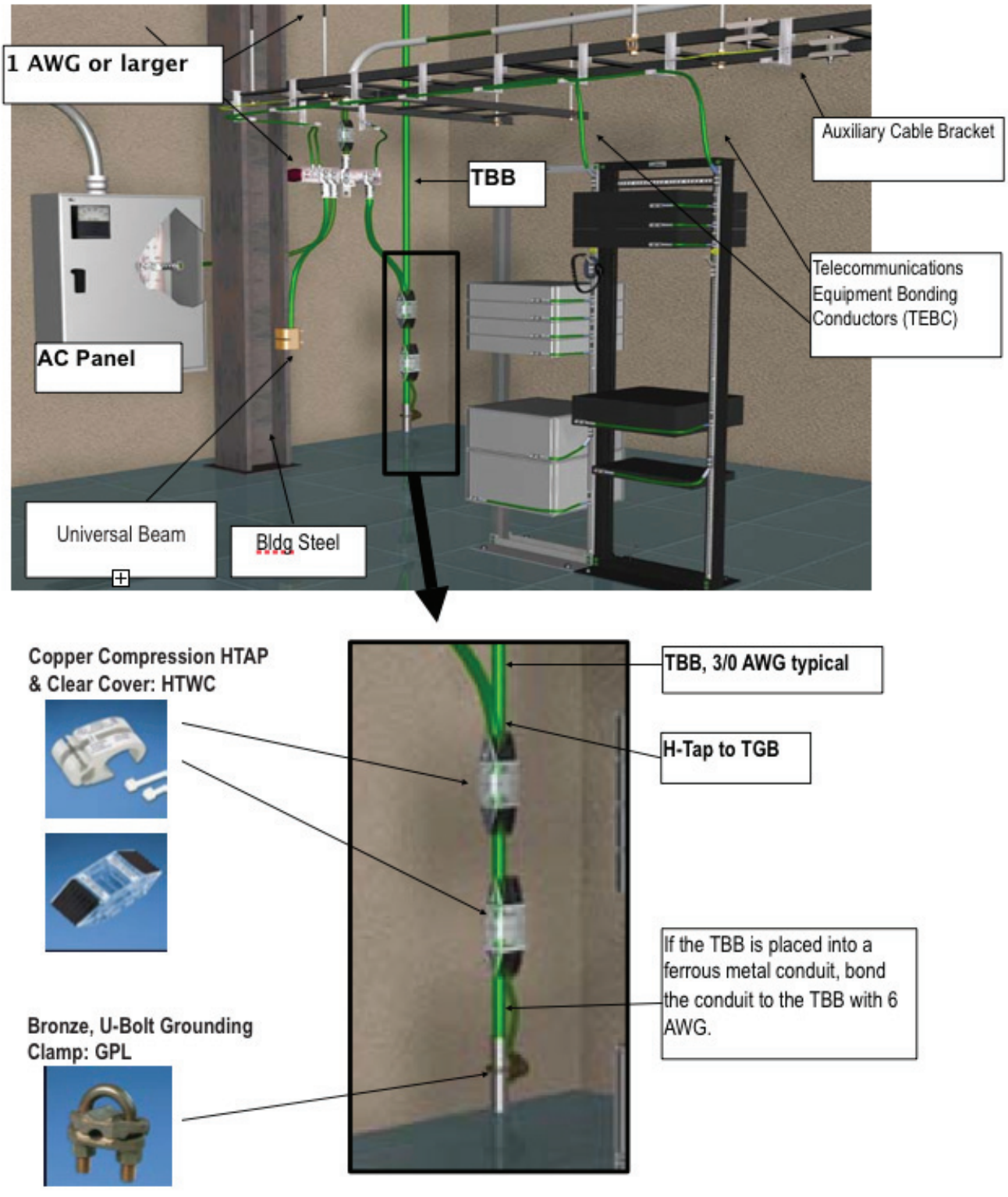


Figure 4.3-7. Control Room Grounding

4.3.1.3 Telecommunications System Grounding (Control Rooms and Data Centers)

Telecommunications grounding and bonding topologies are based on standards, ANSI/J-STD-607, TIA-942 and IEEE Std. 1100-2005. This is a typical practice found in enterprise data centers and telecom type service provider facilities (see Figure 4.3-8). These same standards and practices can be applied to the industrial data centers, control rooms and remote instrumentation enclosures (see Figures 4.3-2, 4.3-6, and 4.3-7).

be deployed and bonded to the TGB. This process can be broken into two smaller steps: (1) ensuring electrical continuity within rack and cabinet units, and (2) bonding these units to the busbar.

When assembling and installing racks and cabinets, TIA-942 and the upcoming BICSI/607 require the installer to verify that electrical continuity exists between all structural members. The paint used on racks and cabinets acts as an electrical insulator, preventing the flow of electricity from one section of the rack or cabinet to another. Therefore, attaching

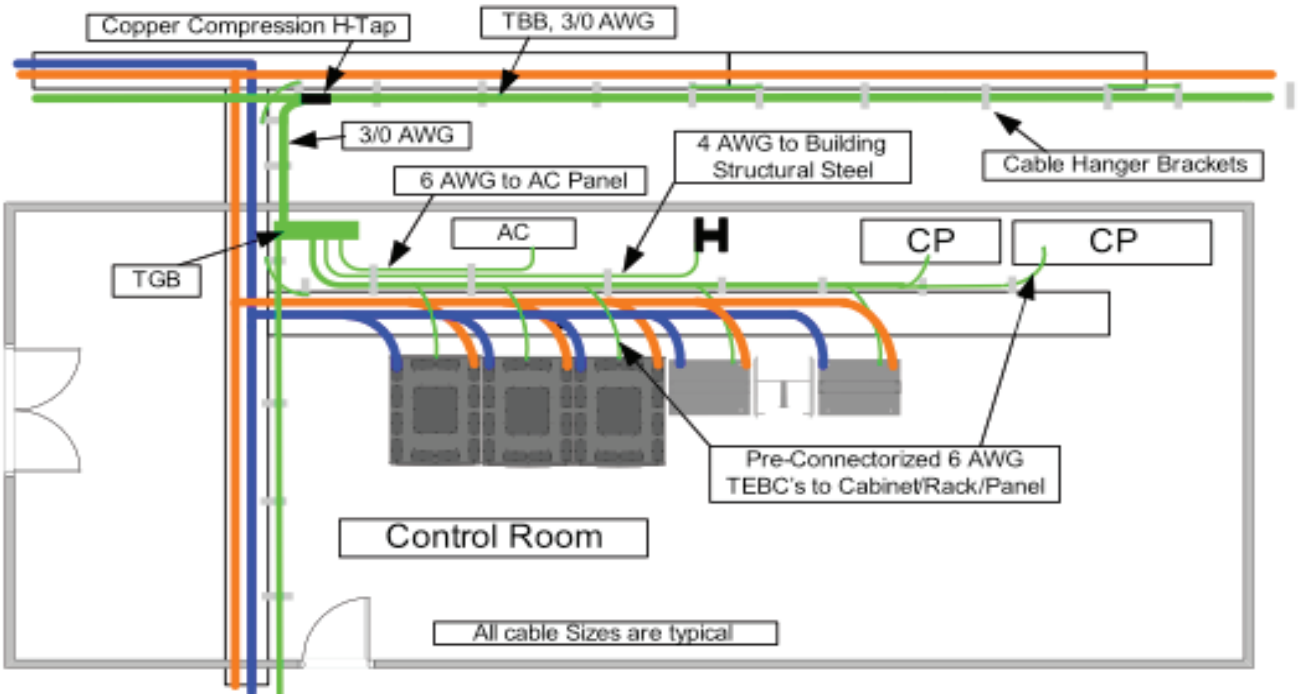


Figure 4.3-8. Schematic Diagram of Typical Grounding and Bonding of the Control Room

In general, once the AC power ground has been bonded to the TGB, installers can follow these basic steps in common TR spaces to deploy a robust grounding and bonding system that satisfies the intent of the standards and is professional in appearance:

1. Verify that the AC panel board is bonded to the TGB
2. Bond the TGB to the telecommunications grounding and bonding infrastructure
3. Create continuity within racks and cabinets
4. Bond the racks and cabinets to the TGB
5. Bond the equipment to the racks

Grounding Cabinets and Racks. Once all bonds from TGB to building steel, raceways, and TBB have been made, the telecommunications room is ready for racks and cabinets to

a grounding jumper from the rack to the TGB may not actually ground the entire rack, which results in a safety hazard.

Racks and cabinets are available that are fully bonded upon arrival from the manufacturer. Other rack designs contain provisions to create electrical continuity via grounding washers as the units are assembled in the field (see Figures 4.3-9 and 4.3-10). Otherwise, it is important to use paint-piercing hardware tested for its ability to create an electrical bond as the rack or cabinet is being assembled or, a last option is to scrape the paint between the mating components (see Figure 4.3-11).

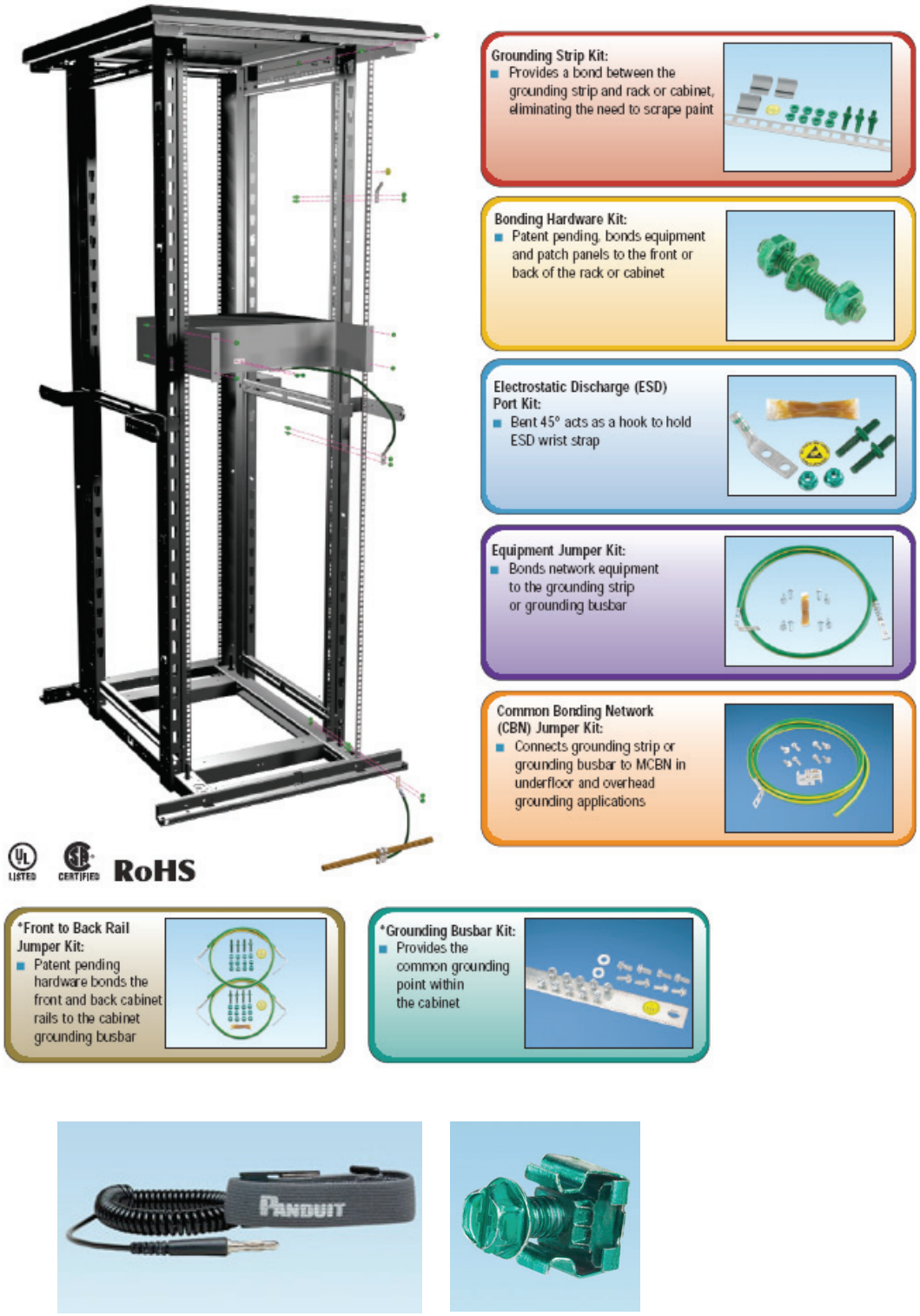
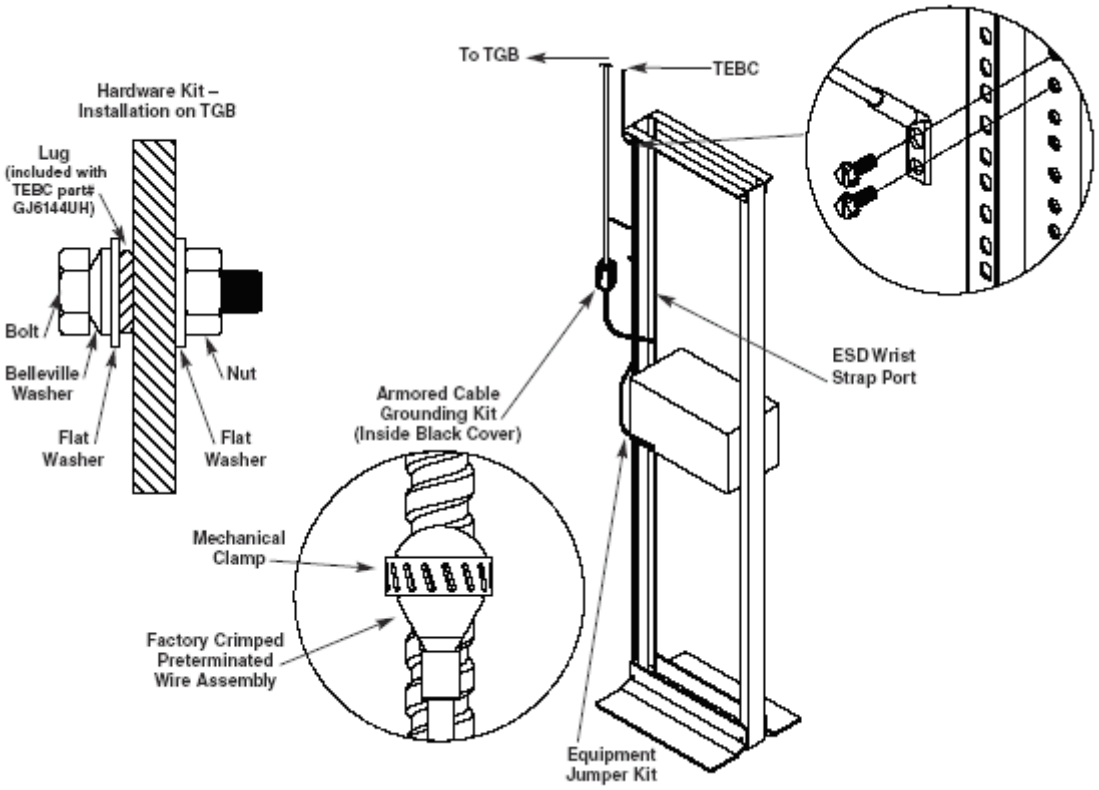


Figure 4.3-9. Cabinet Grounding


To TGB
TEBC
Hardware Kit –
Installation on TGB
Lug
(included with
TEBC part#
GJ6144UH)
Bolt
Belleville
Washer
Flat
Washer
Nut
Flat
Washer
Armored Cable
Grounding Kit
(Inside Black Cover)
ESD Wrist
Strap Port
Mechanical
Clamp
Factory Crimped
Preterminated
Wire Assembly
Equipment
Jumper Kit

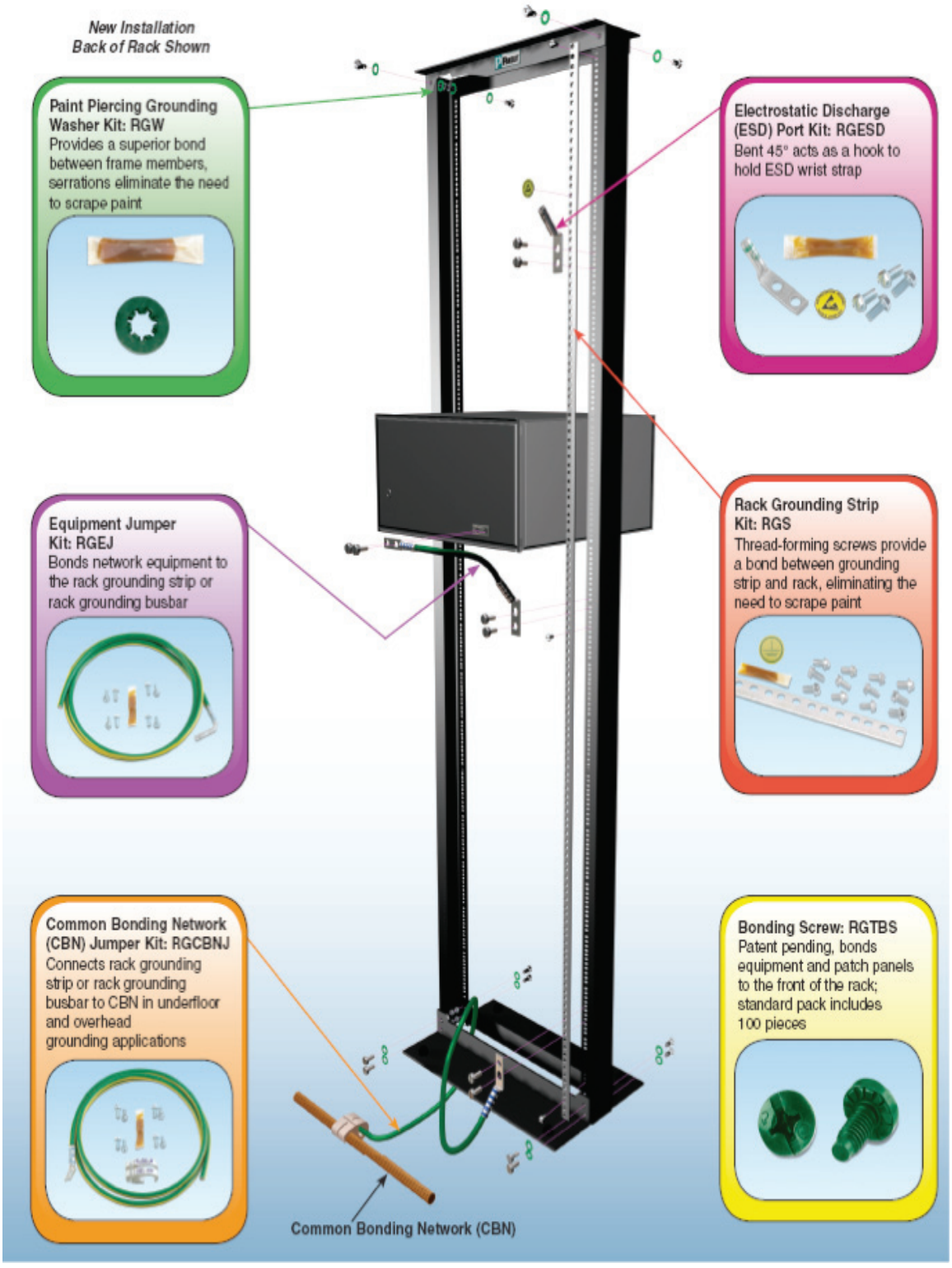


Figure 4.3-10. Rack Grounding

After the rack is assembled, install electrostatic discharge (ESD) wrist strap ports approximately forty-eight inches above the floor in racks that house active equipment, such as switches. Having such ports available allows people who service that equipment to have a convenient place to plug in their ESD protection wrist straps, thus protecting the equipment from damage while it is being worked upon (see Figure 4C-12).

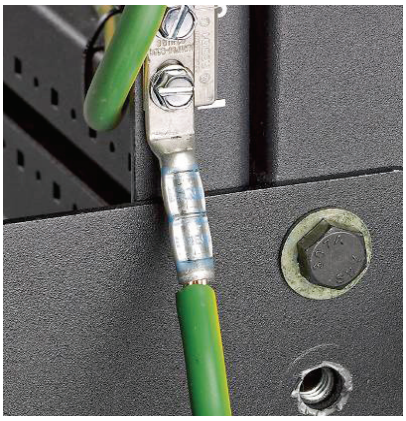


Figure 4.3-11. Grounding washers can be used to create electrical continuity in racks and cabinets. In this photo a bolt and washer is removed, showing paint removal from the contact area (bottom right).

Figure 4.3-12. ESD wrist straps and ports enhance equipment protection.

Different options exist for how to bond racks to the busbar (see Figure 4.3-13). Which method is chosen often depends upon the size and configuration of the installation. In TRs with about a half-dozen racks or less, such as most industrial control rooms, the most convenient method of bonding the racks to the busbar is to run a jumper known as a telecommunications equipment bonding conductor (TEBC) directly from each rack to the TGB.

In larger installations, the number of lug mounting locations on the busbar and the management of the grounding cables present a more complicated bonding situation. Under these circumstances, the installer should run a continuous TEBC from the TGB down each row of racks, making a bond from the TEBC to each rack. These jumpers should be bonded to the TEBC using compression HTAP connectors, and bonded to the rack using a two-hole compression lug.

The use of this lug at the rack is quite important, as this is a series circuit (where only one connection is made between rack and TEBC) and a two-hole compression lug will maintain the reliability of the connection at the same level as connections to the TGB (see Figure 4.3-14). Compression connectors are required by many grounding standards and specifications because the connector barrel will not loosen from the conductor over time.

The conductors used in bonding the racks to the TGB should be insulated with an all-green jacket or a green jacket having a distinctive yellow stripe to visually indicate them as being used for grounding purposes. In most telecommunications closets, use #6 AWG TEBC which will be sufficient due to the limited length required within a closet space.

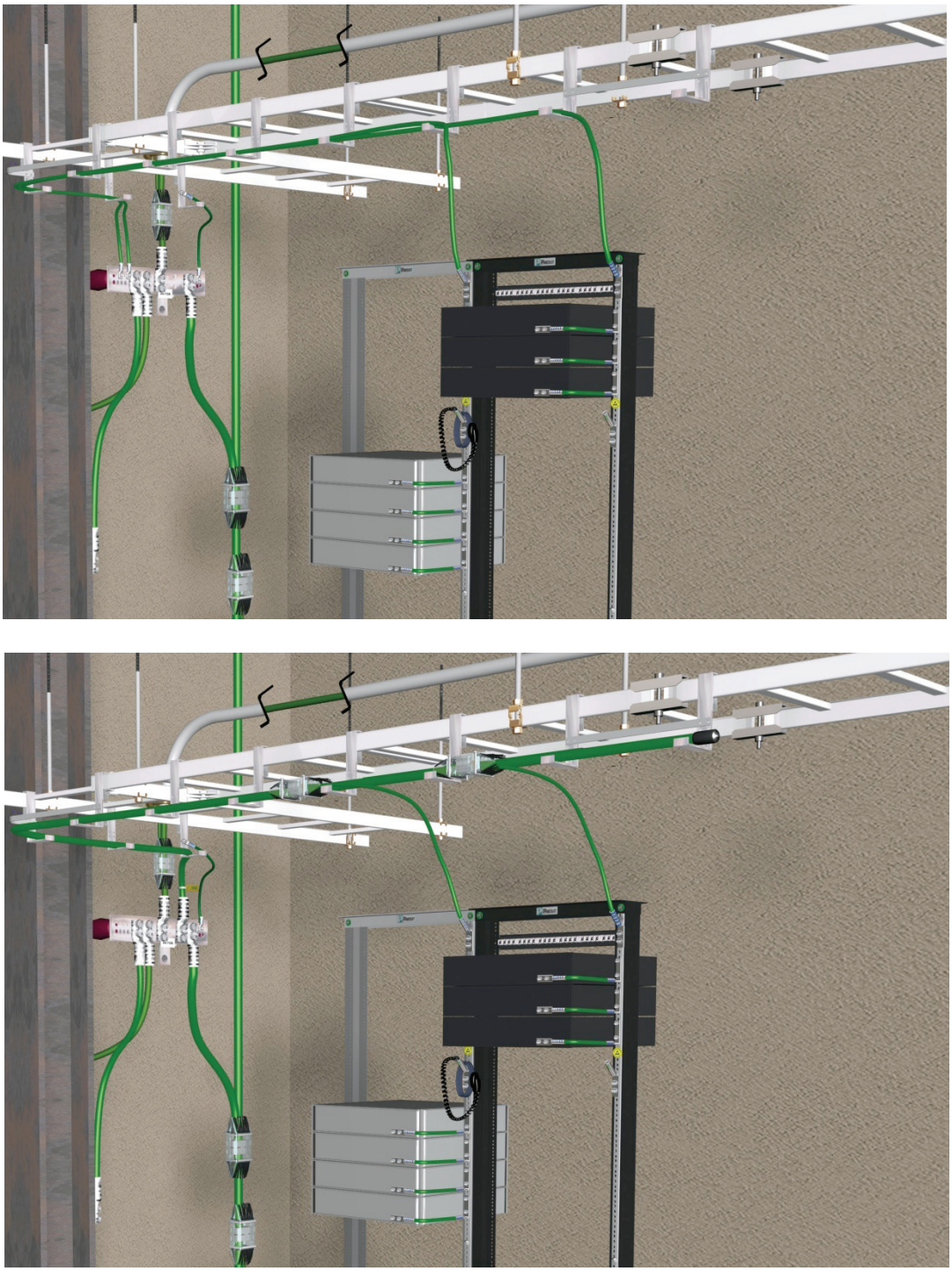


Figure 4.3-13. Telecommunications room bonding topologies (no access floor). Top – several TEBCs used to bond each rack directly to the TGB. Bottom – racks bonded to a single TEBC which then bonds to the TGB.

Busbar Hardware Kit

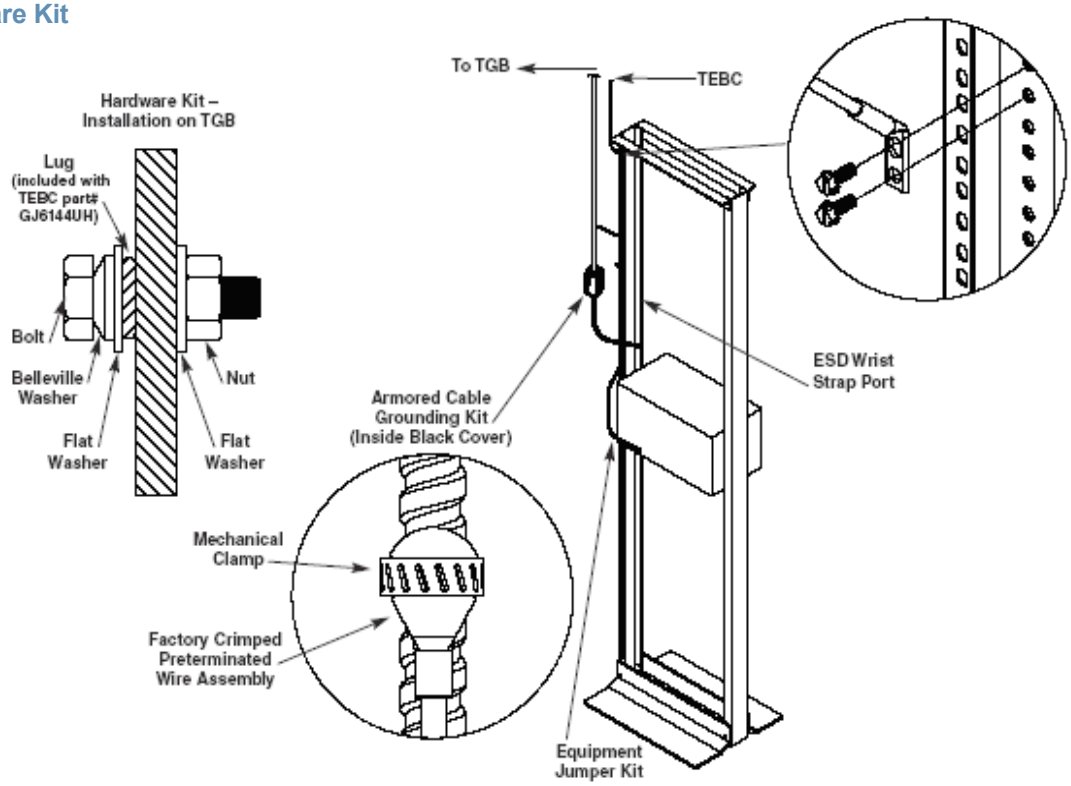


Figure 4.3-14. Busbar Hardware and Armored Fiber Grounding Kits

When bonding the conductor to the rack, it is important to remove insulating paint from the mating surface to complete the connection. For this purpose, most installers prefer to use thread-forming screws that remove paint from the thread holes as they are installed, or to use suitable bonding hardware for cage nut rail applications. It is also acceptable to simply scrape the paint off the rack in the area that the lug will bond, but is more time and labor intensive than using thread-forming screws.

Bonding Equipment to Racks. The final step for an installer is to bond active equipment (such as switches and servers) to the rack or cabinet as it is installed. The forthcoming BICSI/607 standard will likely contain the following statement when it is officially adopted:

"Grounding through the equipment AC (alternating current) power cord does not meet the intent of this standard. It is intended that the ac power ground path and the telecommunications ground path offer redundant and specific ground paths for the equipment. 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 on the AC power cord ground wire, it is desirable that equipment be grounded in a verifiable manner as described in this Standard."

The best strategy to meet the intent of this statement is to use a discreet jumper wire that bonds from a lug mounting pad (if provided by the manufacturer) on the active equipment and terminates via a two-hole compression lug at a busbar or vertical grounding strip attached to one of the rack's equipment mounting rails. The busbar or vertical grounding strip should be used to provide a visually-verifiable, all-copper grounding path (see Figures 4.3-9 and 4.3-10).

When equipment does not provide a lug mounting pad, the next best option is to bond the equipment mounting flanges directly to the rack rails. If the equipment mounting flanges are painted or covered in a non-conductive coating, bonding screws can be used to make this bond (i.e., thread-forming screws with serrations under the head of the screw will remove coatings from the surface to which they are mounted).

Bonding STP Shielded Cables in Control Systems.

Shielded twisted pair Ethernet cables provide an important means of returning high frequency noise to the noise source (see Table 4.3-2). The design of shielded cables and the proper termination of these cables require careful study of vendor recommendations and understanding of the system's bonding and grounding design to avoid ground loops.

The key issue with shielded cable systems is provide proper bonding to prevent high frequency noise from coupling to cable while reducing risk of ground loops and hazardous voltage from causing equipment or personnel concerns. There are several techniques and solution approaches that have been developed to provide options, depending on the magnitude and frequencies of the noise involved, that impact the quality of the ground system and topology of cable channel.

Table 4.3-2. Key Techniques for Effective Shield Bonding 360 degree Shield termination

360 degree Shield termination	Avoid the high impedance caused by long pigtail drain wires by using shield clamps that encircle the circumference of the shielded cable.
Ground loop avoidance	Proper system bonding between machine and control cabinets can allow bonding both ends of shield without concern of ground loop for maximum shield benefit for controlling noise. Otherwise, consider hybrid bonding through RC circuit or else bonding only one end of shielded able.
Motor Cable shielding	Shielding motor cables can reduce this noise source risk but requires termination at the motor and at the drive only. Do not terminate the motor cable to the subpanel to avoid noise problems.

Ground Loop Concerns. A ground loop can form when there is a different voltage potential between two ends of a cable (see Figure 4.3-15). The concern is that even a small voltage difference can result in high enough noise currents to cause coupling to cables. In some cases, this voltage can be quite high and cause real concern about communication disruptions - even equipment damage. This fear leads to common wisdom to only ground one end of a shielded cable. However, this common wisdom falls down for high frequency noise mitigation where inductive and capacitive effects prevent a single point ground from effectively reducing noise voltages.

For best noise mitigation, therefore, it's desirable to extend the ground plane by bonding both ends of the cable. However, this is not readily done without creating a ground loop. This dilemma has led to development of hybrid bonding solutions to provide bonding at both ends while blocking low frequency ground loops.

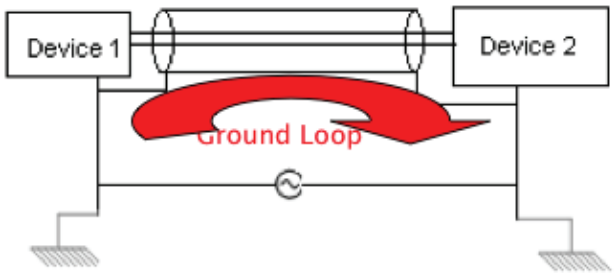


Figure 4.3-15. Example of Ground Loop caused by voltage difference between equipment grounds at two ends of a shielded cable.

Hybrid Bonding. To allow for bonding both ends of a shielded cable with some mitigation of the ground loop concern, a technique called hybrid bonding is employed where an RC circuit only allows high frequency noise to pass through the loop and blocking the lower frequencies (e.g. 60 Hz) that may be present because of ground level differences.

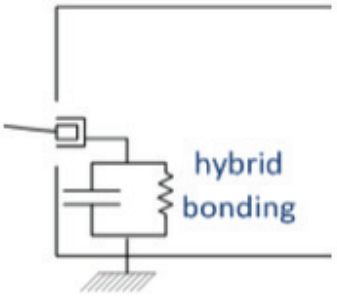


Figure 4.3-16. Hybrid bonding using RC circuit that blocks low frequency ground loop currents

Ethernet/IP use of Hybrid bonding, overall channel design. Most Ethernet/IP devices built today employ hybrid bonding built into the device. However, due to legacy and third party non-Ethernet/IP devices, a system designer needs to examine each device and make appropriate decisions on when and where to bond to avoid ground loops. The overall shielded cable channel design from switches through patching to devices needs to be analyzed from the bonding perspective to gain important noise control benefits brought by the shielded cable while avoiding ground loop problems. The following details patching options that can assist with mitigating noise and avoiding ground loops in automation systems that employ switches and devices with hybrid bonding or mixed approaches.

Shielded Cable Patching Options for Stratix switch based systems. To complicate the design of proper even further, you need to consider the physical infrastructure arrangements related to patch panels in rack/enclosure systems in a control rooms, zone enclosures, and control panels. The distribution of network cabling from control rooms out to control systems greatly benefits from use of consolidation and patching areas as discussed in Sections 2.3 and 2.4 of this Reference Architecture Guide. The complication arises with shielded cable systems is avoiding introducing ground loops at the patch points when installing shielded components.

Ground loop problem associated with a patch panel. Ground loop problems can arise in a control room even between a switch and a patch panel mounted in the same or a few feet away in an adjacent rack depending on the noise frequencies involved. At high frequencies, noise can capacitatively or inductively couple through paths that are not the intended ground path. Voltage differences can develop between areas of rack or enclosure systems that appear to be securely bonded. A patch panel for shielded cable that is bonded may actually be at different voltage than the switch in the same vicinity! This problem is illustrated in Figure 4.3-17.

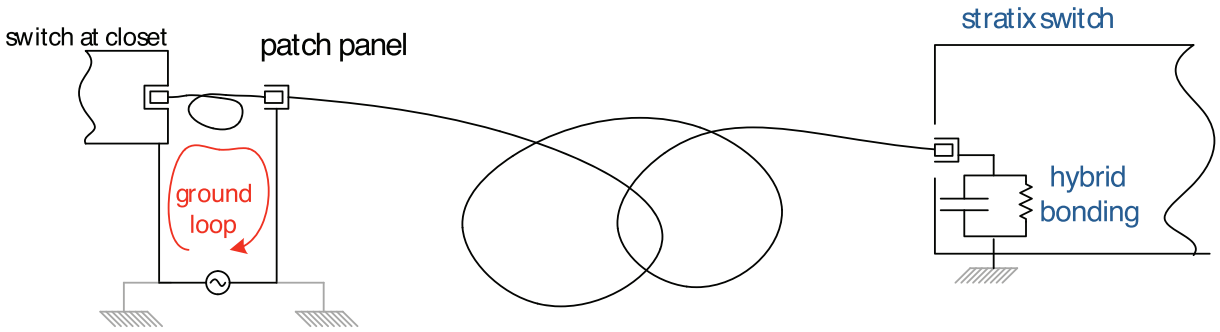


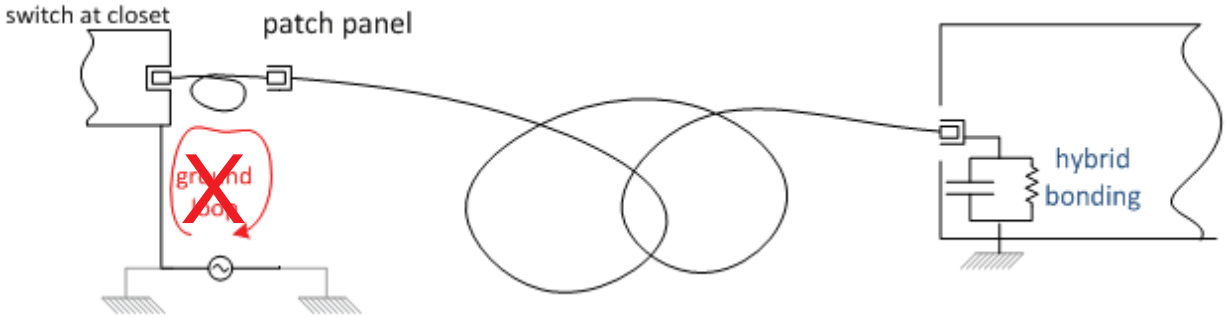
Figure 4.3-17. Ground Loop formed between patch panel and switch due to ground voltage differences. The hybrid bond at the device prevents ground loop from patch to device for lower frequencies.

Standard data center practice for shielded patch panels is to bond the patch panel and shielded connector together which, in turn, is bonded to the rack. This bonding is effective for the typical data center noise and ground loop issues. However, for industrial applications in control rooms, zone enclosures and patch panels, direct bonding at the patch panel can introduce a ground loop as in the diagram above.

Method to prevent ground loops when using patching.
One recommended method to prevent ground loops forming at the patch area or out to the field device is to use an electrically isolated, insulated patching solution. This requires that the shielded jack snap into plastic or other insulating material rather than bonding to the patch panel and to the rack which is typically bonded to the room ground system.

A patch panel or outlet assembly that is not bonded but that does allow continuity of the shield through the patch field can effectively eliminate the patching ground loop concern. Figure 4.3-18 shows an insulated patch approach. The shielded jack and shielded patch cord would pass the high frequency noise back to the switch but not introduce a ground loop at the patch.

Figure 4.3-18. Insulated patch panel prevents ground loop at switch and patch panel



The following are PANDUIT parts that can aid in implementing an insulated patch panel solution at the control room, zone cabling enclosure or control panel.

PANDUIT Part#	Description		
CPPA24FMWBLY	Angled 24-port flush mount patch panel	QPPABL For use with QuikNet Panels and or QuickNet 0RU Bracket	Accept QuickNet™ Copper Cable Assemblies and QuickNet™ SFQ Series MTP* Fiber Optic Cassettes
CPP24FMWBLY	24-port flush mount patch panel supplied with rear mounted faceplates.	CWPP12WBLY	12-port patch panel supplied with three factory installed CFFP4 snap-in faceplates with integrated wall mount bracket.
UICMPPA24BLY	24-port angled patch panel with six UICPPL4BL Mini-Com® Ultimate ID® Faceplates.		

In cases where there are no substantial ground loop concerns (e.g. facility with well engineered mesh ground system), it may be desirable to bond shielded cables at the patch panel especially for cabling run within the control room or other well bonded areas. The following procedure and diagram outlines basic methods for this approach.

As an example and outlined in Figure 4.3-19, the PANDUIT four step process to properly bond the shield at the patch panel is as follows:

1. Bond all the shielding (foil and/or braid) of the data cable to the shielded jack module, which provides 360° shielding termination, as shown in Figure 4.3-20.
2. Snap the jack module into an all-metal patch panel to create a bond between the module and the unpainted tabs on the patch panel.
3. Attach the patch panel to the rack using thread-forming bonding screws; the thread on the screws removes paint from the thread holes on the rack and the serrations on the head of the screws remove paint from the patch panel, creating a high-performance electrical bond between the patch panel and the rack.
4. So long as electrical continuity exists throughout the rack, the last step is to bond the rack to the main busbar or MCBN located under the data center raised floor. To ensure long-term integrity of the system, always use compression connectors, not mechanical, so the connection does not loosen with vibration.

Once cabling to the patch field has been bonded, attention can be turned to the rest of the bonding and grounding system. The rest of this article focuses on several best practices that must be considered during the design and installation of the rest of your shielded structured cabling system.

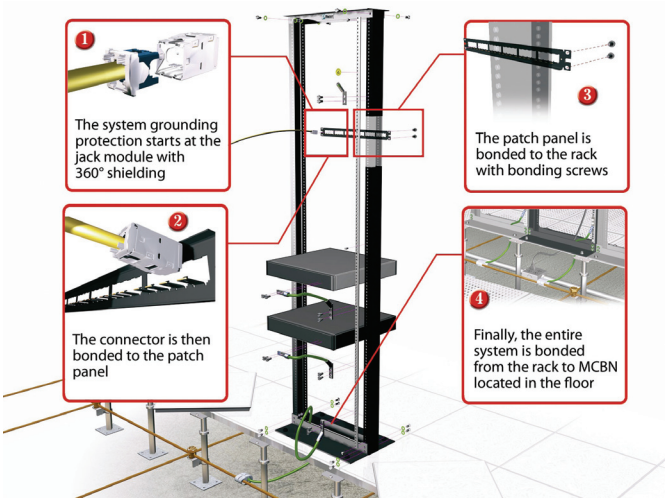


Figure 4.3-19. The PANDUIT® StructuredGround™ System for data center grounding provides robust connections that have low resistance, are easy to install, and are easily checked during inspections.

Grounding the Cable Shield. During installation, a frequently asked question is whether the installer should ground one end or both ends of a shielded cable channel. Generally, the cable shield is bonded to the grounded equipment chassis or rack at each access or patch location. In other words, if all ITE is grounded, then any shielded cables used to connect equipment to patch panels, or to other equipment, must be grounded.

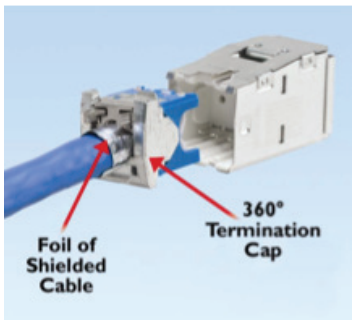


Figure 4.3-20. PANDUIT Shielded Cable and Jack Module Termination

A typical shielded structured cabling channel runs from a switch to the workstation and is comprised of two patch cord links and the shielded horizontal link. One end of the channel starts in the data center, where the switch, patch panel, and shielded patch cord linking them must be properly bonded to the rack. The rack is tied to the telecommunications grounding system, which in turn is bonded to the AC power system (see Figure 4C-19).

The other end of the channel terminates outside the data center at a workstation outlet. An issue that must be considered is whether a shielded cabling link at this outlet location can be properly bonded to a grounding system without inducing a ground loop. A cable shield that is terminated at the workstation may be bonded to the AC ground via connections within the workstation itself, but the outlet AC ground must be at the same potential as the telecommunication grounding system.

The recommended method for grounding the shielded link is to use the workstation-provided ground. Use of a shielded patch cord grounds both ends of the shielded cable link and completes the shielded channel. However, when both ends of a shielded link are grounded, there is the possibility for a ground current to be conducted across the shielding if the grounds are not at the same potential. In this example, a voltage difference may exist on the ground between the AC

power source serving the workstation and the telecommunication ground within the data center.

Therefore, to reduce the magnitude of such ground currents, all serving AC power systems must be bonded together to the same grounding electrode system (a building can have only one grounding electrode system, as required by the NEC). This approach will reduce any ground voltage differences that may exist either between differing AC power system grounds or between the AC power system ground and the telecommunications ground.

4.3.1.4 Control System Grounding

Bonding and grounding is the foundation for controlling EMI in control systems. Because grounding is a legal NEC requirement for electrical safety, the sight of green and yellow ground straps, ground bars, and PE conductors are common and relatively well understood. However, you can have a fully compliant, ultra safe grounding system yet have equipment that encounters serious disruptions, stoppages, and even damage due to an inadequately installed and engineered low impedance ground/bonding system for high frequency noise.

Control Panel Grounding. Three concepts of best practice control panel layout and design (see Figure 4.3-21) for this high frequency noise are:

1. High Frequency Return Path

High frequency noise currents will return to their source to complete a circuit. In some cases this can lead to noise being coupled into adjacent Ethernet cables. The goal is to layout noise sources and cabling with their associated grounds and cable shields so that the noise currents return in a safe controlled path rather than inadvertently traveling through sensitive circuit cables and devices. This requires understanding the noise sources and the role of shielded cables and equipment grounds.

2. Braided Bond Straps

A low-resistance 3-foot 14awg wire which serves quite adequately as a safety ground for 60Hz power is totally inadequate as a conductor for high frequency return current since at 10 MHz it has 300 ohms of impedance. At high frequencies of >1 MHz, multiple short 1” minimum width braided bond straps should be used between sub-panels and doors to allow the high frequency current to conduct with less impedance.

3. Ground Plane Principle

Printed circuit board designers were the first to use the ground plane principle when designing high frequency circuits. Everything is at the same potential at the surface and the impedance is practically zero at all frequencies.
The back plane or sub-panel makes an ideal ground plane to bond control panel components. Ideally, the ground plane should extend to include the entire machine or process by connecting to a mesh ground system or with large equipotent bonds run to external cabinets or machine bases.

Tips for Using the Ground Plane Principle

- Use an electro galvanized sub-panel instead of the more common painted panel. This avoids need to remove paint for bonding with resultant long term corrosion potential risking poor performance.
- Bond multiple sub-panels together using 1” wide short flat braided bonding straps to create one large ground plane. (See Figure 4C-22).
- Bond the incoming ground conductors to the sub-panel where they enter the panel.
- Bond the equipment grounds from the components in the cabinets directly to the sub-panel using equipment manufacturer recommended conductors or short flat braided bonding straps.
- Bond the enclosure door(s) with short flat braided bonding straps.
- Bond incoming cable shields (see Figure 4C-5), conduits and cable trays to enclosure

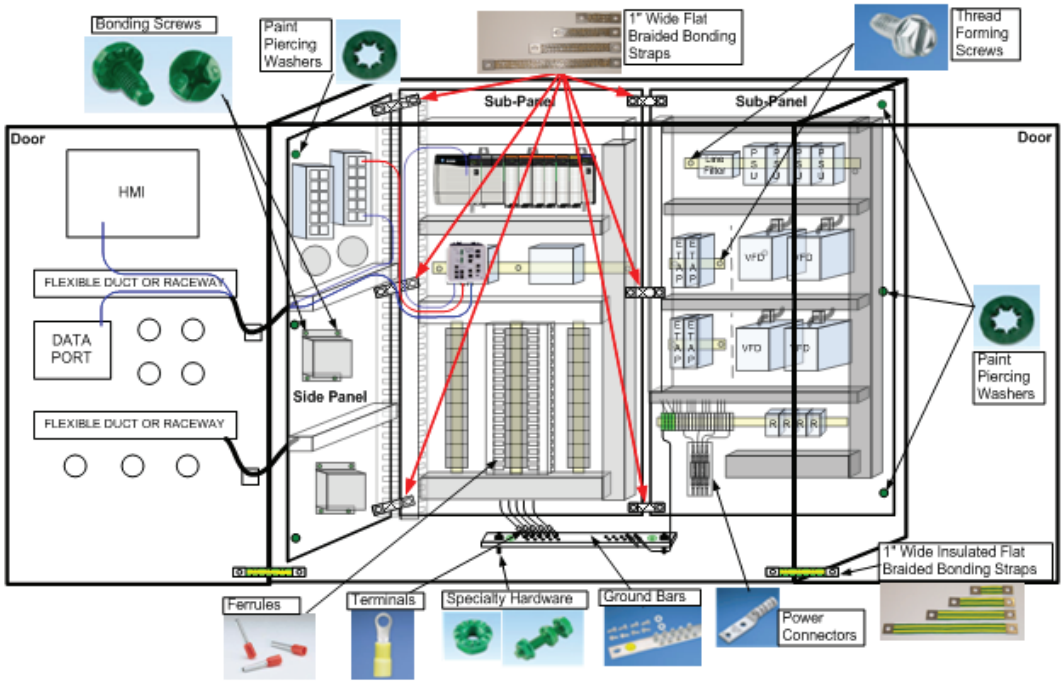


Figure 4.3-21. Schematic Diagram of Control Panel Grounding and Bonding

\Motor Cable Termination Best Practice. Control system noise problems can cause intermittent communication problems that are difficult to diagnose and solve. One important recommendation is to prevent potential noise problems from high frequency noise that can be introduced from poor termination practice with servo or VFD motor drive cabling systems. There are well established best practices for motor cable termination to avoid noise problems that are published by vendors and in technical journals. However, mistakes are still being made that cause communications and control disruptions because of a failure to change installation practice in the field.

Figure 4.3-22 describes the best practices for motor cable grounding, and Figure 4.3-23 shows how using shielded cable presents a low impedance return path for motor noise currents with greatly reduced noise through the ground systems. This approach reduces the size of the ground return loop and reduces the coupling of noise to adjacent communication cables.

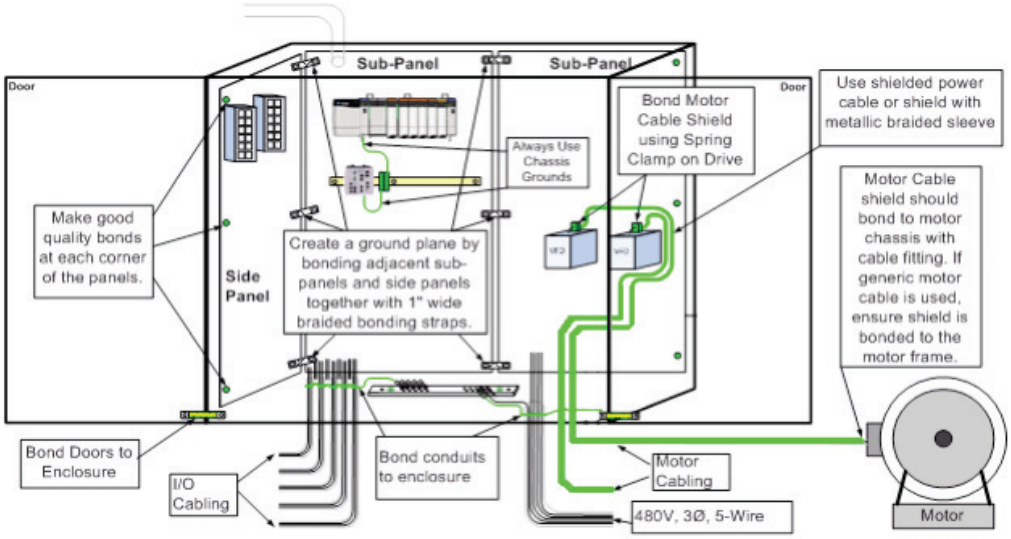


Figure 4.3-22. Motor Cable Grounding Best Practices

4.3.2 Selection

Most facilities are subjected to many electrical disturbances including lightning strikes, voltage fluctuations, static electricity and electrical noise, all of which are capable of affecting production in virtually everyone's business. A designer or engineer of any of these systems needs to understand the requirements of the grounding and bonding system for each of their applications.

Selection of appropriate and robust power system grounding schemes, equipment grounding methods, surge protection equipment, lightning protection equipment, ground electrode systems and the protection of sensitive electronic equipment are critical to the performance and reliability of industrial systems.

A full example specification documents for GES connections and for a data center / control room environment are provided in Appendices C-1 and C-2, respectively.

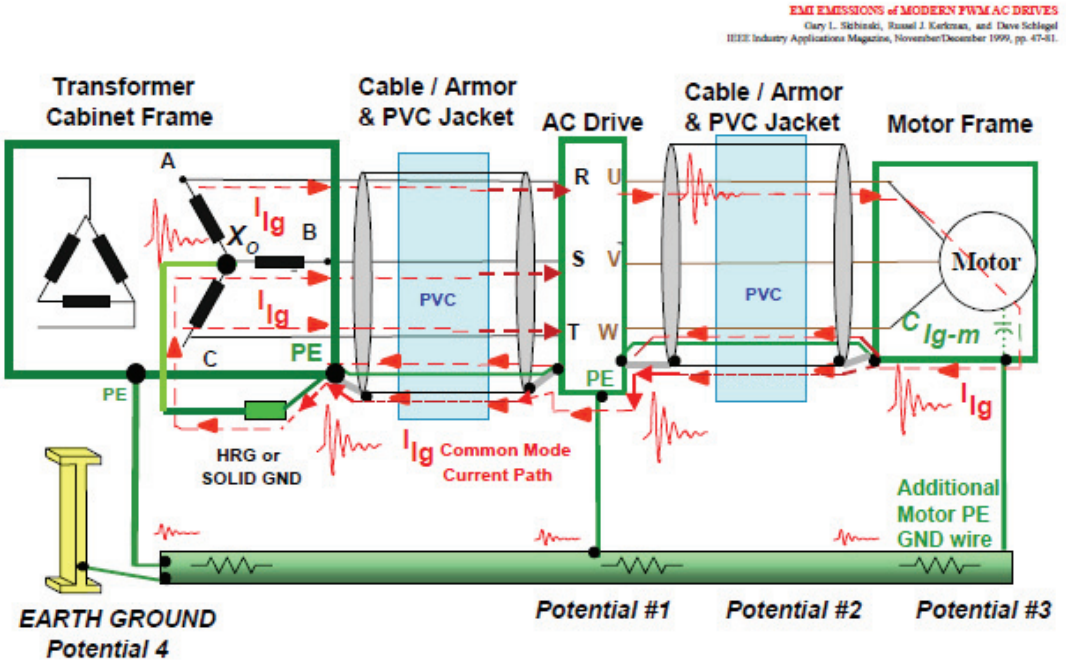


Figure 4.3-23. Best Wiring Solution: Shielded input/output with insulated jacket completely avoids ground noise problems in system.

4.3.3 Installation

The ground/earth system must be designed for high reliability. Therefore, the grounding/earthing system shall meet following criteria:

1. Local electrical codes shall be adhered to.

2. The grounding/earthing system shall comply with J-STD-607-A, ANSI/TIA-942, IEEE Std 1100™, and in international regions BS EN 50310:2000.

3. All grounding/earthing conductors shall be copper.

4. Lugs, HTAPs, grounding strips, and busbars shall be UL Listed and made of premium quality tin-plated electrolytic copper that provides low electrical resistance while inhibiting corrosion. Antioxidant shall be used when making bonding connections.

5. Wherever possible, two-hole lugs shall be used because they resist loosening when twisted (bumped) or exposed to vibration. All lugs shall be irreversible compression and meet NEBS Level 3 as tested by Telcordia. Lugs with inspection windows shall be used in all non-corrosive environments so that connections may be inspected for full conductor insertion (battery rooms are an exception where windowless lugs may be used).

6. Die index numbers shall be embossed on all compression connections to allow crimp inspection.

7. Cable assemblies shall be UL Listed and CSA Certified. Cables shall be a distinctive green or green/yellow in color to signify that they are grounding conductors, and all jackets shall be UL, VW-1 flame rated.

4.3.3.1 Visual Inspection

To optimize the safety and performance of your network grounding and bonding system a visual inspection should be performed upon installation and on an annual or semi-annual basis thereafter. An inspection that follows a line-by-line work order allows early detection of potential problems such as loosened or corroded connections, missing labels, conductors that have been damaged, cut, or removed, and new metallic elements that require connections to the grounding system. Connections to Busbars, Racks, Cabinets, Enclosures and Network Equipment should be inspected on a yearly basis. An example of an inspection process and a form for documentation of basic requirements and verifications can be found in Appendix C-3.

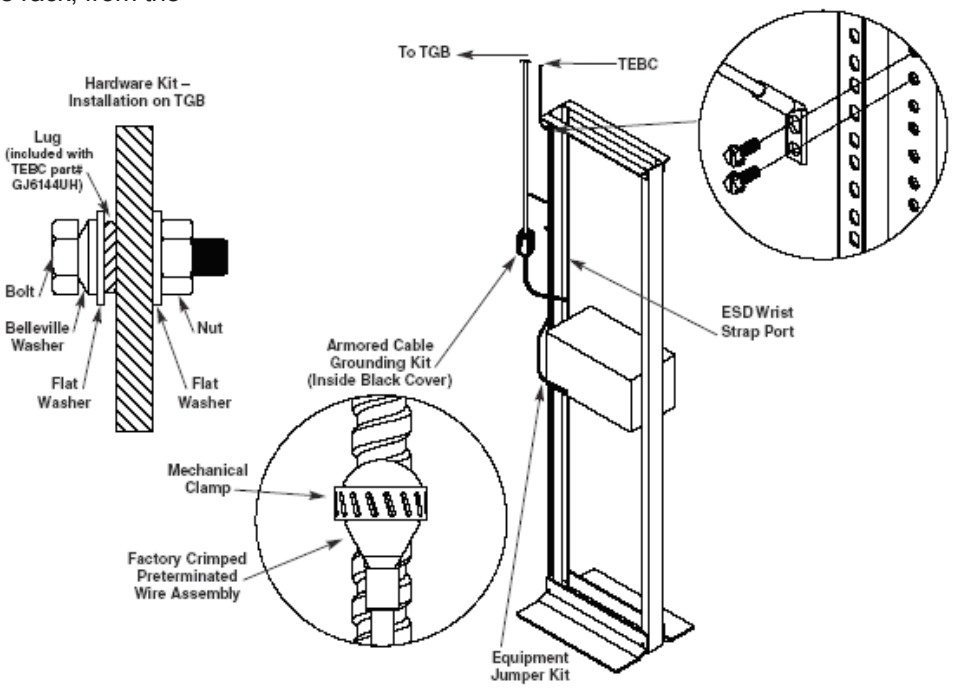
To facilitate inspection of the grounding system, install connectors, busbars, and conductors in such a way to allow visual verification of the bond. There should be a logical flow as you follow the grounding path(s); for example, follow the path(s) from the equipment chassis to the rack, from the rack to the data center grounding infrastructure, then over to the local TGB. The TGB connects to the telecommunication bonding backbone (TBB), or grounding cable, that runs back the telecommunications main grounding busbar (TMGB), which is bonded to earth ground via the electrical entrance facility and links all the TBBs together. Inspect all splices for proper crimping, and inspect labels to ensure that proper labeling has been followed.

Attempting to measure the resistance of any bond will actually result in the measurement of all electrical paths available, making it difficult to measure the resistance of any single bonding connection. As such, it is important to combine a visual inspection with measurements when verifying an installation. An inspection should include the following steps:

a) Check for excessive currents on the conductors bonded to the TGB. Using a clamp-on ammeter check to be sure AC RMS currents are between 0.0 A and 1.0 A and DC currents are between 0.0 A and 0.5 A.
b) Complete visual verification of the bonding and grounding system:
   ---Confirm bond between AC panel board and TGB
   ---Verify continuity within racks/cabinets
   ---Look for two-hole compression lugs on racks/cabinets and on busbars
   ---Ensure that ESD wrist strap docking stations are convenient
   ---Confirm that equipment is bonded to the rack/cabinet
c) Perform two-point continuity checks between surfaces where a bond is desired.

4.3.4 Documenting

A good documentation process goes hand in hand with a good inspection program. Grounding inspections should be well documented. An example of an inspection process and a form for documentation of basic requirements and verifications can be found in Appendix C-3.



4.4 Racks and Cabinet Enclosures

As modern manufacturing continues to evolve, operations have become intensive producers and consumers of data. The heart of any data management and storage system is the physical layer equipment: switches, routers, servers, cabling/connectors, and patch panels. This equipment finds its home in the racks and enclosures that provide a robust environment, managing risks to equipment from physical damage, temperature variations, and unauthorized access.

Rack and cabinet enclosures are available in a variety of configurations to address the variety of risks that manufacturing data systems are exposed to in the industrial environment. “Open” enclosure systems allow excellent air flow for keeping equipment cool, and include 2- and 4-post racks plus their accessories. Ironically, the main advantage of open systems can also be their main disadvantage. In a manufacturing environment, fibers and dust can migrate from the plant floor and come into contact with physical layer equipment, potentially disrupting network operations and increasing maintenance costs.

Open systems, however, present security and safety risks because anyone with access to the control room has direct access to all physical layer equipment. Cabinet enclosures offer many of the advantages of an open 4-post rack system with the added security of side panels, a top and bottom, and lockable doors at front and back. These features help manage risk associated with keeping office and control networks linked yet segregated, and help prevent unauthorized access or inadvertent damage to control networks from Internet users. (See Section 4.8 of this Guide for more information on Safety and Security issues related to Industrial Ethernet networks.)

Outside the control room, smaller enclosures (often referred to as “Zone Cabling Enclosure”) are available that allow remote deployment in factory applications for either active equipment or for patching the factory Ethernet network into manufacturing equipment.

PANDUIT offers specialized cabinets for server applications, such as those running FactoryTalk, RSView SE, or other manufacturing application software. Cabinets are also available for switching applications, where cabling management issues need to be addressed in ways that differ from server cabinet applications.

STANDARDS and CODES

Industrial network stakeholders can leverage the expertise of Data Center standards in industrial automation areas (both in the Control Room and on the factory floor) to mitigate performance risks and enable system convergence.

TIA/EIA-942

TIA/EIA-942 (Telecommunications Infrastructure Standard for Data Centers) specifies the minimum requirements for the telecommunications infrastructure of data centers and computer rooms.

CEA-310-D

Consumer Electronics Association CEA-310-E, design requirements for Cabinets, Panels, Racks and Subracks (formerly EIA-310-D).

TIA/EIA-568-B

TIA/EIA-568-B (Commercial Building Telecommunications Cabling Standard) covers structured cabling systems (both balanced copper cabling and fiber optic cabling) for commercial buildings, and between buildings in campus environments. The bulk of the standards define cabling types, distances, connectors, cable system architectures, cable termination standards and performance characteristics, cable installation requirements, and methods of testing installed cable.

4.4.1 Selection

Selecting an end-to-end enclosure system extends beyond choice of racks and cabinets, and includes horizontal and vertical cable managers. Together, these systems optimize thermal management in dense active equipment environments by routing cables away from exhaust fans and neatly managing them in horizontal and vertical pathways.

Open Racks

CMR19X84
19” EIA rack, aluminum.
Dimensions:
84.0”H x 20.3”W x 3.0”D
(2134mm x 514mm x 76mm).

Standard 2-post open rack

CMR4P84
4-post EIA rack with #12-24 threaded rails.
Dimensions:
84.0”H x 23.3”W x 30.2”D
(2134mm x 591mm x 767mm).
4-post open equipment rack.

Cabinet Enclosures

CS1
Server cabinet frame with top panel. Single hinge perforated front door. Split perforated rear doors open in the middle to minimize door swing footprint.
Designed for servers and patch panels.

CN1
Switching and patching cabinet frame with top panel. Single hinge perforated front door. Split perforated rear doors open in the middle to minimize door swing footprint.
Designed for switches and patch panels.

Cable Managers

NM2
NetManager Horizontal Cable Manager High Capacity Front and Rear 2 RU. Cat6A cabling.

Horizontal cable manager used with racks or cabinet enclosures

PRV8
Patchrunner Vertical Cable Manager Front & Rear 8” (203mm) for 84” High (2134mm) Racks.

Vertical cable manager used with open 2- or 4-post racks

Zone Cabling Enclosure

PZC12W
12RU Wall mount cabinet with windowed front door; black.

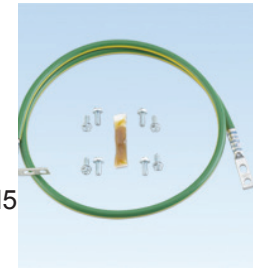
Used for remote installation of RU based equipment.

Blanking Panel

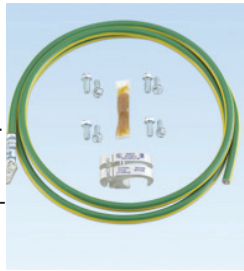
DPFP8
Filler Panel 8 RU
Used to blank out unused rack spaces in open racks or enclosures. Also used to mount panel equipment into open racks and cabinets.
NOTE: DIN rails can be mounted to these filler panels for DIN rail based equipment.

Grounding and Bonding

RGEJ624PFY
6 AWG (16mm²) jumper; bent lug on grounding strip side to straight lug on equipment; provided with .16 oz. (5cc) of antioxidant and two each #12-24 x 1/2”, M6 x 12mm, #10-32 x 1/2” and M5 x 12mm thread-forming screws



RGCBNJ660P22
#6 AWG (16mm²) jumper; 60” (1.52m) length; 45° bent lug on grounding strip side; provided with .16 oz. (5cc) of antioxidant, two each #12-24 x 1/2”, M6 x 12mm, #10-32 x 1/2” and M5 x 12mm thread-forming screws and a copper compression HTAP* for connecting to the MCBN.



4.4.2 Installation

Proper installation of cabinets and open 2 and 4 post racks rely heavily on the directions supplied by the manufacturer. Some overriding best practices are common among all manufacturers and weight load -- cabinets and open racks are rated for their load supporting capability. It is important that the weight rating is not exceeded. Reputable manufacturers have their cabinets and racks weight capacity certified by Underwriters Labs.

Stability: Especially for 2 post open racks, stability under load should be evaluated. If stability is a concern, a 4 post open rack or cabinet may be required. If the installation environment is in an earthquake-prone area, extra steps will need to be taken to insure stability and safety. Bellcore GR-63-CORE standards cover seismic requirements.

Electrical safety: Virtually all cabinets and open racks have provisions for grounding and bonding the structure. Modern data center and control equipment need proper grounding for electrical noise control and personnel safety. Proper grounding should be established on installation.

- Cabinet CN1, CS1 installation instructions: 108487.pdf
- 4 Post Open Rack installation instructions: 104554.pdf
- 2 Post Open Rack installation instructions: 069026.pdf

4.4.2.1 Physical Infrastructure Management

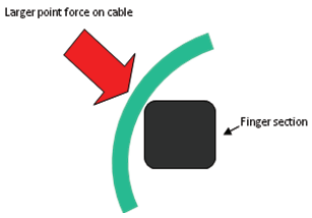
Cabling to and from the equipment in the cabinets or open 2 and 4 post racks must be managed. Of primary importance here is the care and management of modern high performance data cabling. The mechanical construction of the cable dictates much of its electrical performance. Therefore, it's necessary that any physical equipment such as cabinets, open 2 and 4 post racks have vertical and horizontal cable management.

- Cable performance is based on:
  - The locations of the twisted pairs inside the sheathing
  - The spacing of the twisted pairs, (most cable will have plastic structures to maintain spacing and create air gaps between twisted pairs)
  - The twist rate, is crucial in managing the capacitance, inductance and maintaining the high frequency performance of data cables.

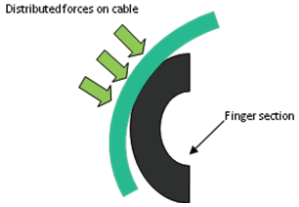
Screened Unshielded Twisted Pair (S/UTP, F/UTP, or SF/UTP) (a.k.a. FTP)

Proper bend radius control reduces the risk of performance degradation due to deformation of the structured cabling.

Poor bend radius control



Good bend radius control



4.4.2.2 Selection of Cabinets or Racks

Cabinets

- Select for maximum security for equipment
- Select for server applications or switch and patching applications
- Recommended for enterprise switches and server applications
- 2500Lb rating

4 Post racks

- Recommended for enterprise switches and server applications
- 2000Lb rating
- 2 Post 6 inch channel
- Suitable for enterprise switches
- 1500Lb rating

2 Post 3 inch channel

- Recommended for patching and smaller RU height equipment
- 1000Lb rating

4.4.2.3 Selection of Vertical and Horizontal Cable Managers

Cable capacity charts are available for all Panduit vertical and horizontal managers. Be sure to check them before selecting a catalog number.

- Select the horizontal and vertical managers for the system cable being installed.
- Select CEA-310 compliant

  Cat6A Managers
  - Bend radius to support Cat6A cable
  - Stated Cat6A compatibility.
    Typically deep with support for cable transition from the horizontal to vertical
  - Aesthetics suitable for the installation
  - Compatible with system wide components

  Cat5e and Cat6
  - Bend radius to support cable
  - Stated Cat5e and Cat6 compatibility.
    Support for cable transition from the horizontal to vertical
  - Aesthetics suitable for the installation

Compatible with system wide components

- Front and rear or front only
  - Select front and rear managers to provide support for back bone/horizontal cabling.
  - Select front only for installations where the backbone/horizontal cabling will be manually tied down
  - ccable should not be allow to pull on termination / punch downs
  - Select front only for 4 post rack installations where horizontal cable support in back is not needed.

Selecting Vertical Cable Managers

Vertical cable managers are available in a variety of widths. The widths vary based on the number of cables the manager will carry. Knowing the number of cables to be managed, select the vertical manager from the selection charts available from the manufacturer.

- Use cable capacity charts provided by the manufacturer
- Vertical Managers
  - Panduit recommends a fill ratio of 35%.
  - Allows space for slacking of cables and moves, adds and changes (MAC).
  - TIA -569-B covers tray capacities

Capacity Chart	Front Channel						Rear Channel		
	w/ Slack Spool			No Slack Spool					
Part Number*	Channel Area (In.²)	Cable Capacity** Cat. 6‡	Cat. 6A^	Channel Area (In.²)	Cable Capacity** Cat. 6‡	Cat. 6A^	Channel Area (In.²)	Cable Capacity** Cat. 6‡	Cat. 6A^
PRV6 (front/rear) PRVF6 (front only)	28.2	201	130	37.8	269	175	27.6 —	196 —	128 —
PRV8 (front/rear) PRVF8 (front only)	44.7	318	207	54.3	387	251	39.0 —	277 —	180 —
PRV10 (front/rear) PRVF10 (front only)	61.1	435	283	70.7	504	328	50.3 —	358 —	233 —
PRV12 (front/rear) PRVF12 (front only)	77.6	553	359	87.2	621	404	61.7 —	439 —	289 —
PRV15 (front/rear) PRVF15 (front only)	102.3	729	474	111.9	797	518	78.7 —	561 —	365 —

*For part numbers that fit in 8' rack, add "96" to end of part number.
‡ = .25" diameter; ^ = .31" diameter

**Capacities are based upon a fill rate of 35% to accommodate proper cable routing techniques.

Selecting and Cabling Horizontal Cable Managers

Horizontal cable managers are available in a variety heights based on Rack Units (RU). One RU is 1.75 inches. The height in RU and depth of a horizontal manager vary based on the number of cables the manager will carry. Knowing the number of cables to be managed, select the horizontal manager from the selection charts available from the manufacturer

- Horizontal managers are used with flat patch panels
- Use cable capacity charts provided by the manufacturer
- Common horizontal manager sizes are 1, 2,3, and 4 Rack Unit (RU)
- Horizontal Managers
  - Panduit recommends a fill ratio of 40%.
  - Allows space for moves adds and changes (MAC)
  - TIA -569-B covers tray capacities

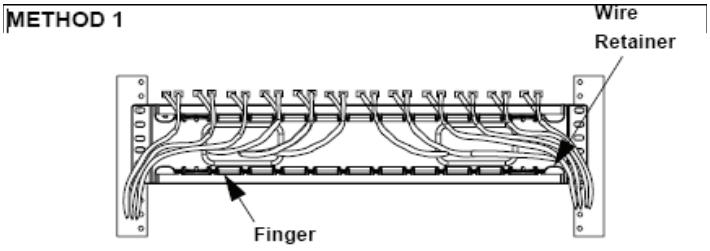
Cable Capacity Chart

	Category 6A (.298)		Category 6A (.289)		Category 6 (.250)		Category 5e (.187)		Fiber (3mm)	
Part Number	Front	Back	Front	Back	Front	Back	Front	Back	Front	Back
NM1	18	18	18	18	24	24	48	48	120	120
NM2	54	54	54	54	78	78	138	138	348	348
NM3	96	96	102	102	132	132	246	246	618	618
NM4	144	144	144	144	192	192	348	348	882	882
NMF1	12	—	24	—	48	—	120	—	—	—
NMF2	54	—	54	—	78	—	138	—	348	—
NMF3	96	—	102	—	132	—	246	—	618	—
NMF4	144	—	144	—	192	—	348	—	882	—

Cabling Techniques for Horizontal Managers

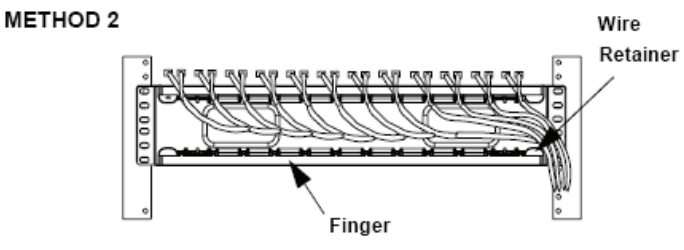
Method 1: Split each way

- Maximize the usage of manager cable capacity
- More cables if both end exits are used



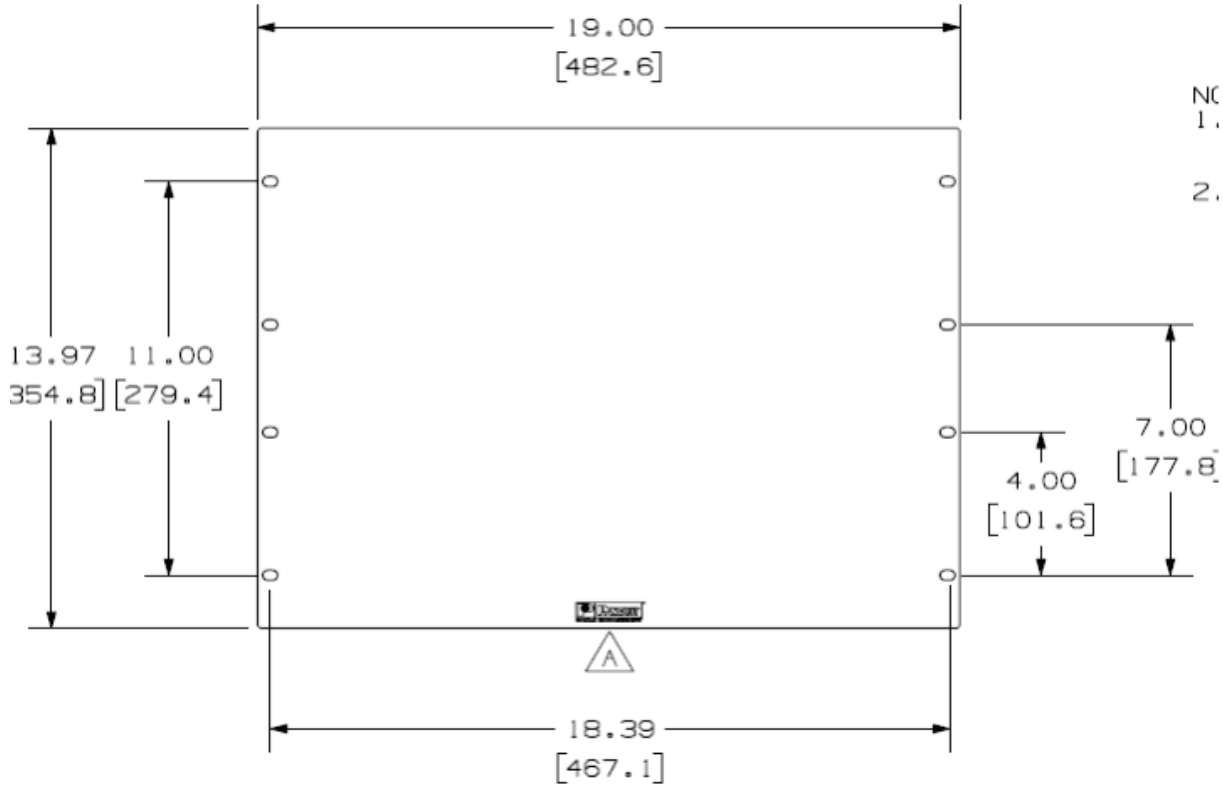
Method 2: All One Side

- One direction needed.
- One exit point for all cables may limit number of cables



4.4.2.4 Mounting Stratix Switches on DIN Rail or in Blacking Panels

Stratix switches or panel mount equipment not configured in the data center rack unit configuration can be mounted in open racks or enclosures by using available blanking panels. These panels are used to block off sections of open rack space. The template for the equipment being used can be transferred to the blanking panel. The necessary holes can be drilled into the panel for mounting.



4.4.2.5 Patching

For testability and organization of cables through moves, adds and changes, it would be recommended that for most manufacturing centered installation that flat patch panels and horizontal managers be used.

• Standard density patching
  - Use Flat Patch Panels and Horizontal Mangers
  - Up to 450 ports per rack plus switch
  - Moves, adds and changes (MAC) are occasional to frequent

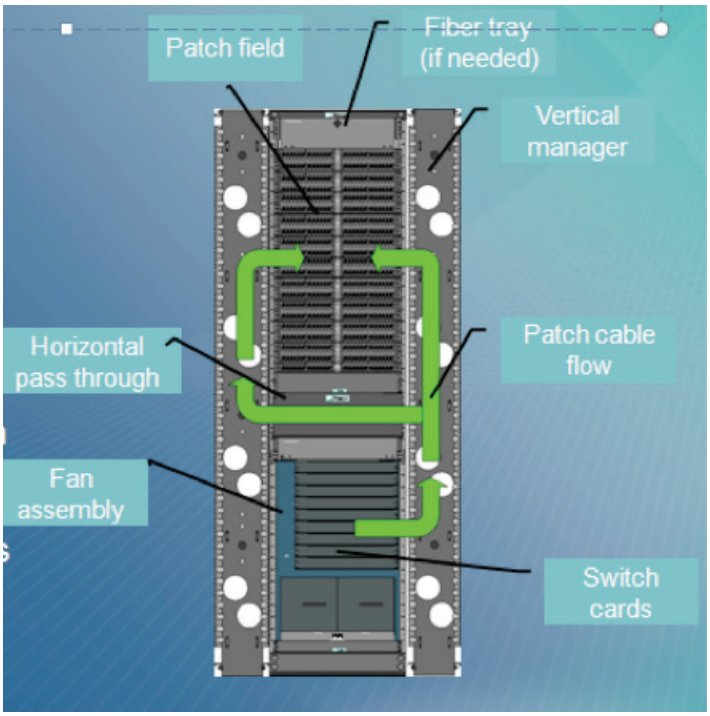
- Applications:
  - Leased office space
  - Cubicle based office space
  - Telecommunications rooms
  - Co-location sites

Table 4D-1. Dedicated Switch Rack and Patching Rack Recommendations

Recommended Application	Description	Maximum Ports	Moves Adds & Changes (MAC) frequency	Recommended Vertical	Recommended Horizontal	Rack
Rack cable management solution. Medium to high density patching.	Flat Patch Panels with horizontal managers.	500 to 700	MACs are occasional	PatchRunner PRV10 or PRVF10 Cat5e or Cat6, PRV12 or PRVF12 for Cat6A	FRME1 or 2 on top for fiber to switch*. PatchLink WMP1E, WMPH2E for Cat5e or Cat6. High Capacity NetManager NM2 or NMF2 for Cat6A	Select 4 Post CMR4P84,96 preferred for equipment and 2 post CMR19X84,96 for Patching
Rack cable management solution. Low to medium density patching	Flat Patch Panels with horizontal managers.	Up to 500	MACs are frequent	PatchRunner PRV8 or PRVF8 for Cat5e,Cat6. PRV10 or PRVF10 for Cat6A	FRME1 or 2 on top for fiber to switch*. PatchLink WMP1E or WMPH2E with Cat 5e or Cat 6. High Capacity NetManager NM1 or NMF1 with Cat6A.	
Rack Low density patching or patching with some active equipment Planning for future expansion	Flat Patch Panels with horizontal managers.	Under 350	MACs are frequent	PatchRunner PRV6 or PRVF6 for Cat5e,Cat6. PRV8 or PRVF8 for Cat6A	FRME1 or 2 on top for fiber to switch*. PatchLink WMPFSE, WMPLFSE, WMPLSE or WMPSE with Cat5e or Cat6. High Capacity NetManager NM2 or NMF2 with Cat6A.	

4.4.2.6 Thermal Management

Managing heat in switch or server installation depends on understanding the equipment being installed and how installation and cabling affects the equipments ability to stay cool. Some enterprise switches cool themselves by pulling air from front to back, others move air from side to side. The units that move air from side are more sensitive to cabling and the effect it has on the switches ability to move air. A common technique for switches that require side-to-side airflow switch is to cable “fan avoidance” which involves using a horizontal manager in the rack or cabinet to take cables around the fan tray.



4.4.2.7 Security

For security, cabinets provide the highest level of physical security to equipment and patch fields. For “Zone Cabling” enclosures, locking mechanisms, either built in or padlock are ready to secure its internals. In some instances the control room or area will have its own security policies, such as the following:

- Structuring the industrial network with smart switches or firewalls to prevent unauthorized access.
- Securing individual data ports
  Approval process that require enterprise IT personnel and manufacturing data personnel to approve patching changes.
- Using advanced patching management systems to authorize and verify any enterprise to manufacturing changes.

.

4.5 Pathway Systems

Pathway systems are critical factors because they give network stakeholders the ability to segregate, route, and protect communications cabling from other infrastructure elements and from adverse impacts from environmental hazards. Both overhead and under-floor systems are available to maintain the integrity of the fiber and copper cabling plant. Cable management accessories also ease the transition points from horizontal pathway spaces (overhead or under-floor) to an equipment rack or cabinet to vertical, maintaining proper bend radius and relieving cable strain.

Overall, pathway systems provide greater system flexibility and they contribute to improved industrial Ethernet network reliability. They also reduce the time and cost of installing your cabling infrastructure.

STANDARDS and CODES

GR-63 CORE (NEBS) Level 3

This Generic Requirements document (GR) presents minimum spatial and environmental criteria for all new telecommunications equipment used in Central Offices (COs) and other environmentally controlled telephone equipment spaces. This document provides only those requirements related to the physical aspects of equipment-building interfaces, including physical dimensions and environmental performance criteria. Issue 3 of GR-63 includes the following updated information:

- Fire resistance requirements incorporating new ANSI methods and specific carrier requirements
- An earthquake and vibration method for wall mounted products
- New criteria for equipment airflow patterns
- New criteria and test methods for thermal margin testing and operation with fan failure

ULC 2024A, Optical Fiber Cable Raceway

This standard covers the following types of optical fiber cable raceways and fittings designed for use with optical fiber cables in accordance with Article 770 of the National Electrical Code (NEC):

- Plenum - Evaluated for installation in ducts, plenums, or other spaces used for environmental air in accordance with the National Electrical Code as well as general purpose applications.
- Riser - Evaluated for installation in risers in accordance with the National Electrical Code as well as general purpose applications.
- General Use - Evaluated for general purpose applications only.

NEMA VE1 / VE2

National Electrical Manufacturers Association (partnered with CSA) Standard for Metal Cable Tray Systems / Installation Guidelines

IEC 61537

International Electrotechnical Contractors Standard for Cable Tray Systems and Cable Ladder Systems for Cable Management

IEC 60204

International Electrotechnical Contractors Standard for Safety of Machinery/Electrical Equipment with Machinery

NFPA 70 and 79

National Fire Protection Association's Standards.

4.5.1 Selection: Control Room

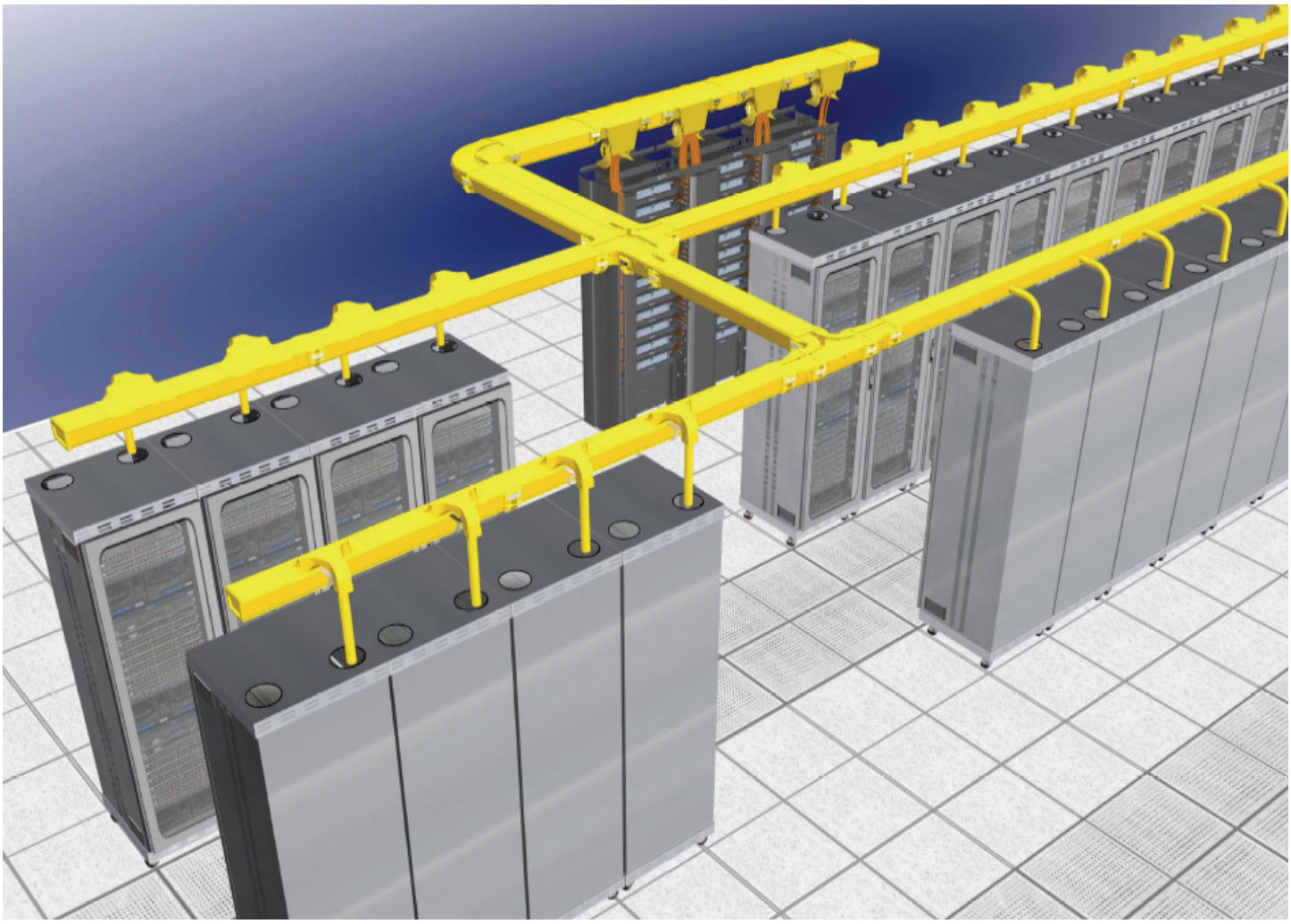


Figure 4.5-1. PANDUIT® FiberRunner® and FIBER-DUCT™ Routing System protects fiber optic cables from damage to support network reliability.

FiberRunner ® and FIBER-DUCT™ Routing Systems
The PANDUIT® FiberRunner® and FIBER-DUCT™ Routing Systems are overhead, solid pathway system designed specifically for fiber optic cables and patch cords. It is ideal for jacketed ribbon-style interconnect cables or small diameter distribution cables (6, 12, or 24 fiber cables) that do not have a separate strength member.

These systems consist of channels, fittings and brackets designed to segregate, route and protect fiber optic and high performance copper cabling. Typical applications include control rooms where cable is routed from distribution areas to equipment cabinets or racks (see Figure 4.5-1). They also can be deployed in approved under-floor installations.

Transition Point: from FiberRunner® Overhead Pathway to Equipment Rack/Cabinet
When routing distribution or interconnect cables from FiberRunner® pathways to an equipment rack or cabinet, an appropriately sized spill-out should be used to assist in the transition from the pathway to the equipment rack (see Figure 4.5-2). These spill-outs will also ensure proper cable management and maintain minimum cable bend radius. Some installations may use split corrugated loom tubing to provide extra protection for the cable transition between FiberRunner® pathway and the rack/cabinet (see Section 4.5.2).

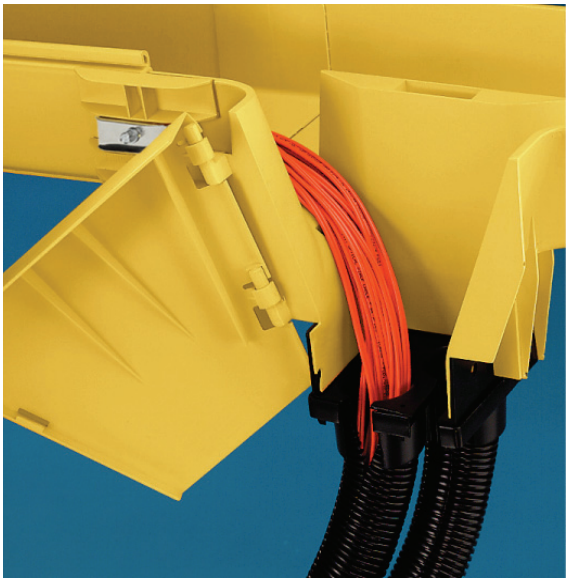


Figure 4.5-2. PANDUIT® FiberRunner® Overhead Pathway with Spill-Out

Once the fiber optic cables have transitioned from the FiberRunner® pathways into the rack or cabinet, it is critical to properly manage the cable routing prior to entry to the rack-mounted fiber enclosures or patch panels. This is best accomplished using PANDUIT® Tak-Ty® Hook & Loop Cable Ties. The use of PANDUIT® Pan-Ty® Cable Ties should be avoided with jacketed ribbon-fiber interconnect cables or small fiber-count distribution cable (6, 12, and 24 fiber cables) that do not have an internal strength member, as the cable tie could be over-tightened and crush the optical fibers. See Figure 4.5-3 for routing and tie-off point details, and Figures 4.5-4 and 4.5-5 for application examples.

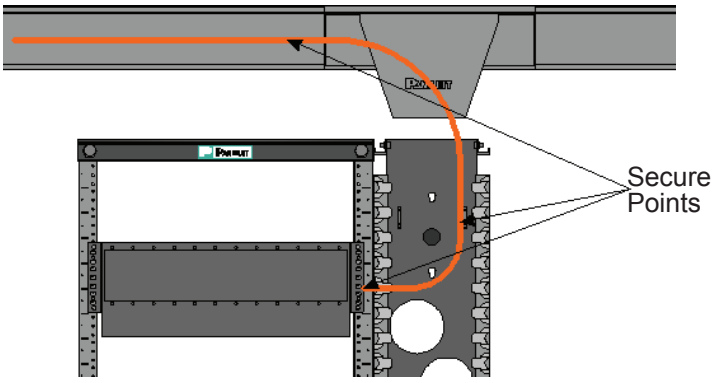


Figure 4.5-3. Schematic of FiberRunner® overhead pathway to rack/cabinet transition.

Figure 4.5-4. Example installation of FiberRunner® overhead pathway showing transition to 4-post racks. Cable is 12- fiber jacketed ribbon interconnect.

Figure 4.5-5. Example installation of FiberRunner® overhead pathway to PANDUIT® NetAccess™ cabinets. Cable is 12-fiber trunk. Note copper cabling installed in wire basket above FiberRunner® pathway system.

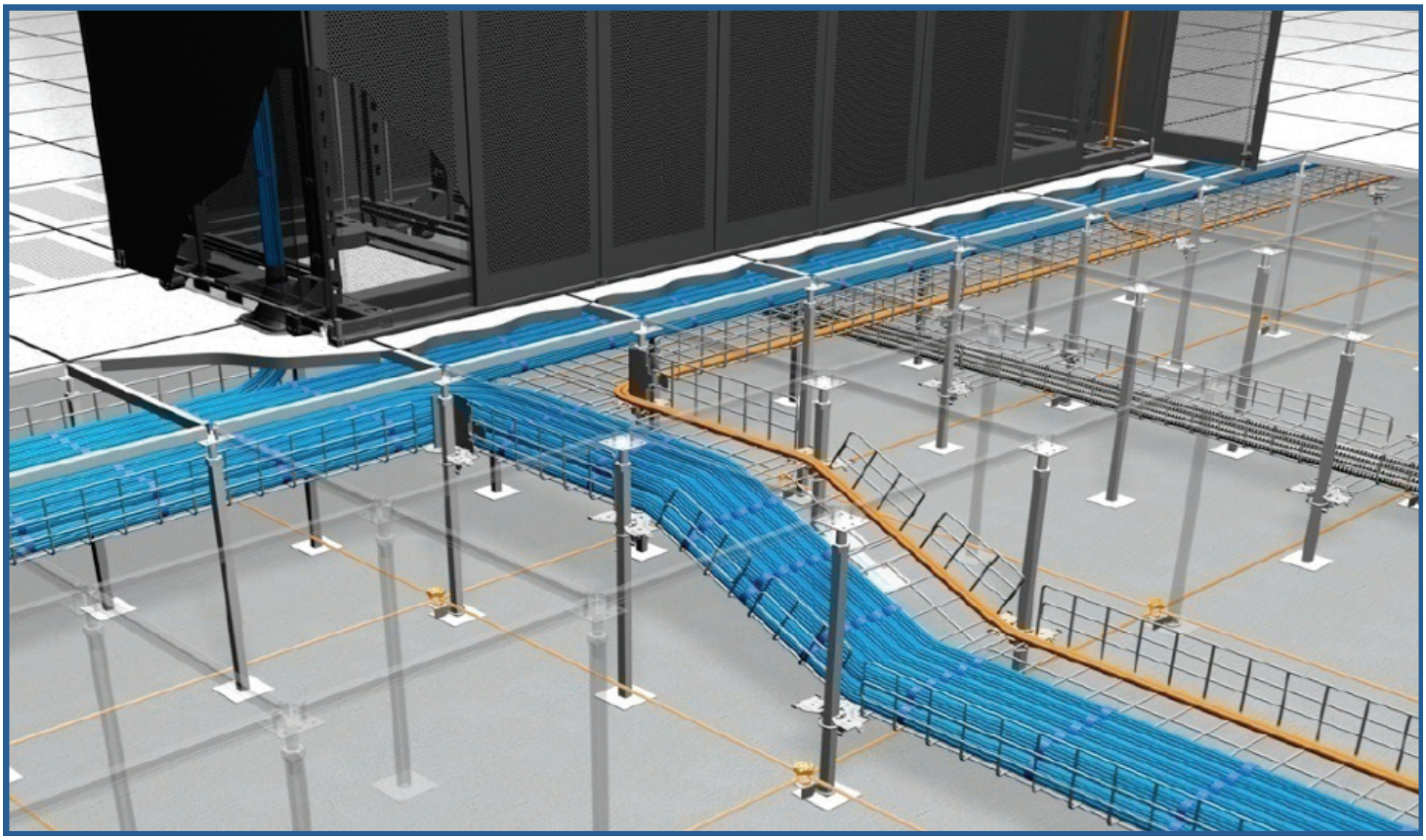


Figure 4.5-6. The PANDUIT® GridRunner ™ Under-floor Cable Routing System supports high-density applications and provides integral bonding to the mesh common bond network (MCBN), improving user safety and equipment protection.

GridRunner ™ Under-floor Cable Routing System

The PANDUIT® GridRunner ™ Under-floor Cable Routing System is a wire basket pathway designed to route and manage network data and power cabling beneath the raised floor in a control room or data center (see Figure 4.5-6). This innovative system supports high cable capacities, protects cables from damage to improve network performance, and is fully electrically bonded to facilitate proper grounding.

Transition Point: PANDUIT® GridRunner ™ Under-floor Pathway to Equipment Rack/Cabinet

In under floor pathway installations, high-performance copper cables and fiber optic trunk cables transition upward from the under floor pathway (PANDUIT® GridRunner ™ or similar) through an opening in a raised floor tile, and are secured on the vertical cable manager or rack/cabinet post with PANDUIT® Pan-Ty® Cable Ties. As the transition from under floor wire basket to the rack or cabinet is often an unguided route, cable transitions must flow gently and minimum bend radius allowances must be observed at all times (see Figure 4.5-7).

Some installations may use split corrugated loom tubing to provide extra protection for fiber optic cable transition from the under floor wire bask to the vertical cable manager and/or rack/cabinet post. In these installations, the corrugated loom tubing should be secured with PANDUIT® Tak-Ty® Hook & Loop Cable Ties to avoid over-tightening and crushing of the small-diameter fiber optic cables.

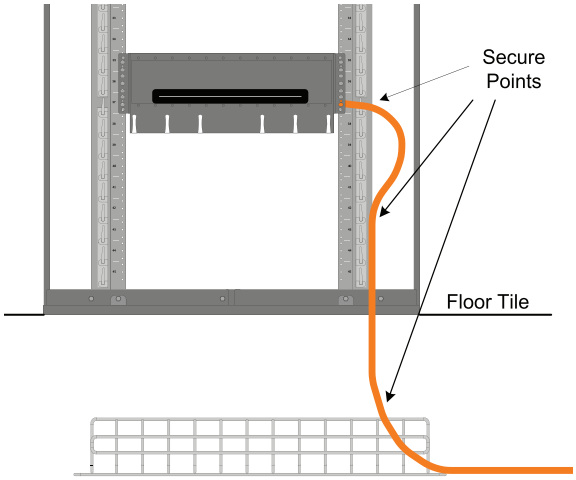


Figure 4.5-7. Schematic of under-floor wire basket pathway to rack/cabinet transition.

Figure 4.5-8. Example installation of fiber optic trunk cable transitioning from under floor pathway, through floor tile, to 2-post rack with PANDUIT® PatchRunner ™ vertical cable manager. Cable is 48- fiber pre-terminated trunk.

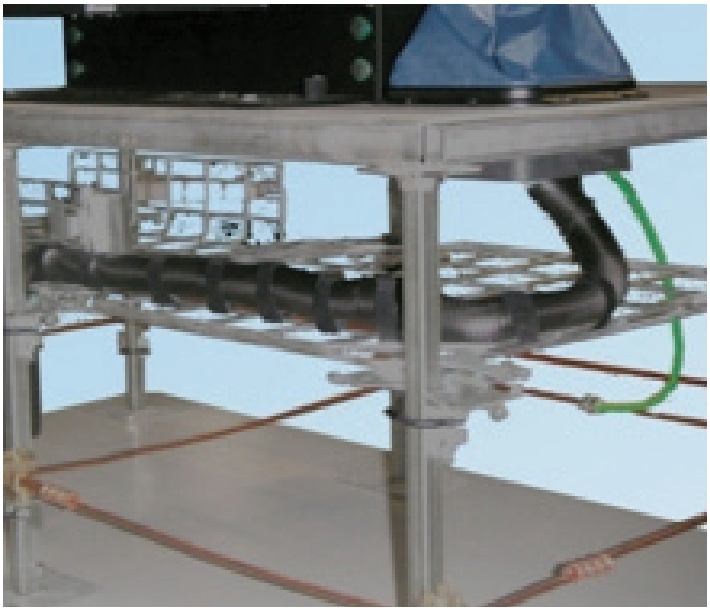


Figure 4.5-9. Example installation of GridRunner™ under floor wire basket pathway with 2-post rack and vertical cable manager. Cable is 12- fiber jacketed ribbon interconnect inside split loom tubing. Note PANDUIT® Cool Boot ™ Raised Floor Air Sealing Grommet (dark blue) installed to minimize air leakage through opening in raised floor tile.

Transition Point: Overhead Wire Basket to Equipment Rack/Cabinet

When routing distribution cable from an overhead wire basket pathway to an equipment rack or cabinet, it is recommended to utilize Panduit Waterfall Accessories to assist in the transition from the wire basket to the equipment rack (see Figure 4.5-10). These accessories will also assist with managing of the cable bend radius.

Once cabling has transitioned from the overhead pathway into the rack or cabinet, it is critical to "tie-off" and strain relieve the cable to the vertical cable manager or rack/cabinet vertical post prior to cable break-out and/or cable entry to the rack-mounted fiber enclosures or patch panels. See Figure 4.5-11 detailing the routing and tie-off points, and Figures 4.5-12 and 4.5-13 for application examples.

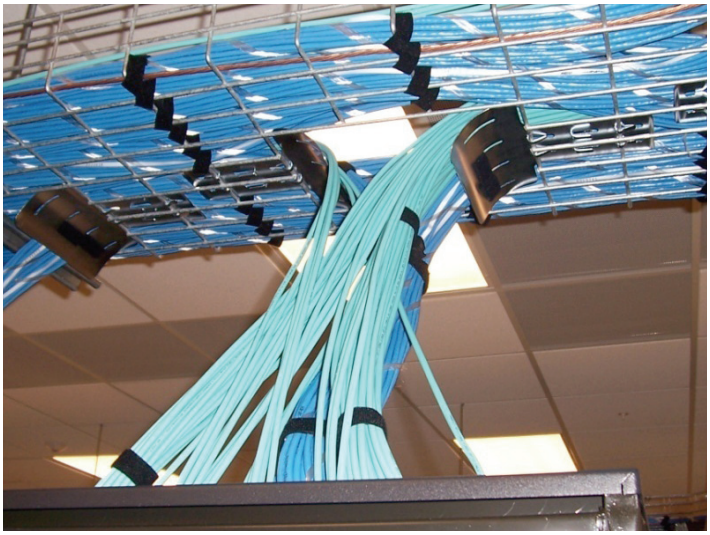


Figure 4.5-10. Overhead wire basket to four-post rack transition.

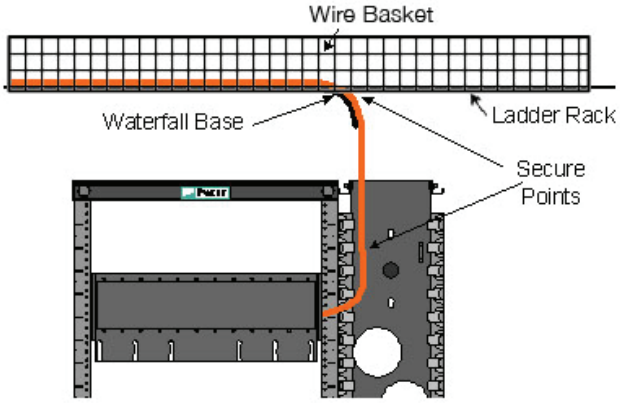


Figure 4.5-11. Schematic of overhead wire basket to rack/cabinet transition

Figure 4.5-12. Example installation of transition from overhead wire basket. Cable is 24- fiber trunk routing down to 4-post rack. Note use of PANDUIT® Tak-Ty® Hook & Loop Cable Ties to secure and manage cable.

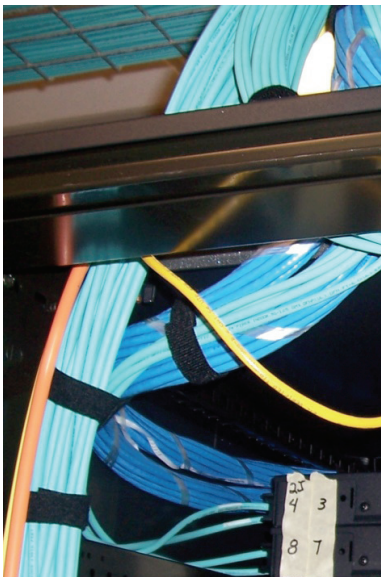


Figure 4.5-13. Example installation of overhead wire basket to 4-post rack transition. Cable is 24- fiber trunk routing along vertical rack post to FCE1 enclosure. Note use of PANDUIT® Tak-Ty® Hook & Loop Cable Ties to secure trunk cable to vertical rack post.

Transition Point: Overhead Ladder Rack to Equipment Rack/Cabinet

When routing distribution cable from an overhead ladder racking system to an equipment rack or cabinet, it is recommended to utilize *PANDUIT* Waterfall Accessories to assist in the transition from the ladder rack to the equipment rack (see Figure 4.5-14). These accessories will also assist with managing of the cable bend radius.

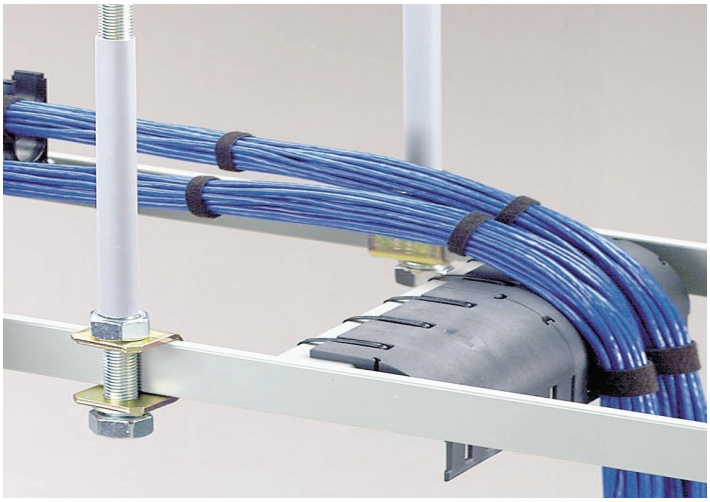


Figure 4.5-14. Overhead ladder rack with PANDUIT Waterfall Accessory

Once the cable has transitioned from the overhead pathway into the rack or cabinet, it is critical to "tie-off" and strain relieve the cable to the vertical cable manager or cabinet vertical post prior to cable break-out and/or cable entry to the rack-mounted fiber enclosures or patch panels. See Figure 4.5-15 detailing the routing and tie-off points, and Figures 4.5-16 and 4.5-17 for application examples.

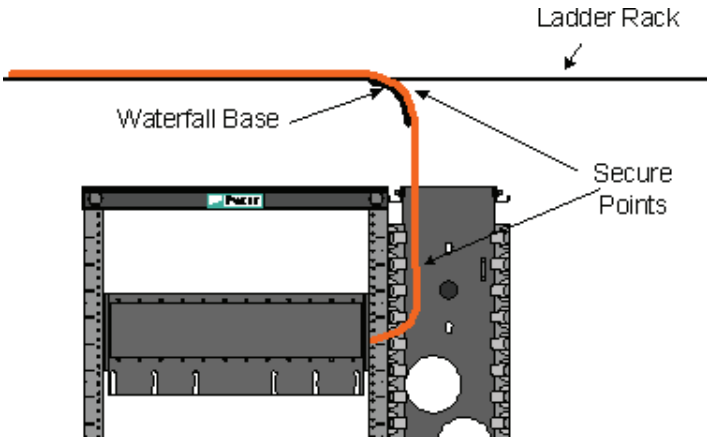


Figure 4.5-15. Schematic of overhead ladder rack to rack/cabinet transition.

Figure 4.5-16. Example installation of overhead ladder rack to two-post rack transition with PANDUIT® PatchRunner ™ Vertical Cable Manager. Cable is 48-fiber trunk routing through PRV12 vertical cable manager into FCE4 enclosure. Note use of PANDUIT® Pan-Ty® Cable Ties to secure trunk cable to vertical cable manager.

Figure 4.5-17. Example installation of overhead ladder rack to two-post rack transition with PANDUIT® PatchRunner ™ Vertical Cable Manager. Cable is 12-fiber trunk routing through PRV12 vertical cable manager into FCE4 enclosure. Note use of PANDUIT® Tak-Ty® Hook & Loop Cable Ties to secure trunk cable to vertical cable manager.

4.5.2 Selection: Plant Floor

Plant floor pathways formerly required extensive cable tray or conduit arrangements. With industrial Ethernet networks, it is much more common and economical to run small groups of Ethernet cabling between control rooms or enclosures using J-Hooks to secure cable or fiber media from the ceiling joists.

The PANDUIT® J-Pro™ Cable Support System is designed to provide an economical cable system to route communication cable along horizontal pathways, whether above suspended ceilings or under raised floors, or across the ceiling of a factory floor. The J-Hook is made of strong and durable non-metallic material to prevent cables from coming in contact with metal, and the low friction nylon surface facilitates pulling cable (and eliminates "shiners" created by metallic hooks).

This system provides complete horizontal and vertical 1" bend radius control, preventing pinch points that could cause damage to cable, and is available in four sizes (¾", 1-5/16", 2" & 4" bundle capacities). The large channel size allows the use of **TAK-TY® Hook & Loop Cable Ties** to retain and manage the cable bundle.

A variety of mounting options, including pre-riveted mounting assemblies, provide the ability to attach to walls, ceilings, beams, threaded rods, drop wires, and under floor supports to meet the requirements of a variety of applications.

Corrugated loom tubing also can be used to protect fiber optic media in light industrial environments. This tubing creates a cable pathway that is easy to pull through, and is available in a variety of diameters, materials, and in split or solid versions. This tubing can be suspended from J-Pro cable supports as a pathway solution.

4.5.3 Installation

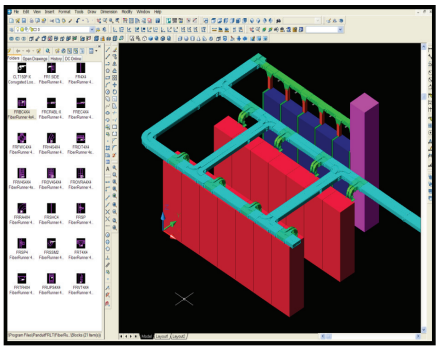
FiberRunner ®	GridRunner ™
1. Configure the pathway runs to the cabinets or racks.	1. Configure the pathway runs to the cabinets or racks.
2. Design logical routes that optimize cable lengths and minimize turns.	2. Design logical routes that optimize cable lengths and minimize turns.
3. Snap-together assembly reduces installation time: • QuickLock Coupler provides fast mechanical assembly • No tools required to make reliable connection • Brackets attach system to common infrastructure elements (ladder rack, strut, etc.) • Loosen clips, slide into position, and re-tighten to mount channel to bracket.	3. Drop-in assembly reduces installation time: • Position and install pedestal support bracket on pedestals. • Secure one captured fastener. • Drop wire basket section between stringers. • Secure wire baskets to pedestal support brackets with pedestal clamp.
4. Size the main runs and branches for the anticipated fills. Generally, plan the initial cable channel fill at a 40% fill density.	4. Size the main runs and branches for the anticipated fills. Generally, plan the initial cable channel fill at a 40% fill density.
5. Determine the amount of cables to be spilled out into racks/cabinets and select choice of spill-over or transition accessory.	5. Determine the amount of cables to be spilled out into racks/cabinets and select choice of spill-over or transition accessory.

4.5.4 Documentation

FiberRunner Design tools

Panduit provides design tools for AutoCAD and VISIO that speed system design, specification and documentation.

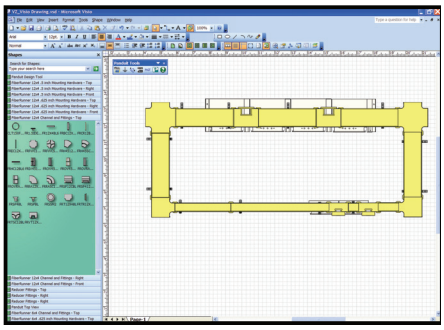
AUTOCAD**



FiberRUNNER™ Design Tool for AutoCAD** includes:

- **Available on free CD - SA-FRCD02**
- **Drag & Drop**
- **Design in 2D or 3D**
- **BOM Generator**
- **Allows FIBERRUNNER to be incorporated into working drawings**

VISIO*



*VISIO** Layout Tool includes:

- **Free download from panduit.com**
- **Drag & Drop**
- **BOM Generator**
- **Great for incorporating visuals into proposals**

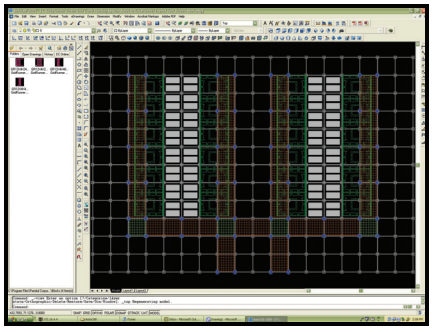
**VISIO is a registered trademark of Microsoft Corporation in the United States and/or other countries.*

***AutoCAD and AutoCAD LT are registered trademarks of Autodesk, Inc.*

GridRunner Design tools

Panduit provides design tools for AutoCAD and VISIO that speed system design, specification and documentation.

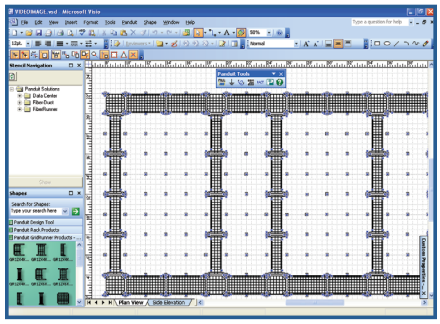
AUTOCAD**



GRIDRUNNER™ Design Tool for AutoCAD** includes:

- **Drag & Drop Functionality**
- **Ability to design in 2D and 3D**
- **Versions compatible with AutoCAD** and AutoCAD LT****
- **Automated BOM Generator**
- **Available on CD, SA-FRCD02 free through Customer Service**

VISIO*



Data Center VISIO* Layout Tool includes:

- **Drag & Drop Functionality**
- **Ability to design in 2D (stencils for three different views are provided)**
- **Automated BOM Generator**
- **Free download from: www.panduit.com/gridrunner/visio**

**VISIO is a registered trademark of Microsoft Corporation in the United States and/or other countries.*

***AutoCAD and AutoCAD LT are registered trademarks of Autodesk, Inc.*

4.6 Wire Management

One of the most critical layers for the physical infrastructure is the management of wires encountered throughout the various environments. The physical infrastructure must be specified with enough support, environmental rating, and protection features to ensure that components will perform consistently and reliably. Wire management can often times be overlooked, but as the industry transitions to more integration of sensors and automation components out onto machines and into harsher environments, it will be an essential area for consideration.

Environmental factors in the space can range from extreme cold or hot temperatures outdoors or in a process line to humidity. In addition, chemical exposure can degrade insulation to vibration or shock that can cause mechanical connection failures. The MICE rating system allows these factors to be categorized and analyzed for mitigation. Wires and cables must be protected in different ways within these various environments. Cable bend radius control and excessive deformation through over tensioning of cable ties and mounts are additional items you need to consider.

STANDARDS and CODES

TIA/EIA-568-B

TIA/EIA-568-B (Commercial Building Telecommunications Cabling Standard) covers structured cabling systems (both balanced copper cabling and fiber optic cabling) for commercial buildings, and between buildings in campus environments. The bulk of the standards define cabling types, distances, connectors, cable system architectures, cable termination standards and performance characteristics, cable installation requirements, and methods of testing installed cable.

TIA/EIA-569-A

TIA/EIA-569-A (Commercial Building Standards for Telecommunications Pathways and Spaces) provides design specifications and guidance for building facilities relating to telecommunications cabling systems and components. Bend radius control of conductors also warrant consideration in this area.

UL 1565 – Wire Positioning Devices

This standard applies to those metallic and nonmetallic devices used for positioning – which may include bundling and securing – or to a limited extent supporting cable, wire, conduit, or tubing of a wiring system in electrical installations, to reduce the risk of fire, electric shock, or injury to persons. This standard applies to, but is not limited to, cable ties, cable tie mounting blocks, cable clamps, cable and conduit clips, and non-raceway ducts.

ANSI/NFPA 70 - National Electrical Code

This Code covers the installation of electrical conductors, equipment, and raceways; signaling and communications conductors, equipment, and raceways; and optical fiber cables and raceways for installations used by the electric utility, such as office buildings, warehouses, garages, and machine shops.

UL 94 – Tests for Flammability of Plastic Materials for Parts in Devices and Appliances

These requirements cover tests for flammability of polymeric materials used for parts in devices and appliances. They are intended to serve as a preliminary indication of their acceptability with respect to flammability for a particular application.

UL 224 VW1 – Vertical Wire Flame Test

Samples of fully recovered tubing are placed over a length of fine spring steel music wire. The test requires the precise placement of a controlled flame that contacts the heat shrink tubing. The flame is applied in five 15-second intervals with a time period between applications. If the flame extinguishes immediately after the first flame removal, subsequent flame applications are made to the tubing. Duration of specimen flaming is noted. A piece of surgical cotton is placed under the specimen. If a flaming or glowing piece of tubing drips and ignites the cotton, this is also noted.

4.6.1 Selection

4.6.1.1 Abrasion Protection

Full Coverage. Choose from heat shrink, braided sleeving, CLT, Pan-Wrap™ Split Harness Wrap, spiral wrap, and grommet edging. All product lines are available in various sizes and materials to meet the application needs.

Selecting the Appropriate Heat Shrink. Generally, the largest tube that shrinks down tightly onto an object should be chosen. This allows the heat shrink tubing maximum stress relief and this will yield the longest service life.

Example: *A multi-conductor cable needs to be covered with HSTT Type Heat Shrink. The area to be covered has a measured outside diameter of .700" (17.8mm). The two possibilities are HSTT75-48-5 and HSTT100-48-5.*

Part Number	Expanded I.D. In. (mm)	Recovered I.D. In. (mm)
HSTT75-48-5	.750 (19.0)	.375 (9.5)
HSTT100-48-5	1.00 (25.4)	.500 (12.7)

The proper choice is HSTT100-48-5 since the tube will recover more than HSTT75-48-5. The HSTT75-48-5 and HSTTAF100-48-5 will fit over the .700" (17.8mm) outside diameter; however, this is not the proper choice since the recovered I.D. is smaller than the HSTTAF100-48-5. In general, heat shrink should recover at least 10% - 20% to reduce stress and yield the longest service life.

Table 4.6-1 indicates the approximate outside diameter of various electrical wires. Utilize this table when selecting abrasion protection or cable accessory products, such as heat shrink or fixed diameter cable clamps.

	Approximate Wire Outside Diameter In. (mm)			
Size	With TF Insulation	With THW Insulation	With TW Insulation	With TFN/THHN/ THWN Insulation
18 AWG	.11 (2.8)	.11 (2.8)	.11 (2.8)	.09 (2.3)
16 AWG	.12 (3.0)	.12 (3.0)	.12 (3.0)	.10 (2.5)
14 AWG	.13 (3.3)	.16 (4.1)	.16 (4.1)	.10 (2.5)
12 AWG	.15 (3.8)	.18 (4.6)	.18 (4.6)	.12 (3.0)
10 AWG	.17 (4.3)	.20 (5.1)	.20 (5.1)	.15 (3.8)
8 AWG	.24 (6.1)	.28 (7.1)	.28 (7.1)	.22 (5.6)
6 AWG	.32 (8.1)	.32 (8.1)	.32 (8.1)	.26 (6.6)
4 AWG	.37 (9.4)	.37 (9.4)	.37 (9.4)	.33 (8.4)
3 AWG	.40 (10.2)	.40 (10.2)	.40 (10.2)	.36 (9.1)
2 AWG	.43 (10.9)	.43 (10.9)	.43 (10.9)	.39 (9.9)
1 AWG	.51 (12.9)	.51 (12.9)	.51 (12.9)	.45 (11.4)
1/0	.55 (14.0)	.55 (14.0)	.55 (14.0)	.49 (12.4)
2/0	.59 (15.0)	.59 (15.0)	.59 (15.0)	.54 (13.7)
3/0	.65 (16.5)	.65 (16.5)	.65 (16.5)	.59 (15.0)
4/0	.70 (17.8)	.70 (17.8)	.70 (17.8)	.65 (16.5)
250 MCM	.79 (20.1)	.79 (20.1)	.79 (20.1)	.72 (18.3)
300 MCM	.84 (21.3)	.84 (21.3)	.84 (21.3)	.77 (19.6)
350 MCM	.89 (22.6)	.89 (22.6)	.89 (22.6)	.82 (20.8)
400 MCM	.94 (23.9)	.94 (23.9)	.94 (23.9)	.87 (22.1)
500 MCM	1.03 (26.2)	1.03 (26.2)	1.03 (26.2)	.95 (24.1)
600 MCM	1.14 (29.0)	1.14 (29.0)	1.14 (29.0)	1.06 (26.9)
700 MCM	1.21 (30.7)	1.21 (30.7)	1.21 (30.7)	1.13 (28.7)
750 MCM	1.25 (31.8)	1.25 (31.8)	1.25 (31.8)	1.16 (29.5)
800 MCM	1.28 (32.5)	1.28 (32.5)	1.28 (32.5)	1.20 (30.5)
900 MCM	1.34 (34.0)	1.34 (34.0)	1.34 (34.0)	1.26 (32.0)
1000 MCM	1.40 (35.6)	1.40 (35.6)	1.40 (35.6)	1.32 (33.5)
1250 MCM	1.58 (40.1)	1.58 (40.1)	1.58 (40.1)	
1500 MCM	1.70 (43.2)	1.70 (43.2)	1.70 (43.2)	
1750 MCM	1.82 (46.2)	1.82 (46.2)	1.82 (46.2)	
2000 MCM	1.92 (48.8)	1.92 (48.8)	1.92 (48.8)	

Figure 4.6-1. Approximate Wire Outside Diameter Chart

Building an Abrasion Solution

Braided Sleeving	Highly flexible open weave for abrasion protection; fray resistant available
Corrugated Loom Tubing	Provides protection for cables; slit or solid wall
Grommet Edging	Protect cables from sharp edges; solid or slotted; adhesive lined available
Heat Shrink (4: 1)	Heatshrink insulates and protects cables; 4:1 shrink ratio for terminated wires; adhesive lined
Heat Shrink Thin Wall	Standard thin wall heatshrink insulates and protects cables; 2:1 shrink ratio
PAN-WRAP™ Split Harness Wrap	Maintains uniform bundle with improved flexibility and abrasion protection
Spiral Wrap	Harness multiple cables into a single bundle while allowing breakouts; multiple colors available for identification purposes

4.6.1.2 Cable Ties and Installation Tooling

Cable tie products are used to bundle, mount and identify in countless indoor, outdoor and harsh environment applications. Panduit offers a wide breadth of cable tie designs, sizes and specialty materials to address customer wire management challenges throughout the industrial space.

Cable tie installation tools range from high speed automatic systems to hand operated tools; all with consistent, reliable performance that provide a flush cable tie cut-off limiting exposure to sharp edges. Panduit installation tools are light weight, ergonomic, designed for ease of use and reduce repetitive stress injuries. These tools also provide speed in installation to reduce installed cost.

Control Panel and On-Machine Applications. Environmental factors on the factory floor can range from extreme cold or hot temperatures to humidity or chemical exposure that can degrade insulation, to vibration or shock that can cause mechanical failures of connections.

The *PANDUIT* Material Selection Guide (Table 4.6-2) will help you select the most appropriate specialty cable tie material based on industrial application / MICE requirements. Table 4.6-3 lists recommended *PANDUIT* products for Control Panel and On-Machine Applications.

Figure 4.6-2a. PANDUIT Cable Tie Material Selection Guide

Recommendation Legend	Highest	High	Acceptable	Low	Lowest

	Material	Test Method	Nylon 6.6	Weather Resistant Nylon 6.6	Impact Modified Weather Resistant Nylon 6.6	Heat Stabilized Nylon 6.6	Heat Stabilized Nylon 6.6	Heat Stabilized Weather Resistant Nylon 6.6
	Color	—	Natural (other colors available)	Black	Black	Black	Natural	Black
	Part Number Suffix (Material Designation)	—	No Suffix	0	0	30	39	300
Mechanical Properties	Tensile @ Yield @ 73°F (psi)	ISO 527	12000	12000	9700	12000	12000	12000
	Water Absorption (24 Hours)	ASTM D570	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%
	Radiation Resistance (Rads)	—	1 x 10^5	1 x 10^5	1 x 10^5	1 x 10^5	1 x 10^5	1 x 10^5
	Weathering Life Expectancy (Years) / UV Resistance	—	1-2	7-9	7-9	4-5	1-2	7-9
	Impact Resistance	—						
Chemical Resistance	Salts	—						
	Hydrocarbons (Gas, Oil, Lubricants)	—						
	Chlorinated Hydrocarbons	—						
	Acids	—						
	Bases	—						
	Acid Rain	—						
Thermal Properties	Max. Continuous Use Temperature	UL 746B	185°F 85°C	185°F 85°C	185°F 85°C	239°F 115°C	239°F 115°C	212°F 100°C
	Min. Application Use Temperature	EN 50146	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C
	Flammability Rating	UL 94	V-2	V-2	HB	V-2	V-2	V-2
	Low Smoke	ASTM E662	PASS	PASS	PASS	PASS	PASS	PASS
	Oxygen Index	BS ISO 4589	28	28	—	28	28	28
	Halogen-Free	IEC 60754-2	Yes	Yes	Yes	Yes	Yes	Yes
	Burning Fume Toxicity	BSS-7239	PASS	PASS	PASS	PASS	PASS	PASS
	Heat Deflection Temperature @ 1.8 Mpa	ASTM D648 ISO 75 -1/-2	158¤F 70¤C	158¤F 70¤C	145¤F 63¤C	158¤F 70¤C	158¤F 70¤C	158¤F 70¤C

Table 4.6-2b PANDUIT Cable Tie Material Selection Guide (continued)

	Material	Test Method	Flame Retardant Nylon 6.6	Flame Retardant Nylon 6.6	Weather Resistant Nylon 12	Polypro-pylene	Weather Resistant Polypro-pylene	TEFZEL•
	Color	—	Black	Natural Ivory	Black	Green	Black	Aqua Blue
	Part Number Suffix (Material Designation)	—	60	69	120	109	100	76
Mechanical Properties	Tensile @ Yield @ 73°F (psi)	ISO 527	11000	11000	6700	4100	4100	7500
	Water Absorption (24 Hours)	ASTM D570	1.1%	1.1%	0.3%	0.1%	0.1%	<0.03%
	Radiation Resistance (Rads)	—	1×10^5	1×10^5	3.5×10^6	1×10^6	1×10^6	2×10^8
	Weathering Life Expectancy (Years) / UV Resistance	—	1-2	1-2	12-15	1	7-9	>15
	Impact Resistance	—						
Chemical Resistance	Salts	—						
	Hydrocarbons (Gas, Oil, Lubricants)	—						
	Chlorinated Hydrocarbons	—						
	Acids	—						
	Bases	—						
	Acid Rain	—						
Thermal Properties	Max. Continuous Use Temperature	UL 746B	212°F 100°C	212°F 100°C	194°F 90°C	239°F 115°C	239°F 115°C	338°F 170°C
	Min. Application Use Temperature	EN 50146	-40°F -40°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C
	Flammability Rating	UL 94	V-0	V-0	HB	HB	HB	V-0
	Low Smoke	ASTM E662	PASS	PASS	—	—	—	—
	Oxygen Index	BS ISO 4589	34	34	—	—	—	30
	Halogen-Free	IEC 60754-2	Yes	Yes	Yes	Yes	Yes	No
	Burning Fume Toxicity	BSS-7239	PASS	PASS	—	—	—	—
	Heat Deflection Temperature @ 1.8 Mpa	ASTM D648 ISO 75 -1/-2	154°F 68°C	154°F 68°C	122°F 50°C	122°F 50°C	122°F 50°C	—

Figure 4.6-2c. PANDUIT Cable Tie Material Selection Guide (continued)

	Material	Test Method	HALAR®	PEEK	Metal Detectable Nylon	Metal Detectable Polypro-pylene	Weather Resistant Acetal	Flame Retardant TPU
	Color	—	Maroon	Translucent Brown	Blue	Blue	Black	Black
	Part Number Suffix (Material Designation)	—	702Y	71	86	186	N/A	20
Mechanical Properties	Tensile @ Yield @ 73°F (psi)	ISO 527	7000	15200	—	—	6500	4350
	Water Absorption (24 Hours)	ASTM D570	<0.05%	0.5%	1.2%	0.1%	<0.45%	0.25%
	Radiation Resistance (Rads)	—	2×10^8	1×10^8	—	1×10^5	6×10^5	—
	Weathering Life Expectancy (Years) / UV Resistance	—	>15	1-2	—	1	>20	7-9
	Impact Resistance	—						
Chemical Resistance	Salts	—						
	Hydrocarbons (Gas, Oil, Lubricants)	—						
	Chlorinated Hydrocarbons	—						
	Acids	—						
	Bases	—						
	Acid Rain	—						
Thermal Properties	Max. Continuous Use Temperature	UL 746B	302°F 150°C	500°F 260°C	185°F 85°C	239°F 115°C	185°F 85°C	122°F 50°C
	Min. Application Use Temperature	EN 50146	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-76°F -60°C	-40°F -40°C
	Flammability Rating	UL 94	V-0	V-0	HB	HB	HB	V-0
	Low Smoke	ASTM E662	—	PASS	—	—	PASS	—
	Oxygen Index	BS ISO 4589	52	35	—	—	—	—
	Halogen-Free	IEC 60754-2	No	Yes	Yes	Yes	Yes	Yes
	Burning Fume Toxicity	BSS-7239	—	—	—	—	—	—
	Heat Deflection Temperature @ 1.8 Mpa	ASTM D648 ISO 75 -1/-2	149°F 65°C	313°F 156°C	145°F 63°C	122°F 50°C	147°F 64°C	—

Figure 4.6-3. Cable Ties Recommended for Control Panel and On-Machine Applications

PANDUIT Part #	Description	PANDUIT Part #	Description
PLT**-M	PAN-TY® Cable Tie - Nylon 6.6, 1”-4” Bundle Diameter (M,I,S Cross sections)	PLT**-M0	PAN-TY® Cable Tie - Weather Resistant Nylon 6.6, 1”-4” Bundle Diameter, (M,I,S Cross sections)
PLC2S-S10-M*	PAN-TY® Clamp Tie - Nylon 6.6, 2” Bundle Diameter, S Cross section (Heat stabilized also available)	PLWP**-**	PAN-TY® Push Mount Tie - Weather Resistant Nylon 6.6, 1”-2” Bundle Diameter, (M,S Cross sections), (Heat stabilized and weather resistant also available)
PLM2S-M*	PAN-TY® Marker Tie - Nylon 6.6, 2” Bundle Diameter, S Cross section (Heat stabilized also available)	PFX-0	Black Marking Pen
PLT**-M30	PAN-TY® Cable Tie - Heat Stabilized Nylon 6.6,1”-4” Bundle Diameter (M,S Cross sections)	PLT**-C186	PAN-TY® Cable Tie - Metal Detectable Polypropylene, 1”-4” Bundle Diameter , (M,S Cross sections)
PLT**-M109	PAN-TY® Cable Tie - Polypropylene, 1”-4” Bundle Diameter (M,S,H Cross sections)	PLT**-*76	PAN-TY® Cable Tie - Tefzel, 1”-4” Bundle Diameter, (M,I,S,H Cross sections)
PLT*S-M702Y	PAN-TY® Cable Tie - HALAR, Plenum Rated, Flame Retardant, 2”-3” Bundle Diameter, S Cross section	GTS	Cable Tie Tool - Manual Install-SM,M,I,S
GTH	Cable Tie Tool - Manual Install-S,HS,LH,H	PTH	Cable Tie Tool - Pneumatic Install-S,HS,LH,H

Control Room, Network Distribution, and Zone Cabling Enclosure Applications. PANDUIT has a comprehensive offering of cable ties that deliver reliability by protecting against over tensioning of high performance fiber and copper cables. Table 4.6-4 lists recommended PANDUIT products for control room, network distribution, and zone cabling Enclosure applications.

• TAK-TY® Hook & Loop Cable Ties. The Hook & Loop fabric maintains network data integrity by protecting against over-tensioning, unraveling and de-lamination. These ties are adjustable, releasable and reusable up to hundreds of times – ideal for applications requiring frequent moves, adds or changes. A wide range of designs, sizes and colors provides flexibility and an aesthetically pleasing appearance. Also available is custom printing text and logos on Hook & Loop ties for identification and promotional purposes.

• Elastomeric Cable Ties. The Elastomeric Cable Tie is an innovative design with elastic material that provides safe and reliable cable bundling preventing over tensioning. The soft material has no sharp edges, promoting worker safety. These flexible ties cinch the cable bundle preventing lateral movement along the bundle. The UL94V-0 flammability rating and Halogen free construction ensures compliance with environmental and industry requirements. The releasable design accommodates frequent moves, adds and changes. These ties are weather and UV resistant, suitable for bundling sensitive fiber and copper cables in both outdoor as well as indoor applications.

• TAK-TAPE™ Hook & Loop Rolls. Strong, low profile material is thin and flexible to quickly wrap around bundles. TAK-TAPE™ is a cost-effective solution for general purpose bundling. The continuous rolls can be cut to size, and the fabric is adjustable, releasable and reusable.

• ULTRA-CINCH™ Hook & Loop Ties. Exclusive Hook & Loop material with hooks and loops on same side allows user to secure a greater range of bundle diameters, including smaller bundles. A low profile contoured cinch ring reduces overall bundle size. These ties are adjustable, releasable and reusable hundreds of times. A tapered tip speeds installation and a strong brass grommet on select styles assure reliable installations that resist pullout. A wide range of colors is available for color-coding requirements.

PANDUIT's Cable Bundle Organizing Tool efficiently arranges up to 24 data cables to optimize bundle size and improve installed appearance prior to installing Panduit hook and loop or Elastomeric cable ties. This user friendly tool accommodates a wide range of cable diameters and reduces cable bundling time by 50% compared to manual methods.

Another important product is the Power Outlet Unit Plug Retention Device which reduces the risk of equipment downtime due to accidental plug disconnection from select PANDUIT power outlet units. This product helps manage risk in network installations by enabling safe and secure power connections for greater reliability of the physical infrastructure. The retention device is compatible with IEC 320 C13/C14 outlet socket and plug models, accommodating various plug strain relief heights and cable insulation diameters. The releasable design is UL 94V-0 flammability rated and includes an integrated label area to identify outlet sockets and cords.

TAK-TY ® Loop Ties
Slot allows for pre-wrapping of bundles

TAK-TY ® Strip Ties
Rolls perforated in convenient 6”, 8” or 12” strips for use with pre-determined bundle sizes

TAK-TY ® Rolls
Continuous rolls of 15’ and 75’ can be cut to any length

TAK-TY ® Stacked Strips
Eliminate cutting and staging 7” strips (100 pieces)

TAK-TY ® Cable Ties – Plenum Rated UL approved for use in air handling spaces

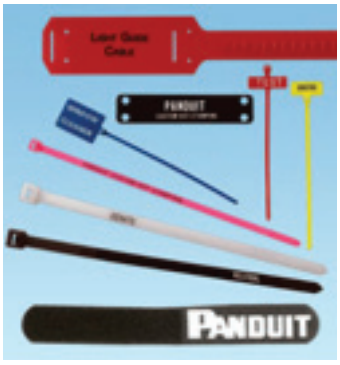
Ultra-Cinch™ Ties
Cinch ring accommodates tighter bundles

Elastomeric Cable Ties
UL 94V-0 flammability rating
Safe and releasable

TAK-TAPE ™ Rolls
General purpose fastener

Hook & Loop Wrap Marker Ties
Write-on identification area
Custom Imprinting Available

Cable Bundle Organizing Tool
Arrange 24 data cables prior to installing cable ties



Custom Imprinting Service
Used for identification, labeling and promotional purposes

POU Plug Retention Device
Reduce the risk of equipment downtime due to accidental plug disconnection

Fig. 4.6-4. Cable Ties Recommended for Control Room, Network Distribution, and Zone Cabling Enclosure Applications

Part Numbers	Description
HLM-15R0	HLM Series 15 Ft. Roll x .330” Width, Black
HLS-75R0	HLS Series 75 Ft. Roll x .75” Width, Black
HLB2S-C0	100 Pc TAK-TY Stacked Strips, 7” Strip Tie, 0.75” Width, Black
HLS3S-X0	HLS Series 12” Strip Tie, Black
HLT*I-X0	HLT Series 8-12” Loop Tie, Black
HLTP2I-X12	HLTP Series 8” Loop Tie, UL, Plenum UL94V-2 - Maroon
HLSP3S-X12	HLSP Series 12” Strip Tie, UL, Plenum UL94V-2 - Maroon
CBOT24K	Cable Bundle Organizing Tool
PRPC13-69 PRPC13-60	Power Outlet Unit Plug Retention Device - Only used with select Panduit Power Outlet Units (Natural and BLK colors)
ERT*M-C20	8.5-11” Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating

4.6.1.3 Adhesive Backed Mounts

PANDUIT adhesive mounts provide a quick, economical, and dependable method of supporting, routing, and protecting wires and cables. Some are used with PANDUIT cable ties and others can be used without cable ties. Adhesive backed mounts adhere to a variety of surfaces. This alternative to mechanical fasteners offers the advantage of lower installed cost with safe, easy-to-use, quality products.

Applications include:

- To route wires in control panels and switchboards
- To support bundles of wires away from moving me chanical devices
- Routing and harnessing cables, both indoors and out, to prevent safety hazards
- To organize flat cables in many locations with low profile construction
- Ideal for supporting wire bundles where holes cannot be made in the substrate
- To separate groups of wires for identification

General Mount Guidelines. PANDUIT pressure sensitive adhesive (foam tape) mounts are intended to secure wire bundles or other light objects to smooth surfaces. These mounts are not designed to support excessive loads and should not be used when the maximum expected load exceeds the rated capacity of the mount.

Choosing the Right Adhesive. PANDUIT offers two standard pressure sensitive foam tapes which are available on most adhesive backed wiring accessories products. The general purpose tape is produced with a rubber based adhesive and is identified by an “-A” in the part number. This tape develops its strength extremely fast and can be used in environments with temperatures ranging from -40°F (-40°C) to +120°F (49°C). We recommend that rubber-based adhesive mounts dwell 2 hours after installation, prior to loading. Rubber-based adhesive tape is the best choice for most adhesive mount applications, including power coated surfaces.

Acrylic-based adhesive tape is also available and is identified by an “-AT” in the part number. This tape is for use in environments where continuous exposure to temperatures as high as 180°F (82°C) is possible. Acrylic-based adhesive develops its maximum strength over a longer period of time than rubber-based adhesive. It is recommended that acrylic adhesive mounts dwell 8 hours after installation, prior to loading. Acrylic based adhesive tape is a good choice for environments with prolonged exposure to UV rays or temperatures about 120°F (49°C).

Proper Storage Conditions. All PANDUIT adhesive products have an expiration date printed on the package label. For rubber and acrylic based foam tape adhesives, store in temperatures of 70°F (21°C) and 45% Relative Humidity (R.H.).

Adhesive Backed Latching Clips	Latching cover withstands vibration	Latching Wire Clip	Latching wire clip with convenient releasable latch
Adhesive Backed Mounts	Adhesive backed cable tie mounts; rubber or acrylic adhesive	Marker Plates	Install as flags, tags, or wrap-around labels to clearly identify harnesses
Adhesive Cord Clip	Adhesive cord clip that easily allows cables to snap into place	Metal Adhesive Cord Clip	Metal adhesive backed cord clip; opens and closes to add/remove cables
Beveled Entry Clip	Beveled entry allows for easy insertion of cable bundles	Multiple Bridge Adhesive Backed Mounts	Multiple bridge adhesive backed mount; has four cable tie mount bridges
Cable Holder	Releasable latch allows cables to be added/removed; adhesive/screw mount	Push Mount Assemblies	Unique barb design with u mbrella tensioning; pre-assembled with standard cable tie
Cable Spacers	Used to separate and/or hang cables	Push Mounts with Umbrellas	Unique barb design with umbrella tensioning
Cable Tie Mounts	Low profile, cradle design keeps cables close to mounting surface; screw mount	Standard Fixed Diameter Clamps	Standard size cable clamps; install with #8 (M4) screw
Control Panel Mounts	Installed behind control panel switches	Standard Multiple Tie Plates	Low profile design used to separate closely bundled cables
Dynamic Cable Manager	Dynamic cable manager for panel strain relief; adhesive backed mount	Swivel Mounts	Separates bundles to avoid abrasion; swivels 360 degrees
Heavy-Duty Fixed Diameter Clamps	Heavy-duty cable clamps; install with #10 (M5) screw	Tie Anchor Mounts	4-way cable tie orientation; small overall size
Rounded Edge Multiple Tie Plates	Heavy-duty design used to separate closely bundled cables	Vertical Cord Clip	Funnel entry design allows for easy installation of cables
J-PRO™ Cable Support System	Durable non-metallic J-hooks can manage/support large numbers of cables		

Building an Adhesive-Backed Mounting Solution

4.6.1.4 Cable Accessories Product Lines

A Cable Management System shall be used to provide a neat and efficient means for routing and protecting fiber and copper cables and patch cords on telecommunication racks and enclosures. The system shall be a complete cable management system comprised of vertical cable managers, horizontal cable manager, and cable management accessories used throughout the cabling system. The system shall protect network investment by maintaining system performance, controlling cable bend radius and providing cable strain relief.

Vertical D-Rings. A vertical cable management solution of flexible Vertical D-rings shall be used on standard communication racks. The Vertical D-rings used for open access shall be manufactured from a Polycarbonate material and shall be black in color. The vertical cable management D-rings shall be a one-piece design. The front arm of the product shall be able to rotate ninety degrees to allow entire cable bundles to be inserted. The vertical cable management solution of flexible D-rings shall be installed with two screws less than 0.25” in diameter.

Part Number	Outside Dimensions (LxW)	Capacity (.187" UTP)	Capacity (.25"ScTP)	Capacity (3mm Fiber)
CMVDR1	5.7"x2"	96	48	252
CMVDR1S	3.3"x2"	52	32	132
CMVDR2	5.7"x3"	192	96	504
CMVDR2S	3.3"x3"	96	48	252
CMVDRC	5.6"x8"	400	200	1000

TAK-TY ® Hook & Loop Cable Tie Mounts. A mounting device shall be used with ¾" maximum TAK-TY ® Cable Ties to secure bundles of communication cabling in cabinets, closets or other environments where cable management is a concern. Adhesive backed products can be utilized to bundle up to .38 lbs. of communication cable. If more than .38 lbs. of holding force is required, a fastener such as a #6 screw shall be used.

Part Number	Mounting Method	Color
ABMT-A-C	Rubber Adhesive	Natural
ABMT-A-C20	Rubber Adhesive	Black
ABMT-S6-C	#6(M3) Screw	Natural
ABMT-S6-C20	#6(M3) Screw	Black
ABMT-S6-C60*	#6(M3) Screw	Black
ABMT-S6-C69*	#6(M3) Screw	Natural

* Flame retardant products are manufactured from a material that is rated UL94V-0.

Waterfall Accessories. Cable Management Waterfall Accessories shall be utilized to transfer communication cable from ladder racks to enclosures or equipment racks below. These cable management waterfall systems shall maintain 1" bend radius control in both vertical and horizontal directions. The system shall be modular in order to allow for multiple widths.

Part Number	Description	Color
CMW-KIT	Waterfall Kit	Black
CMW-KIT10	Waterfall Kit	White
CMWB	Waterfall Base	Black
CMWB10	Waterfall Base	White
CMWW	Waterfall Wing	Black
CMWW10	Waterfall Wing	White

Stackable Cable Rack Spacers. Stackable Cable Rack Spacers shall be utilized to route bulk fiber optic cable or high performance copper communication cable bundles. Stackable Cable Rack Spacers shall be utilized in communication closets and other interior locations where cables and cable bundles are routed along traditional ladder racks that consist of rungs and stringers. The Stackable Cable Rack Spacers shall be applied on every rung up to a recommended maximum stack height. Dovetail slots and a positive latching mechanism shall provide a secure locking feature.

Part Number	Cable Bundles	Bundle Diameter	Recommended Stack Ht.
CRS6-X	6	.8”	5
CRS1-X	1	.8”	5
CRS4-125-X	4	1.25”	4
CRS1-125-X	1	1.25”	1

Threaded Rod Cover. The Threaded Rod Cover shall be utilized to protect communication cable from abrasion caused by contact with threaded rod. The Threaded Rod Cover shall be manufactured from a gray flame-retardant polyethylene material that is UL94V-0 rated. The material shall be pliable to allow for easy installation.

Part Number	For Threaded Rod Size	Length
TRC18FR-X8	1/2”x5/8”	18”

J-MOD ™ Cable Support System. Open top cable supports shall be utilized as a pathway for communication cabling. The J Hook cable supports shall be manufactured from a non-conductive material suitable for use in air-handling spaces. The cable support must maintain complete horizontal and vertical 1” bend radius control and must manage up to 50 four-pair UTP cables. The system must allow for the ability to add future cable routing capacity. The cable support must provide the ability to retain the cable bundle with TAK-TY ® Hook & Loop Cable Ties.

Part Number	Description	Material*	Maximum Static Load (Lbs.)
JMJH2W-X20+	J Hook for wall moutn applictions	Nylon	30
JMJH2-X20+	J Hook for use with brackets	Nylon”	30
JMCB-X	Ceiling Bracket	Galvanized Steel	120
JMCMB25-1-X	Ceiling Mount Bracket (1 level)	Galvanized Steel	180
JMCMB25-3-X**	Drop Wire Bracket (3 level)	Galvanized Steel	180
JMDWB-1-X	Drop Wire Bracket (1 level)	Galvanized Steel	20
JMDWB-3X**	Drop Wire Bracket (3 level)	Galvanized Steel	40
JMTRB38-1-X	Threaded Rod Bracket (1 level)	Galvanized Steel	180
JMTRB38-3-X**	Threaded Rod Bracket (3 level)	Galvanized Steel	180
JMSBCB87-1-X	Screw=on Beam Clamp Bracket (1 level)	Galvanized Steel	180
JMSBCB887-3-X**	Screw-on Beam clamp Bracket (3 level)	Galvanized Steel	180

** Not for use with chaining brackets

+ Available in natural and black

* Suitable for use in air handling spaces per UL 2043. Listed in accordance with CAN/ULC 8102.2 when mounted as single units on/in pairs. Minimum spacing of 1 ft. (1220mm) required between mount points. (Flame Spread Rating - 0, Smoke Developed Classification - 30”)

J-PRO ™ Cable Support System. Open top cable supports shall be utilized as a pathway for communication cabling. The J Hook cable supports shall be manufactured from a non-conductive material suitable for use in air-handling spaces. The pre-riveted J Hook assemblies must maintain complete horizontal and vertical 1" bend radius control. The cable support must provide the ability to retain the cable bundle with TAK-TY ® Hook & Loop Cable Ties.

Part Number	Part Description	Bundle Capacity (In)	Material*	Static Load Rating (Lbs.)
JP75W-120	J Hook for wall mount application One 1/4" (M6) mounting hole for user supplied screw	0.75	Nylon 6.6	15
JP131W-L20	J Hook for wall mount application One 1/4" (M6) mounting hole for user supplied screw	1.31	Nylon 6.6	20
JP2WT-20	J Hook for wall mount application One 1/4" (M6) mounting hole for user supplied screw"	3	Nylon 6.6	30
JP4W-X20	J Hook for wall mount application One 1/4" (M6) mounting hole for user supplied screw	4	Nylon 6.6	100

4.6.2 Installation

4.6.2.1 Mount Spacing

To determine the number of mounts to use in a given application, the following formula can be used as a guideline: (Cable or weight (Lbs. /ft.)/Static Load rating of Mount (Lbs./mt.) = Spacing (Mounts/Ft.)

4.6.2.2 Adhesive Backed Mounts

Surface Preparation. For best results, PANDUIT adhesive mounts should be applied to clean, dry, grease-free surfaces. We recommend that the surface be cleaned prior to mount installation. For rubber and acrylic based foam tape adhesives, a blend of isopropyl alcohol and water 50/50 may be used to clean most surfaces.

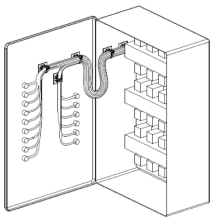
Proper Installation Techniques for Pressure Sensitive Adhesive Mounts. For proper installation of adhesive mounts with foam tape, simply remove the release liner and place the mount in the desired location. Avoid touching the adhesive prior to positioning the mount. Apply firm pressure to the mount for 5 seconds to insure proper adhesion.

1. Clean surface with a clean cloth and isopropyl alcohol
2. Allow surface to air dry
3. Remove the release liner, being careful not to touch the adhesive
4. Apply full thumb pressure for at least 5 seconds
5. Allow mount to properly dwell

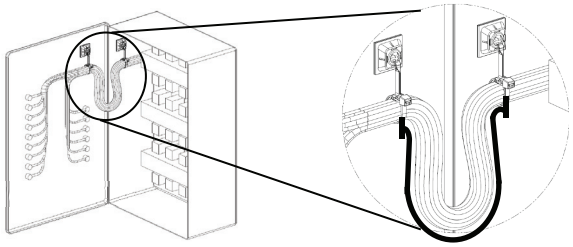
4.6.2.3 Dynamic Cable Manager

- For best results, PANDUIT rubber adhesive mounts should be applied to clean, dry, grease-free sur faces. It is recommended that the surface be cleaned prior to mount installation with a blend of isopropyl alcohol and water 50/50.
- For proper installation, simply remove the release liner and place the mount in the desired location. Avoid touching the adhesive prior to positioning the mount. Apply firm pressure to the mount for 5 seconds to insure proper adhesion. Allow the mount to properly dwell.
- Ball-and-socket tether must hang down from the mount with bundle installed below the mount.
- Unsupported bundle length should be no more than 1.27 lbs. (see illustration below, unsupported bundle length is shown as figure “A”)
- There must be no rigid mounts in line with the dynamic cable manager. These mounts would restrict bundle motion.
- The mounts should not be placed directly next to the hinge. A suggested minimum of 1” between edge of part and hinge is recommended.
- Please see below for a comparison of typical current installations using static mounts and suggested installation using dynamic cable manager mounts.

Typical current installations using static mounts



Suggested installation using dynamic cable manager mounts



4.7 Identification

Proper identification is crucial to the successful design, installation, and management of the industrial automation infrastructure components. Identification provides these important benefits:

- Determining locations of components
- Defining the system connections
- Communicating safety hazards

It is this determining, defining, and communicating that provide quick, clear direction that is necessary to accurately and safely install, maintain, and repair critical industrial automation infrastructure components resulting in efficient and reliable performance.

STANDARDS and CODES

Although no standards currently define labeling practices in the industrial automation space, several existing standards can be used as a guide. These standards are developed by organizations committed to the best practices for network and electrical infrastructure.

TIA/EIA-606A
Identification and Administration of Commercial Telecommunications Infrastructure

TIA/EIA-606A, Addendum 1
Identification and Administration of Equipment Rooms and Data Centers

National Electric Code – NFPA 70

UL 508A – Industrial Control Panel

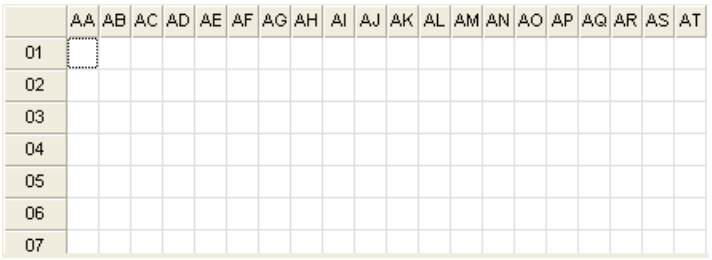
4.7.1 Selection

4.7.1.1 Control Room Infrastructure

The control room environment is much like a data center in that it provides all the computing, storage, and network resources for data communication across the industrial automation space. The identification of infrastructure in this area is based on the TIA/EIA-606A, Addendum 1 Standard for Data Centers. The basis of this standard is the physical location of connection ports.

Grid Labeling.
Component locations in the control room are determined by using an X-Y coordinate system that is usually based on the floor tile system in the control room space. If there is not a raised floor then a 24 inch x 24 inch (61cm x 61cm) grid may be applied to the room.

By using alphabetical designations on one axis of the room and numerical designations on the other axis of the room, you can create a series of alphanumeric designations that can be established for each floor tile or grid in a control room space. These floor tile designations are the basis for determining the location of control room devices.



Cabinet/Rack Labeling

The floor tile or grid designations are used to identify each cabinet or rack in the control room. The cabinet/rack location is based on which floor tile the right front corner of the cabinet/rack rests upon. Cabinets and racks should have location labels applied to the top and bottom of both the front and rear of the device. These labels should be visible whether or not doors are closed or opened on the cabinets.

A typical cabinet/rack label would have the following scheme:

AB04

This identifier would define that the cabinet/rack is located with its right front corner at the intersection of row AB and column 04.

Panel Labeling.

Once the cabinet/rack identifiers are established, the various panels in the cabinet/rack should be identified. The designation for the panel positions in a cabinet/rack can be either an alphabetic designation or a two-digit number that represent the rack unit number (RU) where the top-left mounting screw lands in the cabinet/rack. Using the RU method provides the control room manager with greater flexibility since it allows for panels and equipment to be added or removed later without disrupting the designation of panel identifiers.

A typical panel label would have the following scheme:

AB04-24

This identifier would define that the top left mounting screw of the panel is located at the 24th rack unit position in the cabinet/rack located grid AB04 in the control room.

Port Labeling.

Now that cabinets/racks and panels in each rack are identified, the next task is to establish identifiers for each port on a panel. Port identifiers are very important because they define the connectivity of cabling within the control room infrastructure. Many patch panels come from suppliers with numbers already screen-printed above the ports; if this is the case there is no need to re-label those patch panels.

If the patch panels are not pre-printed with port numbers, labels will need to be created to identify the port numbers. The numbering sequence should proceed from left to right and top to bottom for all ports on a patch panel. The number of digits used for all numbers on a patch panel should be consistent with the total number of ports on that patch panel. For example, a 48-port patch panel should be labeled 01 through 48 and a 144-port patch panel should be labeled 001 through 144.

In a data center, a typical port label would have the following scheme:

AB04-24:01

This identifier can be decoded to define that this is port 01 located on panel 24 in cabinet/rack AB04.

However, in a control room environment, this information is somewhat redundant given that the cabinet/rack and panel are clearly identified and are not usually required information on the port label, as the cabinet/rack and panel are apparent to the viewer who is standing at the location of the port.

Therefore, a typical control room port label would have the following scheme:

01

This identifier defines that this is port 01.

Cable Labeling and Patch Cord Labeling.

The cabling on the back and front of the cabinet/rack must be identified. Labeling of cables on the back of the panel is considered cable labeling and the labeling of cables connected to the front of the panel is considered patch cord/ equipment cord labeling.

Cable Labels

Cables labels are identified with information that defines the connection between the near end panel connection and the far end panel connection. A near end connection identifier would consist of the cabinet/rack location, panel location, and port location. The far end connection identifier would consist of the cabinet/rack location, panel location, and port location.

A typical cable label would arrange near end / far end information in the following scheme:

AB04-24:01/AB07-36:13

This identifier would be decoded to define that the cable connects between cabinet AB04 panel 24 port 01 going to cabinet AB07 panel 36 port 13. The far end of the cable would have a label that would have the same information in the reverse order.

Patch Cord/Equipment Cord Labels.

Patch cord/equipment cord labels are identified with information that defines the connection between the near end patch panel front connections and the far end patch panel front connections or equipment connections. A near end connection identifier would consist of the cabinet/ rack location, panel location, and port location. The far end connection identifier would consist of the cabinet/rack location, panel location, and port location.

A typical patch cord label would arrange near end / far end information in the following scheme:

AB04-24:01/AB04-36:13

This identifier would be decoded to define the patch cord connection between cabinet AB04 panel 24 port 01 going to the same cabinet panel 36 port 13. The far end of the cable would have a label that would have the same information but in the reverse order.

A typical equipment cord label would information in the following scheme:

AB04-24:01/AB04-Server2:A

This identifier would be decoded to define the equipment cord connection between cabinet AB04 panel 24 port 01 going to the same cabinet port A on equipment named Server2. Rack unit location could be substituted for equipment name if necessary.

Patch Panel Connectivity.

Patch Panel connectivity is considered the most important area of network infrastructure labeling because it defines the critical connections between ports on patch panels and equipment. This information defines the connections between the near-end ports and the far-end ports. This labeling can define the connection of a range of ports on a panel or just define the connection for two individual ports.

A typical patch panel connectivity label would arrange near end / far end information in the following scheme:

AB04-24:ports 01-12/ AB07-36:ports 25-36

This identifier would be decoded to define that the ports 01 through 12 on panel 24 of cabinet AB04 connect to ports 25 through 36 on panel 36 of cabinet AB07.
Grounding and Bonding. Labeling of the grounding and bonding system involves the identification of the main grounding busbar, grounding busbars, conductors connecting busbars, conductors connecting devices to busbars, and equalizing conductors.

The typical scheme for the main grounding busbar would be:

1-B301-TMGB

This identifier can be decoded to define that this is the telecommunications main grounding busbar (TMGB) located on floor 1 in space B301.

The typical scheme for a grounding busbar would be:

2-R201-TGB

This identifier can be decoded to define that this is the telecommunications grounding busbar on floor 2 in space R201.

The typical scheme for the busbar connections would be:

1-B301-TMGB/2-R201-TGB

This identifier can be decoded to define that this is the conductor that connects the main telecommunications grounding busbar located on floor 1 in space B301 to the telecommunications grounding busbar on floor 2 in space R201.

Power Cables.

Labeling of the power system involves the labeling of the cables feeding power outlet units (POU) with information which define the source of power to the POU. This information would include the distribution panel and the circuit that feeds the POU.

A typical scheme for the power labeling would be:

AB03A-PP21-15

This identifier can be decoded to define that this is the power cable that connects POU A located in rack/cabinet AB03 to circuit breaker 15 in power panel 21.

4.7.1.2 Network Infrastructure

The Network Infrastructure can be identified using the guidance of TIA/EIA-606A.

Cable Labels

Cable labels are identified with information that defines the connection between the near end connection and the far end connection. A near end connection identifier would consist of the location of the enclosure, the panel location in the enclosure, and the port location. The far end connection identifier would consist of the location of the enclosure, the panel location in the enclosure, and port location. For cables that do not connect between patch panels the machine name or location and the port number can be used.

A typical cable label would arrange near end / far end information in the following scheme:

AB04-24:01/1ZB.01-2:01

(Origination Port / Destination Port)

This identifier would be decoded to define the cable connects between cabinet AB04 panel 24 port 01 in the control room going to port 01 in patch panel 2 located in zone box #1 on the first floor of the facility. The far end of the cable would have a label that would have the same information but in the reverse order.

Pathways.

Cable Pathways are identified with information that defines routing of the cables contained in a pathway. This information is useful for determining which pathway connects between industrial automation areas. Locating the proper pathway is necessary to remove, add, or repair a cable in the infrastructure.

A typical pathway label would arrange near end / far end information in the following scheme:

AB04/1ZB.01

This identifier would be decoded to define that the pathway connects between cabinet AB04 in the control room and zone enclosure #1 on the first floor of the facility.

Firestopping.

Each firestopping location shall be labeled at each location where firestopping is installed, on each side of the penetrated fire barrier, within 12 inches (300mm) of the firestopping material.

A typical firestopping label would arrange information in the following scheme:

1-FSL01(2)

This identifier would be decoded to define that this is firestopping location number 01 on the first floor and that the firestopping has a two hour rating.

Grounding and Bonding.

Labeling of the grounding and bonding system throughout the network involves the identification of the grounding busbars, conductors connecting busbars, conductors connecting devices to busbars, and equalizing conductors.

The typical scheme for a grounding busbar would be:

2-R201-TGB

This identifier can be decoded to define that this is the telecommunications grounding busbar (TGB) on floor 2 in space R201.

4.7.1.3 Zone Cabling Enclosure Labeling

Labeling in the Zone Cabling Enclosure can be identified using the guidance of TIA/EIA-606A. Ideally the physical location of the zone cabling enclosure within the facility should be used on the label to identify the zone enclosure. This is provides a quick method of locating connections to zone cabling enclosures using information on far end cables.

Often there is not a good method to assigning a physical location so then a unique number and the type of telecommunication space is used. These labels should be visible whether or not doors are closed or opened on the enclosures.

A typical zone cabling enclosure label with a physical location would have the following scheme:

AA10

This identifier would define that the enclosure is located with at the intersection of wall marker AA and wall marker 10.

A typical zone cabling enclosure label without physical location would have the following scheme:

1ZB.01

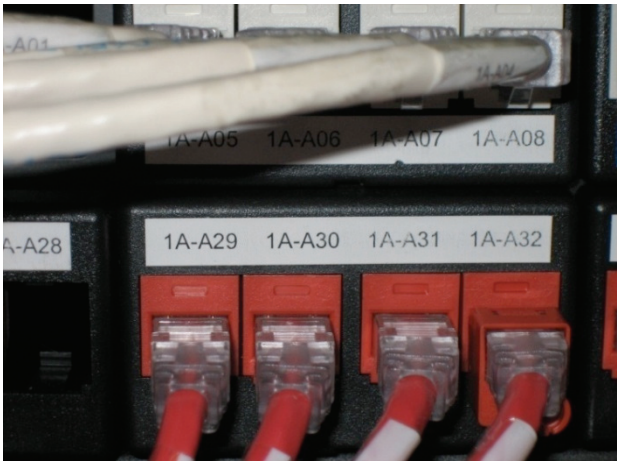
This identifier would define that the enclosure is located on the first floor and is zone cabling enclosure number 1 in the facility.

Panel Labeling

The designation for the panel positions in a zone enclosure can be either an alphabetic designation or a two-digit number that represent the rack unit number (RU) where the top-left mounting screw lands in the zone enclosure. Using the RU method provides greater flexibility since it allows for panels and equipment to be added or removed later and not disrupt the designation of panel identifiers.

A typical panel label would arrange near end / far end information the following scheme:

1ZB.01-2



This identifier would define that the top left mounting screw of the panel is located at the 2nd rack unit position in the zone box # 1 located on the first floor of the facility.

Port Labeling.

Many patch panels come from the factory with numbers already screen-printed above the ports. If this is the case, there is no need to re-label those patch panels. If the patch panels are not pre-printed with port numbers then labels will need to be created to identify the port numbers. The numbering sequence should proceed from left to right and top to bottom for all ports on a patch panel. The number of digits used for all numbers on a patch panel should be consistent with the total number of ports on that patch panel. For example a 48-port patch panel should be labeled 01 through 48 and a 144-port patch panel should be labeled 001 through 144.

A typical port label would have the following scheme:

1ZB.01-2:01

This identifier can be decoded to define that this is port 01 located on panel 2 in zone box # 1 on the first floor of the facility.

This is somewhat redundant information given that the cabinet/rack and panel are clearly identified and are not usually required information on the port label since the cabinet/rack and panel are apparent to the viewer who is standing at the location of the port.

Therefore a typical port label would have the following scheme:

01

This identifier defines that this is port 01.

Production Offices

In the office area, each individual telecommunications outlet/connector shall be labeled with the horizontal link identifier. The labeling shall appear on the connector or faceplate in a way that clearly identifies the origination of the horizontal link.

A typical office outlet connection would arrange information in the following scheme:

1ZB.01-2:01

This identifier can be decoded to define that this connection originates in port 01 located on panel 2 in zone box # 1, in the following scheme:

1ZB.01-2:01

This identifier can be decoded to define that this connection originates in port 01 located on panel 2 in zone box # 1.

4.7.1.4 Control Panel Infrastructure

Enclosure Labels

Ideally, the physical location of the control panel within the facility should be used on the label to identify the control panel. This provides a quick method of locating connections to control panels using information on far end cables. Often, there is not a good method to assigning a physical location. In this case, a unique number and the type of telecommunication space are used. These labels should be visible whether or not doors are closed or opened on the enclosures.

A typical control panel label with a physical location would arrange information in the following scheme:

BE24

This identifier would define that the enclosure is located with at the intersection of wall marker BE and wall marker 24.

A typical control panel label without physical location would arrange information in the following scheme:

1CP.05

This identifier would define that the enclosure is located on the first floor and is control panel number 5 in the facility.

Port Labeling

Industrial Automation control panels can have ports located on any surface of the control panel. To delineate the location of each port in a control panel the mounting surface should be specified.

The following designations can be used to clearly communication the location in the control panel of each port.

Control Panel Part	Designation	Inside Surface (Optional)	Outside Surface (Optional)
Back Plane	BP	IBP	OBP
Panel Door	PD	IPD	OPD
Panel Right Side	PR	IPR	OPR
Panel Left Side	PL	IPL	OPL
Panel Top Side	PT	IPT	OPT
Panel Bottom Side	PB	IPB	OPB

In addition to the control panel surface each port in the control panel should be labeled with a unique number. The numbering sequence should proceed from left to right and top to bottom for all ports in a control panel. The number of digits used for all numbers in the control panel should be consistent with the total number of ports in that control panel. For example a control panel with 48 ports should be labeled 01 through 48 and a control panel with 120 ports should be labeled 001 through 120.

A typical port label would arrange information in the following scheme:

1CP.08-BP:01

This identifier can be decoded to define that this is port 01 located on the back plane of the control panel #8 on the first floor of the facility.

This is somewhat redundant information given that the control panel and surface are clearly identified and are not usually required information on the port label since the control panel and surface are apparent to the viewer who is standing at the location of the port. Therefore a typical port label would have the following scheme:

01

This identifier defines that this is port 01.

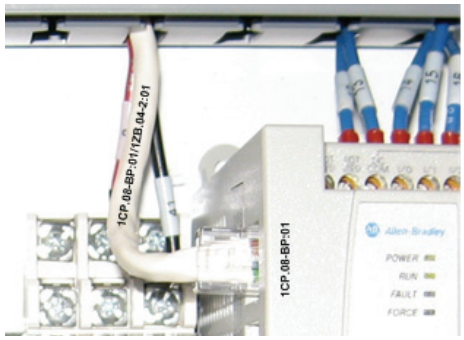
Cable Labels

Cable labels are identified with information that defines the connection between the near end connection and the far end connection. A near end connection identifier would consist of the location of the enclosure and the port location. The far end connection identifier would consist of the location of the enclosure, the panel location in the enclosure, and port location.

A typical cable label would arrange near end / far end information in the following scheme:

1CP.08-BP:01/1ZB.04-2:01

(Origination Port / Destination Port)



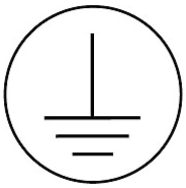
This identifier would be decoded to define that the cable connects between port 1 on the back plane of control panel #8 located on the first floor of the facility going to port 1 on the patch panel 2 in zone box #4 on the first floor. The far end of the cable would have a label that would have the same but with the information reversed.

Enclosure Markings.

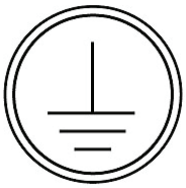
Labels and warning are required to communicate safety information without the use of words.

Protective Conductor

Dangerous Electrical Voltage

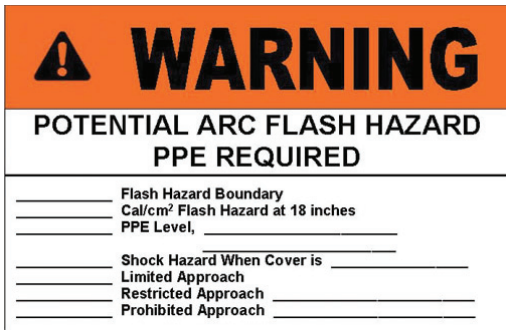


Safety Function Ground



Earth Ground

UL 508A Warning Sign



NEC 70A Arc Flash Warning Sign

4.7.2 Installation

The following label creation and generation products will help you clearly identify all industrial network components according to the schemes described in this section.

4.7.2.1 Label Creation

EASY-MARK™ Labeling Software

- *EASY-MARK*™ Labeling Software simplifies label creation for the specific needs of your applications
- Instructions and user interface are available in English, French, German, Italian, Spanish, Korean, Chinese and Portuguese
- Intuitive interview process allows automatic generation of compliant labels and signs
- Software selects and formats the optimum label
- **WYSIWYG** (What You See Is What You Get) user interface, alpha/numeric serialization, data import, symbol import
- *EASY-MARK*™ Labeling Software is part of a complete line of innovative identification solutions from *PANDUIT*
- Supports most WINDOWS^ fonts drivers for standard thermal transfer, dot matrix, laser and ink jet, including *PANDUIT* thermal transfer printers

System Requirements:

- WINDOWS^ 2000, NT4.x or XP; 64MB hard drive space and 64MB RAM (256MB RAM Recommended)

Part Number	Part Description	Std. Pkg. Qty.	Std. Ctn. Qty.
PROG-EMCD3	*EASY-MARK*™ Labeling Software, supplied on CD-ROM.	1	10

Order number of software packages required.
^WINDOWS is a registered trademark of Microsoft Corp. in the United States and/or other countries.

CAD-CONNECT™ Labeling Software

- Generates labels quickly and easily directly from electronic CAD files
- Eliminates steps and time spent manually copying CAD identifiers into labeling software
- Program combines the power of an innovative wizard interview and *EASY-MARK*™ Labeling Software to capture and organize identifiers from electronic CAD files to automatically create and print labels
- Compatible with full versions of AutoCAD* 2000i or newer, AutoCAD Mechanical 2007, and Visio^ 2002 or newer
- Exports to alternative formats such as EXCEL^ (XLS) or Text (CSV) files for future use and documentation

System Requirements:

- WINDOWS^ 2000, XP, or Vista; 64MB hard drive space and 64MB RAM (256MB RAM recommended)

Part Number	Part Description	Std. Pkg. Qty.	Std. Ctn. Qty.
PROG-CCCD	*CAD-CONNECT*™ Labeling Software, including *EASY-MARK*™ Labeling Software, supplied on CD-ROM.	1	10

*AutoCAD is a registered trademark of Autodesk, Inc.
^Visio, WINDOWS, and EXCEL are registered trademarks of Microsoft Corp. in the United States and/or other countries.

4.7.2.2 Label Generation

TDP43MY Desktop Thermal Transfer Printer and Accessories

- Compact, lightweight design enables use in office or remote locations
- 300 dpi thermal transfer printer creates crisp, clear legends with superior legibility
- Up to 2.00" per second print speed for fast label production
- Use to print a wide variety of self-laminating labels, component labels, non-laminated labels, heat shrink labels, marker plates and continuous tapes up to 4.00" wide
- *EASY-MARK*™ Labeling Software and hybrid ribbon included with printer
- Compatible with most standard PCs

TDP43MY

TDP43M-CASE

Part Number	Part Description	Std. Pkg. Qty.	Std. Ctn. Qty.
TDP43MY	300 dpi printer; includes printer, *PANDUIT® EASY-MARK*™ Labeling Software, RMH4BL hybrid black ribbon, AC power adapter with US and Europlug power cords, manual and quick start card.	1	—
TDP43M-RS	External label roll stand – used to rear feed labels that are supplied on 3.00" cores, such as photoluminescent tape.	1	—
TDP43M-CASE	Hardside carrying case. Accommodates printer, AC power adapter, ribbons, printer cable, labels and tools.	1	—
TDP43M-ACY	Replacement AC power adapter with power cord (US cord only).	1	—
PTR-CLN	Printer cleaning kit – contains bottle of cleaning solution with MSDS, cleaning pen, swabs, alcohol wipes and cleaning instructions.	1	—

4.8 Safety and Security

Increasingly, electrical and network systems are converging throughout the physical infrastructure. In industrial environments this trend toward unifying the infrastructure has introduced new safety and security concerns, particularly at control panel locations. Acce-ssing the control panel has inherent hazards such as arc flash, shock, and the inadvertent or unauthorized disconn-ection of communication cables. All these risks have a potentially adverse impact on reliability and performance.

In addition, the presence of networking physical layer hardware and cabling has the potential to introduce new safety risks. Why? Network technicians who are less familiar with control panel environments may be working in these spaces. The network infrastructure also must be secure from intruders and unauthorized changes to protect sensitive data and to ensure that system uptime and productivity goals are met.

Security

The physical infrastructure must be secured to maintain the highest possibly network reliability. All connections should be secured with restricted access to unused and open ports Costs associated with network downtime or security breach can be tremendous.

The connections in a crowded control room rack or enclosure system are important to document and control from a security perspective. Demilitarized zones (DMZ) and their firewalls depend on segregating connections for enterprise and manufacturing layers yet mistakes or security breaches can develop if patching connections are not made properly. A manual system to identify and audit can be time consuming and difficult to maintain.

Physical Infrastructure Management (PIM) technology can automate this process by monitoring these connections and serving this data to higher level systems. This management software also provides tools for improved efficiency when planning and executing changes to patching or additions to the system. A managed system with logging and configuration tracking makes your infrastructure more transparent and controlled which can be an important piece of the security strategy for a critical process plant or control system.

Safety

Network technicians are not always knowledgeable of the potential hazards around control panels; therefore, proper identification of hazards, such as Arc Flash and shock is critical. It is estimated that the average total cost of an arc flash incident is around $15 million. With this in mind, having a comprehensive safety program which includes identification and control of hazardous energy can be an inexpensive form of risk mitigation. This safety program can include items such as proper Lockout/Tagout, proper arc flash labeling, Short Circuit Current Rating labeling, and the use of Data Ports so that industrial control panels can stay closed as much as possible.

STANDARDS and CODES: Safety

NFPA 70E

The primary National Fire Protection Agency (NFPA) code that is critical for safety is NFPA 70E, Electrical Safety in the Workplace. NFPA 70E addresses the electrical safety requirements for employees' workplaces which are essential to ensure employee safety. As physical infrastructure systems converge, an increasing number of workers are not familiar with electrical or other hazards, so applying NFPA 70E is key to having a safe workplace for all employees.

One of the key areas of NFPA 70E in Industrial Automation is Arc Flash hazard identification. An important change was made in the 2009 version of NFPA 70E where article 130 states that "Equipment shall be field marked with a label containing the available incident energy or required level of PPE." Whereas it was previously mandated that a comprehensive arc flash analysis shall be used to determine the arc flash boundary and the personal protective equipment (PPE) that people within the arc flash boundary must use, it is now also mandated that such information be posted on the equipment so that it is clearly available to all employees.

NFPA 70 (National Electric Code)

The other important code is NFPA 70, which is also called the National Electric Code, is a standard for the safe installation of electrical wiring and equipment. One particular section concerning safety is Article 409, which requires that a Short Circuit Current Rating be marked on all Industrial Control Panels.

Article 409.2 defines an Industrial Control Panel as:
"An assembly of two or more components consisting of one of the following:

(1) Power circuit components only, such as motor controllers, overload relays, fused disconnect switches, and circuit breakers.
(2) Control circuit components only, such as pushbuttons, pilot lights, selector switches, timers, switches, control relays
(3) A combination of power and control circuit components."

For safety purposes, Section 409.110 of the National Electric Code mandates that the Industrial Control Panel be marked with:
"Short-circuit current rating of the industrial control panel based on one of the following:

a. Short-circuit current rating of a listed and labeled assembly
b. Short-circuit current rating established utilizing an approved method"

It is also important to note that a footnote refers to the UL 508A standard, Supplement SB (see below).

UL 508A

UL 508A, the UL Standard for Safety Industrial Control Panels, addresses some of the safety identification requirement for control panels in industrial automation. Section SB5.2 of UL 508A is titled "Cautionary markings". It reads:

"An industrial control panel with a short circuit current rating based on the high fault short circuit current ratings of one or more components as specified in SB4.2.3 shall be marked with the word "WARNING" and the following statement: "Risk of Fire or Electric Shock – The opening of the branch-circuit protective device may be an indication that a fault current has been interrupted. All current-carrying parts and other components protected by this device should be examined and replaced if damaged. If burnout of a current element of an overload relay occurs, the complete overload relay must be replaced"

STANDARDS and CODES: Control of Hazardous Energy

OSHA 1910.147

The Occupational Safety and Health Administration (OSHA) released a standard called the Control of Hazardous Energy (Lockout-Tagout) which is referred to as 1910.147. This standard spells out the steps that employers must take to prevent accidents associated with hazardous energy and its control during servicing and maintenance of equipment or machinery.

NFPA 70E

NFPA 70 E also addresses "Establishing an Electrically Safe Work Condition" in Article 120. It is similar to the OSHA 1910.147 standard except that it is more targeted at electrical energy and not all types of energy. The requirements of both standards for controlling hazardous energy are addressed in the Installation portion of this section of this guide.

4.8.1 Selection: Security

The challenge to maintain security and manage risk along all connection points is becoming a top priority for network stakeholders. Each point of connection within a network represents a risk for a potential security breach and must be safeguarded against intruders, both purposeful and accidental. This requires tight security controls to protect sensitive data running over multiple data systems and networks.

4.8.1.1 Physical Infrastructure Management

The use of integrated server and switch architectures promotes a consolidation model which incorporates a defined upgrade path, whether through capacity increases within existing enclosures and patch fields or via straightforward addition of more enclosures, patch panels, racks, and/or cabinets without costly physical migration, cut-over activities, or “rip-and-replace” schemes. Upgrades are made easier with the use of Physical Infrastructure Management (PIM) software and the complementary PANDUIT® PANVIEW iQ™ System (see Figure 4H-1), which provide real-time monitoring and visibility into dense physical layer connectivity.

PIM systems are designed to increase the speed of configuring consolidated assets and applications, and to identify and resolve problems or security threats in real-time for quick resolution. LC fiber optic and RJ45 copper structured cabling connections can be automatically tracked through the patch field. By continuously monitoring all patch field connections, a PIM system instantly identifies any interruption or disconnection and immediately notifies a network administrator of the event or can provide SNMP data that can link to higher level software systems. These actions help to ensure that any inadvertent disconnections are remedied, minimizing downtime. Likewise, disruptions caused by potential security breaches are instantly identified for quicker response.

Information recorded in the PIM configuration database may be leveraged in several ways. First, the automated documentation of all configuration events can be used to track hardware assets (servers, switches) for commissioning/decommissioning purposes. The data also may be used to meet the reporting requirements of industry regulations or to meet established SLAs, and to provide a “snapshot” of the newly consolidated network to restore connectivity as part of an emergency or disaster recovery measures.

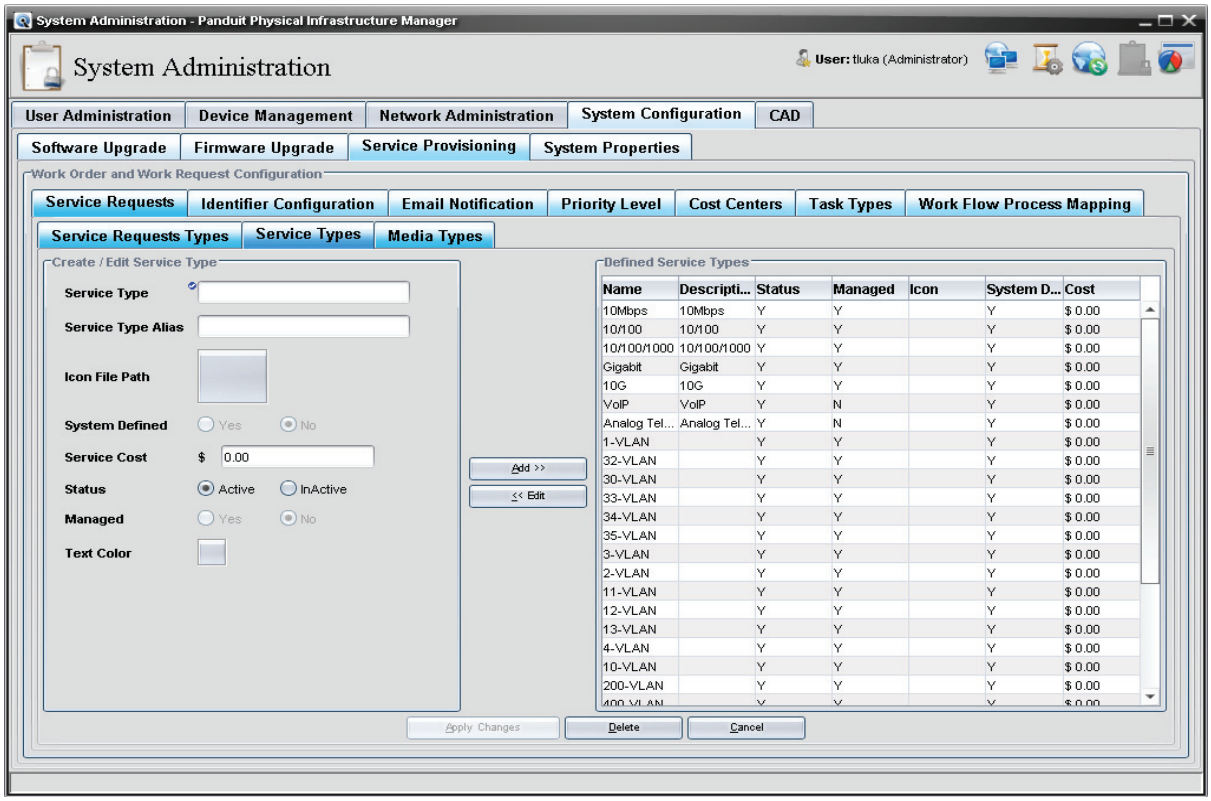
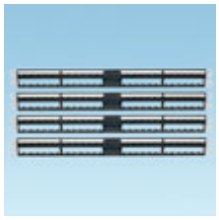


Figure 4.8-1. PIM systems optimize a consolidation strategy and improve business agility by achieving better port utilization through superior management of network ports and IT assets.

Building a PIM Solution

PanView iQ™ Physical Infrastructure Management Solution				
				
Hardware	Patch Cords	Patch Panels	Accessories	Software
PanView™ Physical Layer Management Solution				
				
Hardware	Patch Cords & Attachment cords	Patch Panels	Accessories	Software

4.8.1.2 Keyed Connector Solutions

It is important to select a structured cabling system that uses a modular system of proprietary connector and adapter products to support end-to-end separation of data networks. Innovative keyed system components are available to connect all cabling elements in an enterprise running from the main equipment room to the desk, delivering best value to organizations seeking to increase security and minimize risk.

Other keyed systems in the marketplace have been defeated by permitting an alien connector – either a differently keyed (or non-keyed) connector from the same manufacturer, or another manufacturer's connector – to be substantially inserted into a keyed port. This can result in a complete optical connection and thus compromise network security. In contrast, the PANDUIT Keyed LC System is tamper-resistant and robust against intrusion, securing networks against any other connector except the appropriate matching and color-coded PANDUIT keyed connector.

PANDUIT Keyed LC cable assembly, adapter and quick-termination connector components all feature both positive (key) and negative (keyway) elements that mechanically distinguish connections to maximize network security (see Figure 4.8-2). This combination of keys and keyways results in up to 18 different keying options, allowing a high number of discrete and secure networks to coexist in the same facility while preventing all un-alike keyed connectors and adapter ports from mating.

4.8.1.3 Physical Network Security Devices

Another efficient tool in maximizing physical network reliability and security is the use of Physical Network Security devices. These devices should be universal so that they can be retrofitted in the network infrastructure and be tamper-resistant, using a tool so that only authorized personnel can get access to the unused ports or connections they help to secure. They should also be used on both copper (RJ45) and fiber (LC) network connections to secure the integrity of the entire network infrastructure.

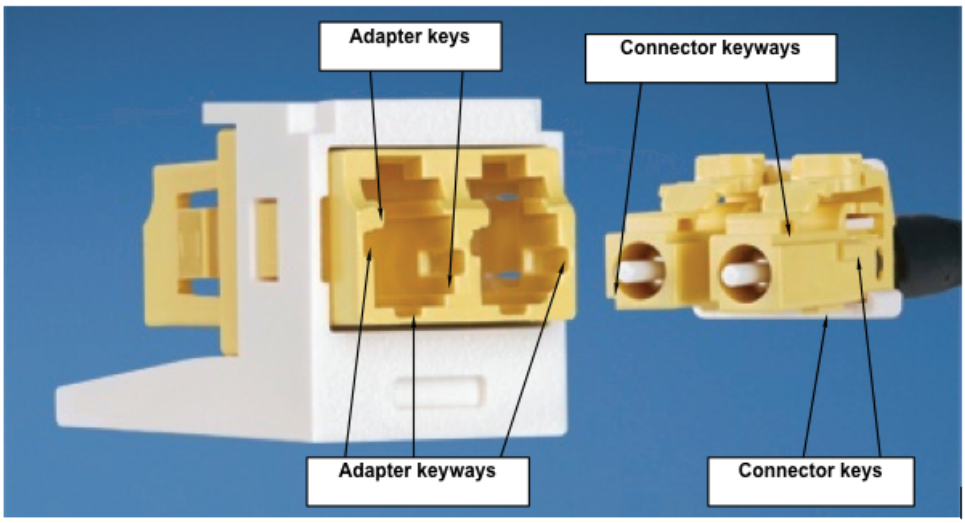
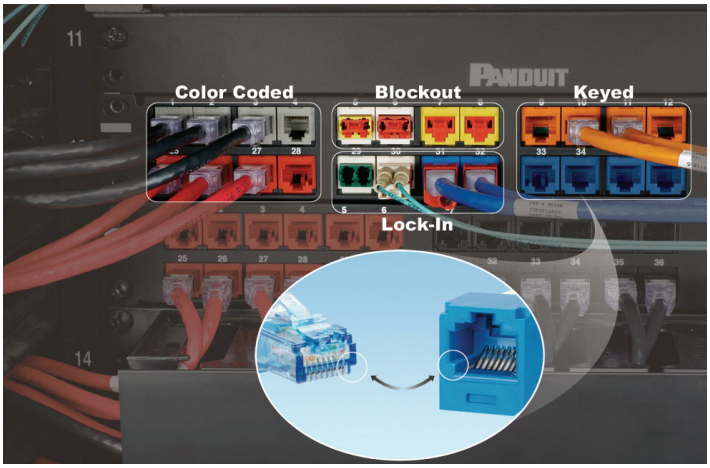


Fig. 4.8-2. The PANDUIT Keyed LC System provides a superior level of security to fiber optic channels because its system of both keys and keyways prevents un-alike keyed PANDUIT connectors, as well as other manufacturers' connectors, from being inserted into a PANDUIT Keyed LC Adapter port.

The Panduit Physical Network Security devices are the leading solution available in the market today to protect the physical layer of the network and are available for both copper and fiber connections. As an additional benefit, they are available in many colors, which can also be used for visual identification. For Copper, the RJ45 Lock-In device is available in standard and recessed versions to address various depths of RJ45 jacks. For example, maximum physical security is achieved on the Stratix switch by using a combination of standard and recessed devices with the downlink and uplink ports.

The Panduit Physical Network Security devices are the leading solution available in the market today to protect the physical layer of the network and are available for both copper and fiber connections. As an additional benefit, they are available in many colors, which can also be used for visual identification. For Copper, the RJ45 Lock-In device is available in standard and recessed versions to address various depths of RJ45 jacks. For example, maximum physical security is achieved on the Stratix switch by using a combination of standard and recessed devices with the downlink and uplink ports.



. The PANDUIT Keyed LC System provides a superior level of security to fiber optic channels because its system of both keys and keyways prevents un-alike keyed PANDUIT connectors, as well as other manufacturers' connectors, from being inserted into a PANDUIT Keyed LC Adapter port.

For the LC physical network security devices, the lock-in duplex clip for the cable assembly connector prevents adapter latches from disengaging from the connector unless an installation/removal tool is used. The tool also enables blockout devices to be snapped in or out of LC adapters or receptacles. These tools are available from PANDUIT to limit installation or removal of lock-in and blockout devices to only authorized users.

4.8.2 Selection: Safety

4.8.2.1 Data Access Port

Electricians, engineers, and network support staff often need to access the network connections internal to a control panel for configuration, programming or troubleshooting. Safety risks arise because many of these activities must be performed with the panel power on so that the machine controller and network switch are powered. Opening a 'live' control panel presents shock and arc flash dangers that can severely injure or even kill.

A dedicated access port that is designed for secure, safe access to data connections along with a power receptacle suitable for a laptop can greatly improve the compliance with the safety mandates concerning opening live control panels. A service person can now simply open this access port and configure or program devices internal to the panel without opening the panel door.

A key advantage of PANDUIT's Data Access Port (see Figure 4.8-5, next page) is a modular construction that can accommodate a number of available interfaces for Ethernet, RS232, and other standard network connections. This adaptability is important because control systems can evolve over time requiring additional connectors to support connectivity to added devices in the panel. This modular approach allows configuring to customers' existing needs then expanding or modifying so that this important safety feature stays useful over time as business requirements change.

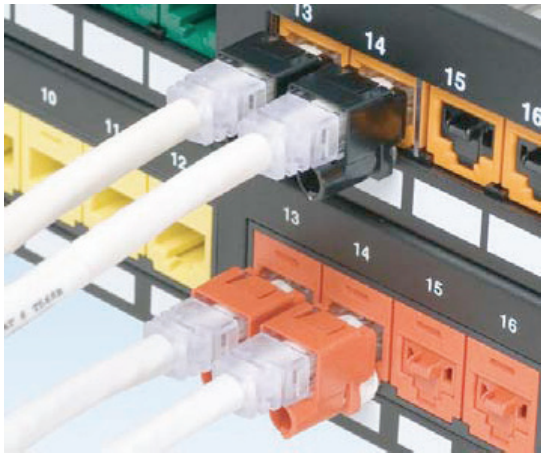


Figure 4.8-3. RJ45 Plug Lock-In device installed on patch cords secures connections to reduce network downtime, data security breaches, and hardware replacement due to theft. The RJ45 Jack Blockout Device installed in unused ports provides a simple and secure method to control access to data and deter vandalism to jacks.

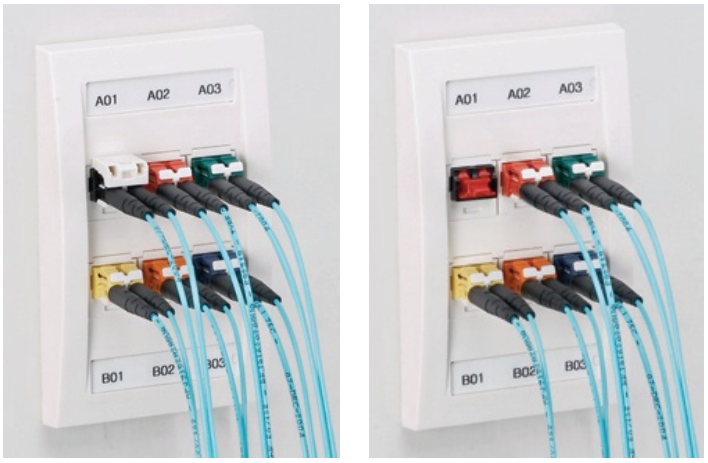


Figure 4.8-4. LC Connector Lock-In (left) and LC Duplex Adapter Blockout (right) devices further prevent unintentional moves, adds, and changes to PANDUIT Keyed LC deployments, mitigating the risk of connectors becoming accidentally dislodged or otherwise compromised.

4.8.2.2 LOTO Devices

Devices selected for Lockout / Tagout should be as universal as possible to cut down on the total number of devices needed to safely control the hazardous energy present in the infrastructure. They should also be easy-to-use so that there is no reason for employees to bypass Lockout / Tagout when performing service or maintenance on equipment or machinery.

4.8.2.3 Safety Labels

It is important to keep in mind the environment when selecting labels to identify hazards. For example, it is a best-practice to use Polyester labels with high-tack adhesive to ensure the longevity of the labels and offer the widest temperature range available. Also, it is best to use one supplier for labels so that the colors and appearance of the labels are consistent throughout the workplace.

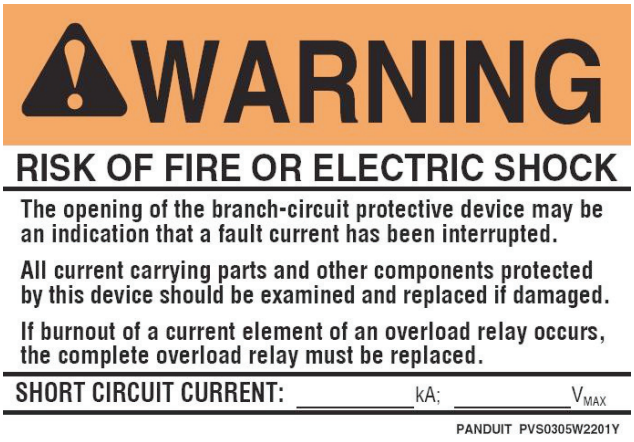
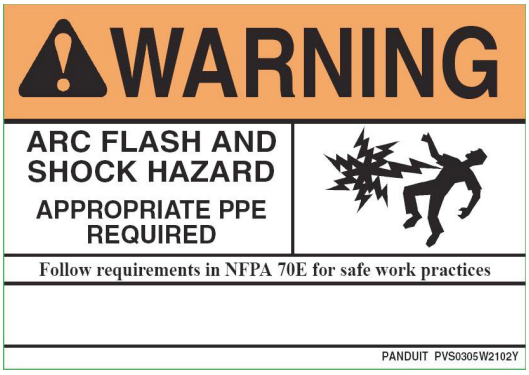


Figure 4.8-7. PANDUIT recommends this label to meet the identification requirement of UL508A, as it provided space to write in the necessary Short Circuit Current Rating information

Figure 4.8-5. Data Access Ports manage risk in industrial settings by providing access to the network without opening the control panel.



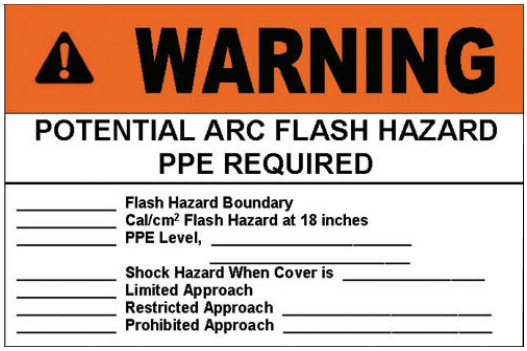


Figure 4.8-6. Arc Flash labels from PANDUIT are recommended for use: (top) label includes space to meet NFPA 70E requirements by writing the available incident energy of the required level of Personal Protective Equipment; (bottom) label contains all of the necessary information for Arc Flash and Shock hazards

4.8.3 INSTALLATION: Security

4.8.3.1 Keyed Systems

Fiber and copper keyed connectivity systems are comprised of all necessary elements (connectors, adapters, patch cords) to deploy a physically secure network infrastructure. These systems employ specialized connectors and adapters that physically prevent access to all but the network for which a user is authorized. The idea is similar to requiring a key to unlock a door.

Color-Coded, Mechanical Keying Functionality. Color-coding ensures visual separation of networks by visually distinguishing connections for user convenience. IT Personnel assign each discrete network its own color, and only connectivity of that color may be used across the channel from outlets and wall plates to zone enclosures and consolidation points.

Positive and negative keying features on each connector match only with corresponding features on similarly colored adapters and/or patch cords. Unwanted connections are prevented by the unique mechanical geometry associated with connectors for each color, keeping multiple networks separate and secure throughout the facility.

These combined features provide true keying security by:

- Limiting network access to specific functional key types
- Preventing the insertion of other keyed and non-keyed connector products that would compromise the secured keyed network
- Ensuring that only authorized personnel perform moves, adds, and changes to the network

Quick Verification of Secure Network Separation. Keyed connectivity systems provide secure data networks with quick visual verification of secure network separation at all points across the channel. These systems ensure that different personnel cannot violate the DMZ through accidental cross-patching, preventing not only a compromise of mission but also a compromise of established physical layer security protocols.

In addition, for installers and similar network technicians working in dense patch field areas, the color-coding on keyed connectivity systems makes it easy to identify correct ports for fast and easy troubleshooting. With best-in-class keyed systems, the chance that a well-meaning user will successfully connect to the wrong network is greatly minimized.

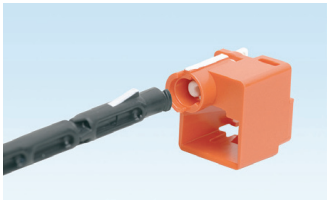
RJ45 Jack Blockout Device

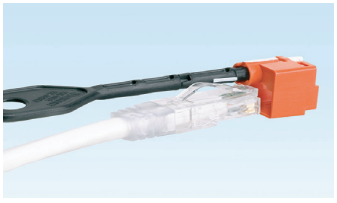
Step 1: To install: snap the blockout device into the jack module

Step 2: To release: insert the special removal tool, which attaches to the blockout device

Step 3: To remove: retract the device

RJ45 Lock-In Device





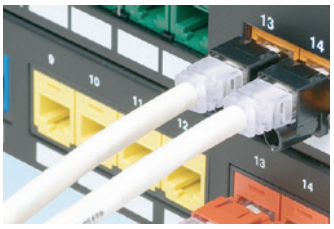
Installing Lock-In device onto RJ45 Plug:

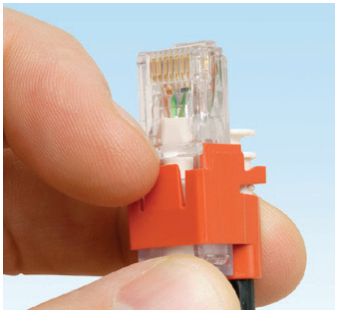
Step 1:
Align white line on tool with white line on device.

Step 3:
Push plug into device until it snaps into place. Check that plug is fully seated in the device.

Step 2:
Insert tool into device and rotate tool clockwise 90°.

Step 4:
Rotate tool counter-clockwise 90° and remove tool from device.



Installing RJ45 Plug Into Jack Insert plug into jack until plug locks into place. Lightly pull on the cable to confirm that plug is locked into the jack.	**Removing RJ45 Plug From Jack** Step 1: Align white line on tool with white line on device. Step 2: Insert tool into device and rotate tool clockwise 180°. Step 3: Remove plug from jack. Step 4: Rotate tool counter-clockwise 180° and remove tool from device.
Removing Lock-In Device From RJ45 Plug Step 1: Align white line on tool with white line on device. Step 2: Insert tool into device and rotate tool clockwise 90°. Step 3: Use a screwdriver or fingernail to release locking tab on bottom of device. While holding release tab, push plug out of the device Step 4: Rotate tool counter-clockwise 90° and remove tool from device.	

4.8.4 Installation: Safety

Several mandatory steps must be taken to deploy an effective lockout/tagout program.

The first step is to conduct a hazard assessment by identifying all equipment that is used, serviced, maintained or stored. All energy sources must be documented, including the type of hazard, the location on the equipment, proper isolation procedure, and lockout device. Next, document the methods used to dissipate the stored energy and verify the isolation.

The second step is to develop a detailed written energy control procedure, which contains the information identified above and also steps to de-energize and re-energize, equipment-specific drawings and diagrams, a list of employees exposed to hazards and qualified to perform lockout/tagout, and the employee in charge of the program.

The third step is to ensure that a robust training program is in place. OSHA mandates that training be given at least annually, but also to new employees or employees with new responsibilities or when new equipment is acquired or a change in machines, equipment or processes presents a new hazard or a change in the energy control procedures.

Levels of lockout/tagout training can be split into two main employee categories:

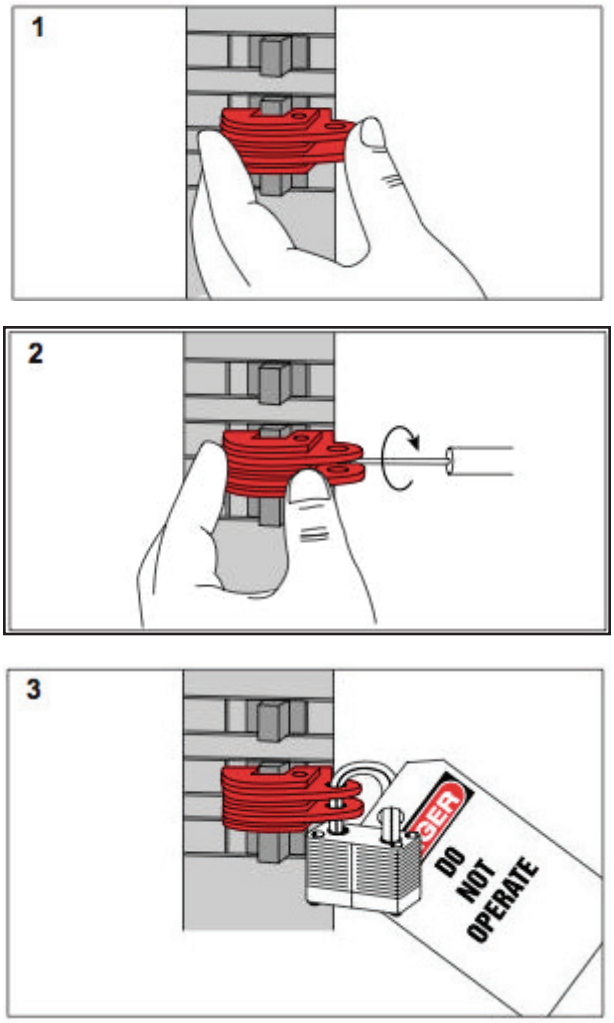
- Authorized employees lock-out and/or tag-out machines or equipment in order to perform servicing or maintenance. Their training should make them proficient in the recognition of hazardous energy sources, the type and magnitude of energy available in the workplace, the methods and means necessary for energy isolation, control and verification of isolation.

- Affected employees are all workers who operate equipment which may be locked out/tagged out during servicing or maintenance, or whose job requires them to work in an area in which such servicing or maintenance is being performed. Their training should instruct them in the purpose and use of the energy control procedure while making it clear that they should never attempt to restart or re-energize equipment which is locked out or tagged out, and that warning tags must be respected.

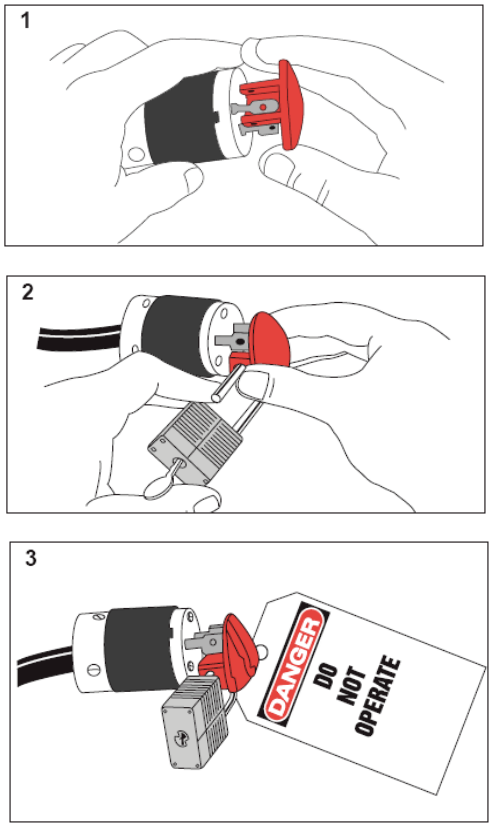
OSHA lists Other Employee as a third category, but for simplicity, Other Employees can be trained in the same fashion as affected employees.

The final step is to perform an annual inspection, which includes not only reviewing the company energy control procedure but also observing an instance of lockout/tagout in progress.

PSL-CB: Circuit Breaker Lockout



PSL-P: Plug Lockout Device



PSL-CBL: Large Circuit Breaker Lockout (for molded-case circuit breakers)	
Step 1: Verify Circuit breaker is de-energized. Place PSL-CBL over breaker with handle centered in lockout opening. Step 2: Turn the toggle set screw knob and tighten firmly against breaker handle.	
Step 3: Rotate/flip the toggle set screw knob down Step 4: Install lock and tag and test for security. Verify that the lockout device secures the breaker handle in an off position.	

PSL-WS: Wall Switch Lockout Device

1. Place the switch in the desired position. If the circuit is controlled by more than one switch, make sure that all switches are in the desired position and have a PSL-WS installed on them.

2. Place the PSL-WS lockout over switch.

3. Tighten the set screw securely with a 1/8” or smaller flat-head screwdriver. Typically,one – to – two (1 – 2)) complete revolutions of the set screw are required after the screw first touches the switch. Do not over tighten the set screw or apply to lighted switches. The switch may fracture.

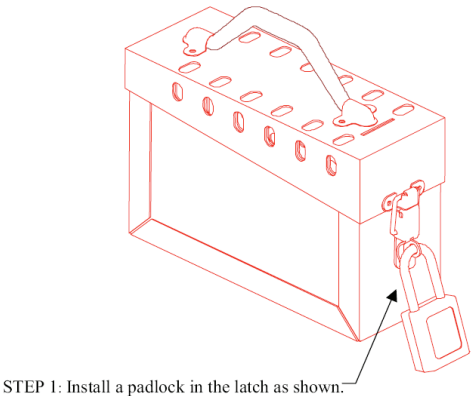
4. Verify that the lockout is adequately secured to the switch.

5. Insert a padlock through both holes. This will prevent access to the set screw. The PSL-WS lockout is designed for use with 9/32” diameter shackle padlocks. Smaller diameter padlocks may not adequately block access to the set screw

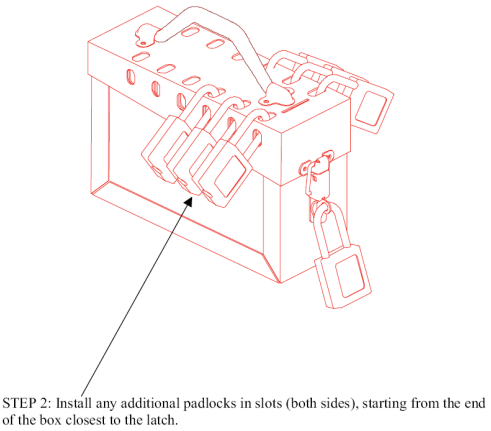
6. Verify that the switch cannot be moved to the undesired position.

7. Attach a safety tag.

PSL-GLB: Group Lock Box

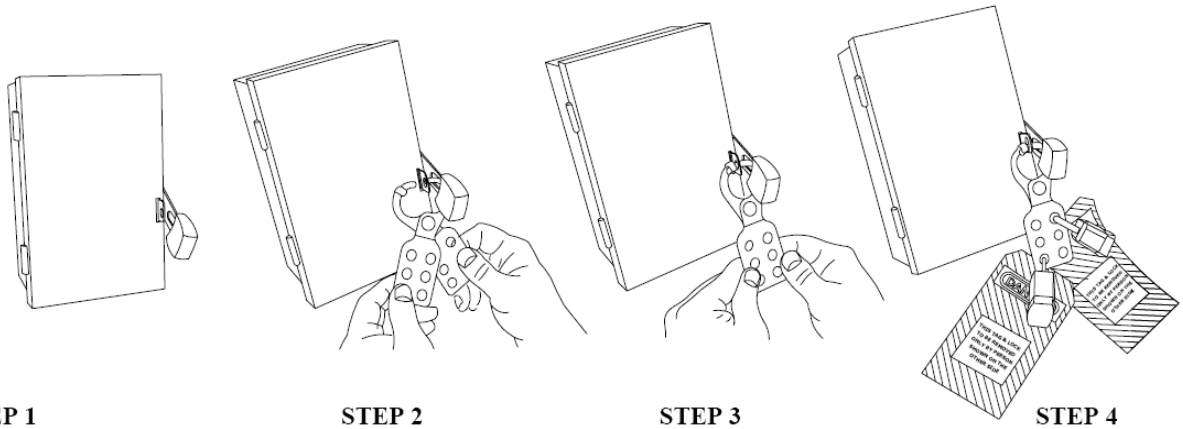


STEP 1: Install a padlock in the latch as shown.



STEP 2: Install any additional padlocks in slots (both sides), starting from the end of the box closest to the latch.

PSL-1 / PSL-1A / PSL-1.5 / PSL-1.5A: Hasps



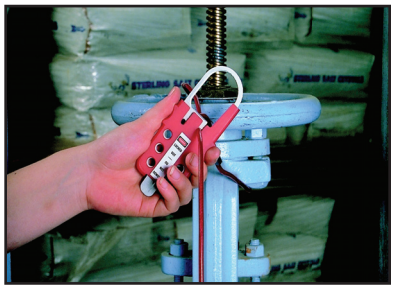
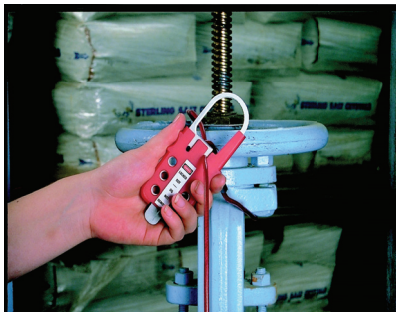
STEP 1
Isolate all energy sources to the equipment.
Test and Verify equipment is de-energized.
Ensure that **ALL** energy sources to the equipment are isolated and release any stored Energy from alternate energy sources.

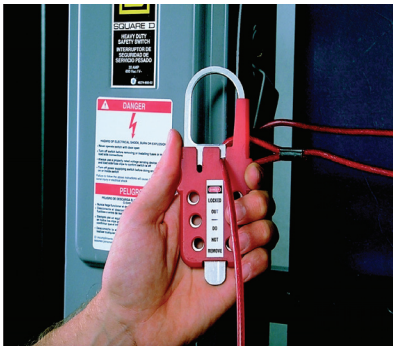
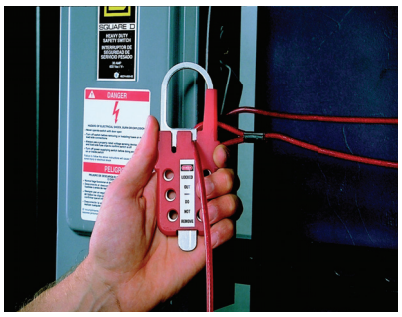
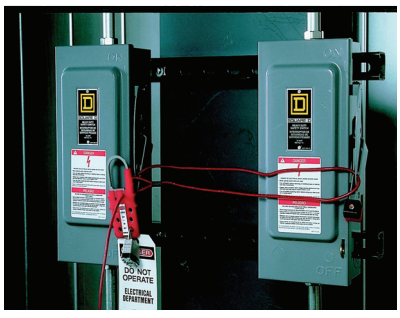
STEP 2
Open hasps Jaws and install onto switch or device to be Isolated.

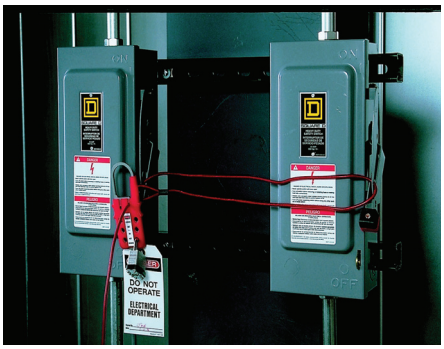
STEP 3
Close hasp so jaws go through the locking hole provided on the device.

STEP 4
Insert up to six padlocks and Danger tags into holes of the hasp.
Verify the disconnect lockout device secures handle in a safe or off position.

PSL-PEL: Pneumatic Lockout Device	
Step 1: Verify valve is de-energized. Thread end of cable through gate valve handle and then through loophole of cable.	
Step 2: Place the opening of the PSL-PEL onto the locking groove of the pneumatic fitting. Use the opening on the PSL-PEL that fits tightest on the pneumatic fitting.	
Step 3: Rotate the PSL-PEL discs to fully enclose the pneumatic fitting. Note arrows that indicate direction of rotation.	
Step 4: Install lock and tag and test for security. Verify that the lockout device fits securely on the pneumatic fitting and that the pneumatic supply line cannot be attached to the equipment.	

PSL-MLD: Multiple Lockout Device (Used as a gate valve lockout device)	
Step 1: Disconnect the pneumatic supply line from the equipment. Protect yourself from any release of pressure in the machine line.	
Step 2: With loophole tight against the gate valve and lockout open, continue threading end of cable through the pre-notched opening of lockout device.	
Step 3: Cinch up plastic lockout body onto cable, forming a secure bond.	
Step 4: Insert up to six padlocks and tags into holes of the hasp. Verify that the lockout device secures the gate valve in a safe or off position.	

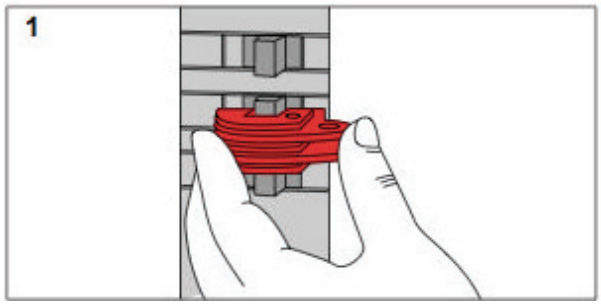
PSL-MLD: Multiple Lockout Device (used as a disconnect switch lockout device)	
Step 1: Verify disconnect is de-energized. Thread cable through holes on each disconnect handle. Insert end of cable through loophole and tightly hold firm near lockout point.	
Step 2: Thread end of cable through pre-notched opening of lockout device.	
Step 3: Cinch up plastic lockout body onto cable, forming a secure bond.	
Step 4: Insert up to six padlocks and tags into holes of the hasp. Verify that the lockout device secures the disconnect switches in a safe or off position.	

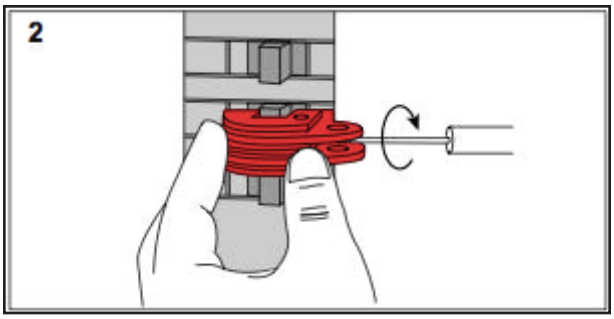


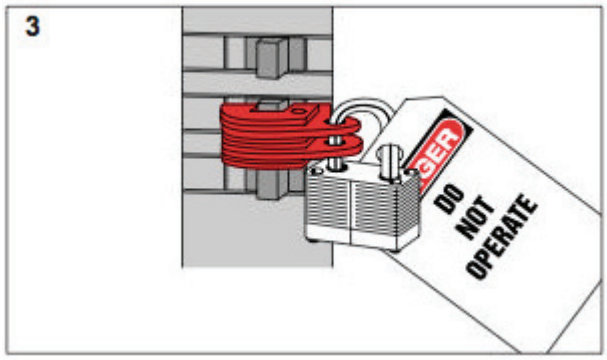
OSHA lists Other Employee as a third category, but for simplicity, Other Employees can be trained in the same fashion as affected employees.

The final step is to perform an annual inspection, which includes not only reviewing the company energy control procedure but also observing an instance of lockout/tagout in progress.

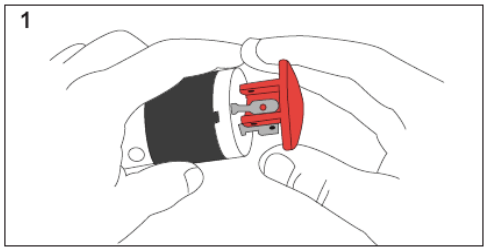
PSL-CB: Circuit Breaker Lockout

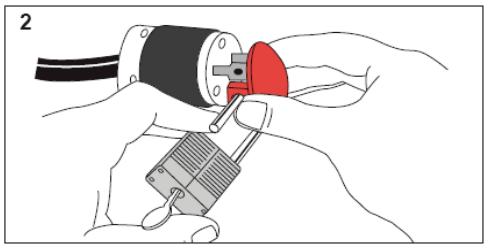


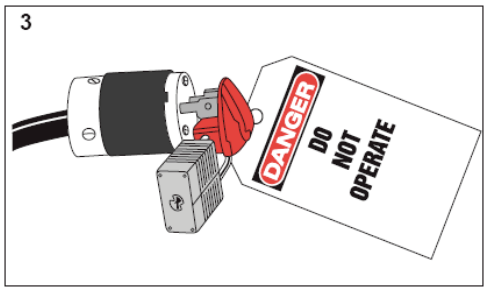




PSL-P: Plug Lockout Device







PSL-CBL: Large Circuit Breaker Lockout (for molded-case circuit breakers)	
Step 1: Verify Circuit breaker is de-energized. Place PSL-CBL over breaker with handle centered in lockout opening. Step 2: Turn the toggle set screw knob and tighten firmly against breaker handle.	
Step 3: Rotate/flip the toggle set screw knob down Step 4: Install lock and tag and test for security. Verify that the lockout device secures the breaker handle in an off position.	

4.9 Wireless Technologies

Integrated wired and wireless networks are an essential element of successful enterprise and industrial environments. The Wireless Local Area Network (WLAN) is a broad term that denotes a wireless network which allows Ethernet data communications as well as other rapidly developing applications. The WLAN can be connected easily to a wired network to allow communication from a wireless client to anywhere within the defined LAN or beyond.

The entry point for the wireless client is the wireless access point (AP), which is a bi-directional transceiver that interfaces from conventional structured cabling of the wired network to radio frequency communications required for wireless client devices. The access point is located at a convenient point –perhaps in the ceiling of the factory floor or another open, public space – and is typically connected to the enterprise computing facilities by means of structured cabling links. This frees client devices on machines and at work stations from being tethered to data outlets, instead using wireless technology to transmit to and receive Ethernet traffic from the closest access point.

Distributed network topologies are increasingly bringing power, switching, and data transfer functions closer to industrial endpoint devices for improved network manageability and scalability. Network stakeholders can use wireless technologies to deliver additional freedom and mobility to users accessing industrial Ethernet networks, as well as added flexibility in deploying wireless-enabled endpoint devices to track assets throughout the warehouse and factory floor.

STANDARDS and CODES

While operation of the wireless network in the United States is unlicensed, it is regulated by the Federal Communications Commission (FCC). The Institution of Electrical and Electronic Engineers (IEEE) 802.11 series of standards defines wireless transmission parameters, including speeds, channels, and operating frequencies for the wireless LAN. Wireless access points operate on a defined channel within the allowable frequency band of operation to reduce direct interference. Typically, equipment will be set to a default channel, but can self-select an alternative channel of operation if excessive interference is detected.

IEEE 802.11a / b / g

Wireless access points on the market today are required to comply with current IEEE 802.11 standards. Several types of multi-standard access points are available, including single-band (802.11b/g) and dual-band (802.11a/b/g) devices.

- The 802.11b standard was released in 1999 and defines wireless operation in the 2.4 GHz unlicensed frequency band at a basic data rate of 11 Mb/s.
- The 802.11a standard was also released in 1999 and defines the wireless operation in the 5 GHz frequency band at a basic data rate of 54 Mb/s.
- The 802.11g standard released in 2003 also operates in the 2.4 GHz frequency band, but at a basic data rate of 54 Mb/s.

Actual data throughput often averages to less than half of the theoretical data rate maximum, depending on the distance of the user to the access point, the number of users sharing the same access point, and the bandwidth required by the applications in use.

IEEE 802.11n (in draft)

The IEEE currently is developing the 802.11n standard, which states a basic data rate of 600 Mb/s in both the 2.4 and 5 GHz frequency bands, with an expected actual data throughput between 100 and 200 Mb/s. The standard is due for release in late 2009, but many “Draft N” products are already available. It is expected that 802.11n products will be backward compatible with 802.11a/b/g products; however, the overall data rate of a mixed network will be limited by the top speed of legacy equipment.

Several new technologies are being implemented in 802.11n access points, including Multiple Input, Multiple Output (MIMO) antenna technology and channel bonding. MIMO technology uses more than one antenna both in the client and within the access point to generate multiple data paths between the client and access point in order to optimize signal reception. With channel bonding, the 802.11n access point uses two separate non-overlapping channels at the same time to increase data throughput, improving over legacy systems which are able to use only one channel at a time.

ANSI/TIA/EIA 42.7 TSB 162; ISO/IEC TR24704

In 2004 the International Organization for Standards (ISO) ratified telecommunications report ISO/IEC TR24704, "Information Technology – Customer Premises Cabling for Wireless Access Points," that outlines a method of integrating APs with the structured cabling infrastructure. The standard defines a cabling grid system for wireless coverage areas, and is popular outside the United States.

In 2006 the ANSI/TIA/EIA 42.7 committee developed Telecommunications Services Bulletin (TSB) 162, "Telecommunications Guidelines for Wireless Access Points," for use in North America. This bulletin proposes two ways to design a coverage area (see Figure 4.9-1): a generic wireless coverage area tailored for North American buildings and a custom-sized coverage area per the building characteristics.

4.9.1 Installing

Because APs are commonly positioned in public areas outside the telecom room or closet, they can be subject to tampering or theft. Therefore APs should be mounted either on the wall or ceiling in secure and aesthetically pleasing enclosures that minimally affect the RF signal propagation. Such enclosures offer protection from harsh industrial environments, and must integrate with the rest of the network infrastructure by offering provisions for conduit or raceway, a demarcation outlet, and grounding.

Access points require data traffic backhauling to the wired network. The format of this traffic is 802.3 10/100/1000BaseT Ethernet traffic, which travels over Category 5e cable or greater. Installing Category 6 cable is recommended, depending on equipment evolution, to extend the life of the network cabling infrastructure. Cabling infrastructure should comply with ANSI/TIA/EIA-568-B.1, TIA-569-B, and forthcoming TIA-1005.

4.9.1.1 Network Architecture Options

Two common logical architectures are used to deploy wireless networks: individually managed wireless access points are known as "autonomous" or "distributed", and centrally managed wireless access points are termed "lightweight" or "centralized". In an autonomous architecture, each AP supports all necessary switching, security, and advanced networking functions necessary to route wireless traffic (see Figure 4.9-2). In this sense, autonomous APs are similar to a traditional Ethernet switch that provides data connectivity to end users, since a wireless controller is not required.

In contrast, lightweight WLAN architecture hardware consists of APs that operate in conjunction with a centralized wireless controller. The difference between the physical infrastructures of lightweight and autonomous WLAN architectures is minimal; the only additional component in a lightweight architecture is the wireless controller. The APs reside at the edge (access layer) of the network to support the Physical Layer (PHY or OSI Layer 1) as well as the real-time portions of Media Access Control management, and the controller resides deeper in the LAN network at the distribution or possibly at the core layer (see Figure 4.9-2).

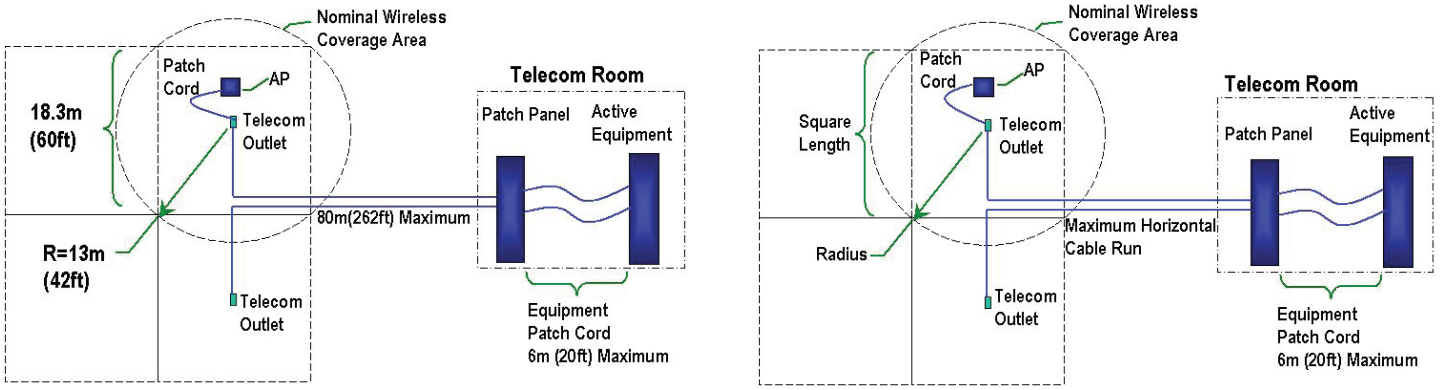


Figure 4.9-1. ANSI/TIA/EIA 42.7 TSB 162 - Generic (left) and Custom (right) Wireless Cell Size

Larger industrial AP deployments usually use lightweight architectures due to the operational cost efficiencies that can be achieved via group management of lightweight APs. Autonomous APs require individual management: any configuration changes can be accomplished via the console port session, a telnet session, a Web connection, or SNMP commands. If a change must be made across the entire WLAN network, every autonomous AP must be individually reconfigured. Also, autonomous APs usually have no visibility or control of neighboring APs, and thus cannot perform self-healing, client load balancing, or other advanced radio resource services.

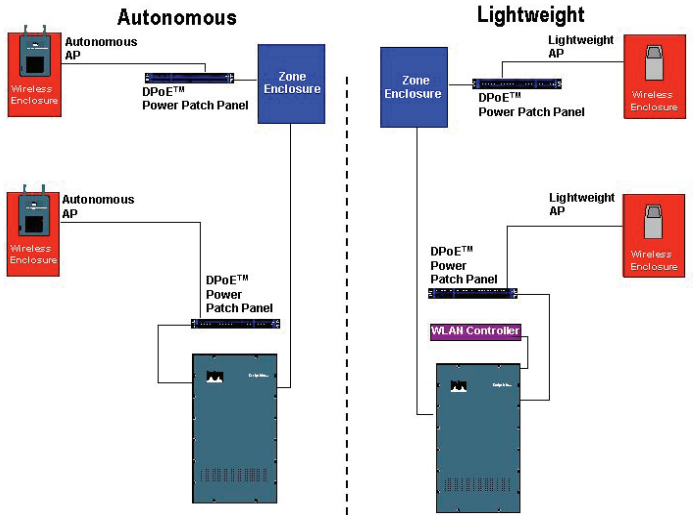


Figure 4.9-2. Physical Layout Showing AP Deployments Powered by PoE Technologies

In contrast, a lightweight architecture eases management of large deployments by controlling all APs from a single device. Because the lightweight APs also have visibility and awareness of their neighboring APs, they can supervise and alert the wireless controller if one of their neighbors becomes faulty. Lightweight WLANs can be self-healing because the controller commands neighboring APs to adjust their power levels to compensate for a failed counterpart. In addition, the wireless controller can offload wireless clients to a neighboring AP if a single AP becomes overloaded. These load balancing and self-healing capabilities mitigate production downtime risks by preventing disruptions to mission-critical applications and processes.

For smaller wireless deployments requiring only a few APs, the WLAN can be designed using autonomous APs. As wireless coverage is expanded with the addition of APs, the solution can be converted into a centralized lightweight architecture. Migration from an autonomous to a lightweight solution is possible with the addition of the wireless controller and an operating system upgrade to selected Cisco APs. A lightweight WLAN solution will in turn ease network-wide policy and security implementations that are of critical importance for large scale deployments.

4.9.1.2 Power

Typically APs will operate at 48 volts of DC power. There are several ways to provide power to access points:

- ***Brick" Type***. A "brick" type power supply is used in the proximity of the access point to convert from 110 volts AC to the required 48 volts DC and supply this to the access point. This then means that the power supply and access point is in the vicinity of a power outlet. This may not be the case for a ceiling mounted access point and the center of a room in an office – and the cost associated with installing a new power outlet can be prohibitive.

- ***Power Injector.*** This is an electronic device that is fed either from a power supply above or from the 110 volt outlet directly, and that provides the appropriate DC voltage on the access point side of the structured cabling. In this way the access point can be powered, but the power supply can be located at a more physically convenient point in the network.

4.9.1.3 Power over Ethernet

Power over Ethernet (PoE) technologies enable WLAN managers to power access points over the network and realize the benefits of ease and speed of deployment, ease of management, and enhanced security (see Section 4K of this document). PoE solutions to power APs are very common in industrial networks as access points often are installed long after the building is finished. This compels network stakeholders to find a power solution that avoids the cost of running new AC outlets and eliminates the expense of power adapters.

The IEEE 802.3af PoE standard allows for a maximum of 15.4 W to be delivered by Power Sourcing Equipment (PSE) to powered devices. Upcoming standard IEEE 802.3at (expected to be ratified in 2009) would increase power delivery

to a minimum of 25 W at up to 45°C maximum ambient temperature over Category 5e, 6, and 6A copper cabling. Some 802.11n access points may draw more power than provided under 802.3at; in these situations, single-port power injectors may be used to accommodate the additional power requirements of these devices.

4.9.1.4 Effective Range

A significant amount of published specification information from the access point vendors states that the access point can operate reliably typically up to 300 ft. This distance applies in an open, unobstructed environment. In reality, the effective range is very dependent on the type of building construction materials used and the specific deployment of obstacles within the building. For example, in a typical building with concrete walls with steel reinforcing bars and light drywall panels for offices or light office furniture, the coverage distance will be less than 300 ft.

TSB-162 balances the needs of coverage from the wireless perspective consistent with meeting performance requirements in the structured cabling system that is used to link the access points to the wired network. The bulletin focuses on a distance of 60 ft as a starting point for consideration of the distance between access points in commercial buildings. However, industrial environments can contain metal surfaces that could reflect RF signals and affect their propagation. Therefore, we recommend that network stakeholders use an RF planner and conduct a site assessment (and in some circumstances an actual site survey) to determine the exact coverage areas and requirements.

4.9.1.5 Security

Wireless technology has developed effective security standards to provide user authentication and authorization. The IEEE 802.11i standard outlines authentication and encryption mechanisms to secure wireless connections. Authentication is accomplished in the same way on a WLAN as it is on a wired LAN, as outlined in the IEEE 802.1X standard. 802.1X provides a framework for mutual authentication (client and network equipment) before a connection becomes active. Data confidentiality is protected with encryption mechanisms such as Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES). Confidentiality **across multiple networks can be ensured with a Virtual Private Network (VPN).**

WLAN security also exists at the physical layer – specifically, sturdy yet aesthetic metal enclosures should be used to provide security and physical protection to access points. IP-rated industrial enclosures include such features as sealed antenna bulkheads, gland plate(s), and vibration-mitigating backplates. Apertures must be drilled in these enclosures to accommodate conduit, cables, and antennas associated with the access point.

WLAN security can be enhanced by remote management capabilities. During the workday, for example, RFID-enabled badges can allow the location of human resources to be monitored across the facility, an application which can be critical in sensitive or high-security business or government environments. Then overnight, remote management of the wireless system permits selective shutdown of access points in order to discourage unauthorized users from attempting to log on to the WLAN while providing coverage for the limited number of authorized users and keeping mission-critical security applications functional (badge-in/badge-out, asset tracking).

4.9.2 Testing

Per ANSI/TIA/EIA TSB 162, cabling should be installed and tested in accordance with TIA/EIA-568B (see Section 4.1 of this document for testing procedures).

4.9.3 Documenting

The process of documenting your industrial wireless network is to aid in troubleshooting and reduce the time required for routine maintenance and moves, adds, and changes. The following are considered essential elements and processes to document:

1. All site surveys conducted to determine access point placement and coverage areas
2. Blueprint or floor plan showing current physical location of each access point and associated cabling
3. **Current configuration, IP address, and security** (i.e., WEP/WPA) settings for each access point
4. Up-to-date maintenance log documenting all moves, adds, and changes
5. Up-to-date labeling information on physical infrastructure (cables, enclosures, etc.) in accordance with TIA-606A.

Building a Wireless Solution

Note: Part numbers given in these tables are illustrative only. A detailed review of required part numbers must be carried out specific to each deployment.

Standard / Technology	Wireless Access Point Panduit Part Number	PanZone ® Enclosure Panduit Part Number
802.11 a/g Distributed, Internal Antennas	P-AP1131AG-A-K9	PZWIFIEW
802.11 a/g Centralized, Internal Antennas	P-LP1131AG-A-K9	PZWIFIEW
802.11 a/g Distributed, External Antennas	P-AP1242AG-A-K9	PZWIFIED
802.11 a/g Centralized, External Antennas	P-LP1242AG-A-K9	PZWIFIED
802.11 a/g/n Draft Distributed, External Antennas	P-AP1252AG-A-K9	PZWIFIEN
802.11 a/g/n Draft Centralized, External Antennas	P-LP1252AG-A-K9	PZWIFIEN

Panduit Part Number Types for the Outdoor / Industrial Environments

Standard / Technology	Wireless Access Point Panduit Part Number	PanZone ® Enclosure Panduit Part Number
802.11 a/g Distributed, Internal Antennas	P-AP1131AG-A-K9	PZNWE12
802.11 a/g Centralized, Internal Antennas	P-LP1131AG-A-K9	PZNWE12
802.11 a/g Distributed, External Antennas	P-AP1242AG-A-K9	PZNWE12
802.11 a/g Centralized, External Antennas	P-LP1242AG-A-K9	PZNWE12
802.11 a/g/n Draft Distributed, External Antennas	P-AP1252AG-A-K9	PZNWE12
802.11 a/g/n Draft Centralized, External Antennas	P-LP1252AG-A-K9	PZNWE12

4.10 Power over Ethernet

Power over Ethernet (PoE) is an established technology that extends the utility of Ethernet connectivity by providing reliable low-voltage DC power delivery to network devices over the same Category 5e and Category 6 cabling infrastructure that traditionally have only carried data.

To implement PoE in a new or existing Industrial Ethernet network, organizations have a choice of varied solutions that include PoE-enabled network switches, midspan power sourcing equipment (PSE), powered patch panels, and single port injectors.

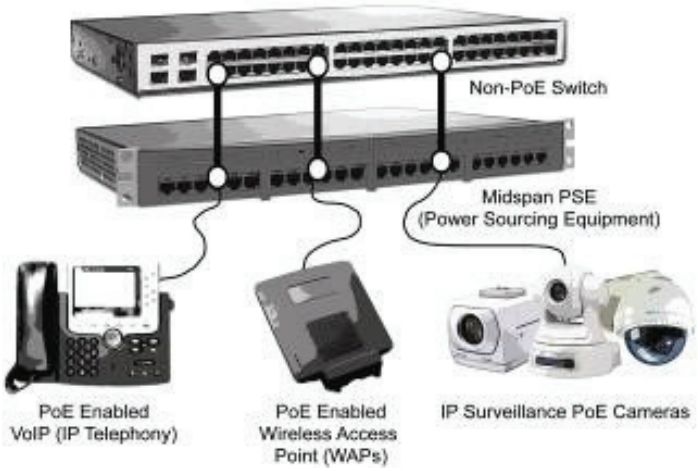


Figure 4.10-1. Applications currently driving the adoption of PoE include Voice over Internet Protocol (VoIP) phones, wireless access points (WAPs), and IP security and surveillance cameras.

PoE offers two benefits that are consistent across applications: cost savings and flexibility of device placement. Because PoE runs data and power together over the same cable to each device attached to the local area network (LAN), devices can be installed without the need for a dedicated AC outlet. This saves money by eliminating the cost and time associated with AC outlet installations, while providing the flexibility to locate PoE devices where performance is optimum.

Also, by using a centralized power source, PoE offers the ability to remotely power and manage connected devices in the event of service disruptions or reconfigurations, and helps manage power sources and battery backups to protect against power outages and spikes. These benefits have helped PoE gain rapid traction in industrial environments for the deployment of wireless access points (WAPs) placed in locations that are difficult to access manually (i.e., attached to high ceilings or above active machinery), which minimizes production downtime and simplifies WAP reconfiguration tasks.

Industrial security applications such as network surveillance cameras, electromagnetic door locks, and radio frequency identification (RFID) systems are beginning to see wider integration with PoE due to reduced power demand from client devices and greater availability of pre-standard PoE Plus equipment.

STANDARDS and CODES

IEEE 802.3af and 802.3at

Since acceptance of the IEEE 802.3af Power over Ethernet standard in 2003, equipment vendors have been designing standards-based products that leverage the numerous advantages and benefits offered by PoE technologies (see Figure 4.10-1). The newer PoE Plus standard is being written to accommodate more power hungry devices such as PLC devices, HVAC units, specialized industrial lighting, motorized (i.e., point-tilt-zoom, or PTZ) network cameras, proximity sensors, or other security apparatus.

- Under IEEE 802.3af, 15.4 W of power are available for each powered device with a maximum DC current of 350 mA per pair, which is adequate for most current PoE applications.

- New standard IEEE 802.3at (commonly referred to as PoE Plus) is expected to be ratified in mid-2009. The standard would increase power delivery up to a minimum of 25 W at a maximum DC current would be 720 milliamps (mA) per pair (or 360 mA per conductor), up to 45°C maximum ambient temperature over Category 5e, 6, and 6A copper cabling. PoE also helps protect network investments, as it is an extension of the established 802.3 Ethernet protocol and is supported under 10Mbps, 100Mbps, 1Gbps and eventually 10Gbps.National Electric Code (NEC) – Safety Extra Low Voltage (SELV) PoE conforms to Underwriters Laboratories (UL) Safety Extra Low Voltage (SELV) classification.An SELV circuit provides extra-low voltage define as <120V DC by the International Electrotechnical Commission

(IEC) which has a low risk of accidental contact with a higher voltage and lacks a return path through earth (ground) that electrical current could take in case of contact with a human body. An SELV circuit typically involves an isolating transformer, guaranteed minimum distances between conductors and electrical insulation barriers. SELV circuits via PoE are designed to transmit power over Ethernet cabling and terminate to an RJ45 connector which would not normally mate with non-SELV circuits.

4.10.1 Developing Industrial Applicaitons

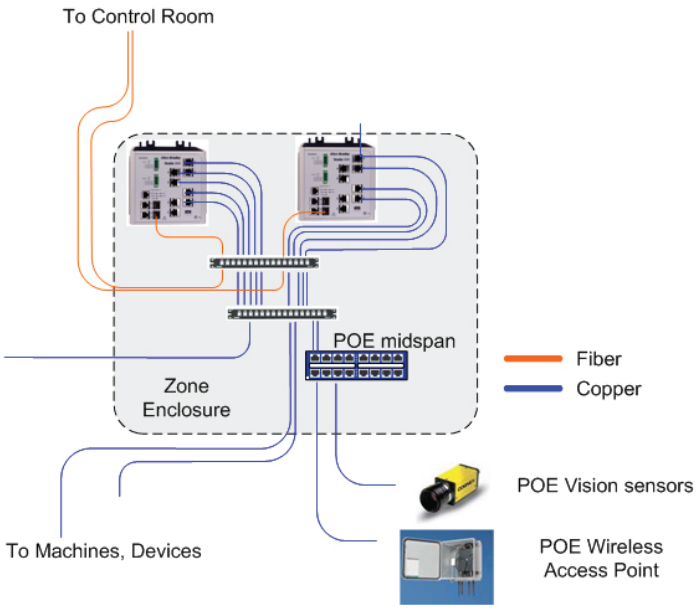


Figure 4.10-2. Hybrid PoE / Logic Control

PoE is pushing into the automated factory environment by providing distributed power and networking for typical devices found in commercial areas such as wireless access points (APs) and video cameras (see Figure 4.10-2). The exciting new application for PoE is to use this approach to power I/O devices which meet the PoE power budget. For example, Ethernet-based vision sensors currently exist that will work with existing PoE-level power. It is anticipated that a greater range of devices available as the PoE standard evolves to support higher power levels, and as endpoint devices are engineered for lower power. Distance limitations are being overcome through fiber distribution through the zone cabling consolidation points and edge switching into the areas of the factory where control and automation is required.

IP SURVEILLANCE

When combined with Power over Ethernet (PoE) systems, IP surveillance devices offer unique opportunities to lower an organization's total cost of network ownership through scalability, flexibility of device placement, and cost-effective deployment. Remote manageability of PoE-enabled devices gives organizations the ability to access, manage, and control power to cameras that are placed in inaccessible or hard-to-reach areas on the factory floor. Functions such as camera resets and calibration of connected devices can be performed either at an internal management workstation or from an external web access point, without the need to physically touch a device that is placed out of reach.

The use of these devices can broaden enterprise security initiatives without the expense of proprietary hardware and software, or traditional CCTV equipment purchases such as multiplexers, repeaters, and signal splitters. With a digital signal, camera views can be monitored over a virtually unlimited number of screens by utilizing almost any workstation with a common web-browser. In addition, digitizing the camera signal enables the use of IP multicast solutions and enhanced hard-disk based recording devices and storage options not available with traditional CCTV systems (see Figure 4.10-3).

PoE systems also increase the reliability of security networks by providing cost-effective centralized backup power to all connected IP surveillance devices. Surveillance cameras

are essential to the security of many organizations, and keeping these devices reliably operational is critical. During local power interruptions, a single UPS unit supporting a PoE powered patch panel can provide seamless, reliable power for all surveillance cameras connected to it. Centralized backup power through PoE offers the additional benefit of increased reliability, lower total cost of ownership through simpler maintenance procedures, easier monitoring, and higher efficiency than a traditional system would offer.

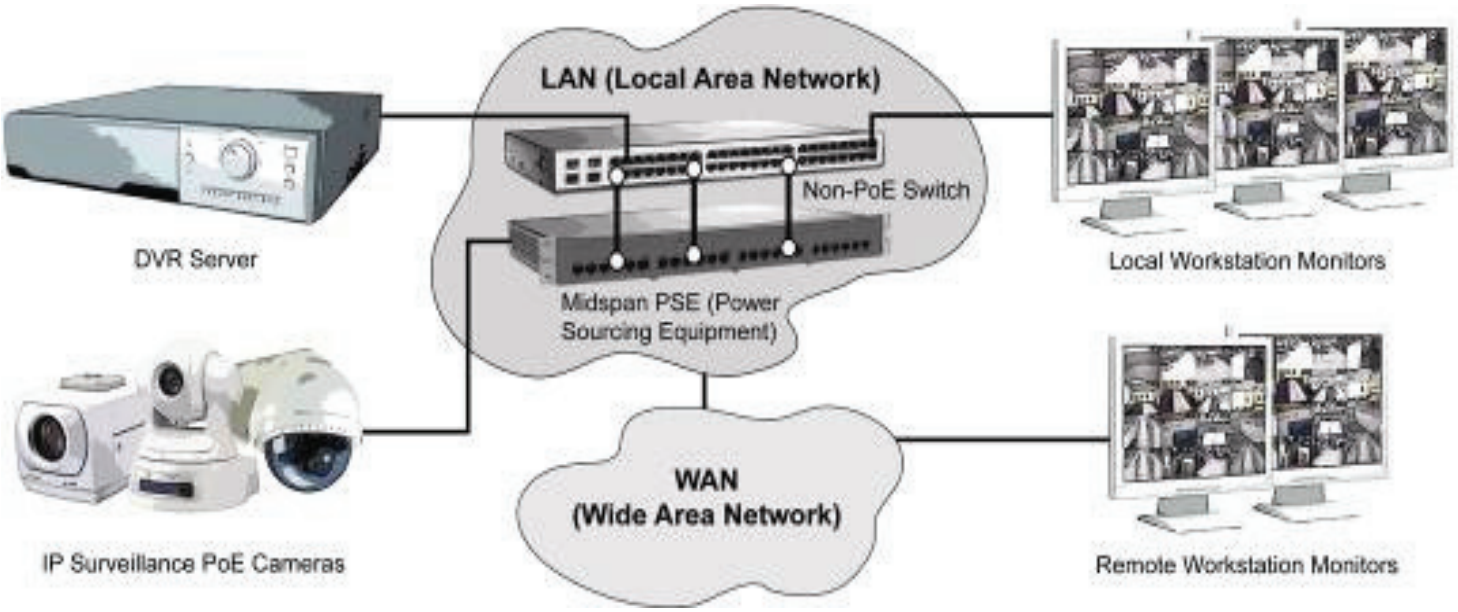


Figure 4.10-3. With the ongoing digitalization of security and surveillance systems organizations today can take advantage of Ethernet, Internet, or wireless technologies as the backbone of their security infrastructure to gain the advantages of greater device capabilities, network convergence, interoperability, and remote or local accessibility.

Radio-Frequency Identification (RFID) Systems

RFID is gaining popularity as another application which can leverage the advantages of PoE, with some analysts projecting the deployment of up to 2 million PoE-enabled RFID readers by 2010. A fully implemented, warehouse-wide RFID system can track shipping containers or a pallet's movement from the time the pallet enters the warehouse to the time it leaves. These systems rely on fixed RFID readers placed throughout the warehouse and at other points between receiving and shipping (see Figure 4.10-4). Each reader must be powered as well as able to transmit data: an immediate and natural match for PoE. Cost savings achieved through reduced installation times and reduced multiple cable pulls make PoE enabled RFID systems a logical choice for improves asset management as new systems are being installed.

Also, unlike WiFi which has a relatively large coverage radius, RFID readers must be spaced strategically and closer together along the entire inventory flow route for accurate asset tracking. Proprietary tracking systems typically require system elements to be hard wired according to number of monitored nodes. However, PoE-enabled RFID readers become part of the network fabric and can be increased or reconfigured as the needs of the business change by increasing or decreasing corresponding PoE ports. Unused PoE ports may be utilized for other functions such as network surveillance cameras which when combined with RFID asset tracking maximize security in warehousing and enterprise applications.

Retailers benefit by reduction of inventory shrinkage, elimination of incorrect deliveries (at the receiving dock), and an improvement in distribution logistics. End customers achieve greater satisfaction as retailers benefit in reduced stock outages as the result of being able to track a pallet's movement through the warehouse.

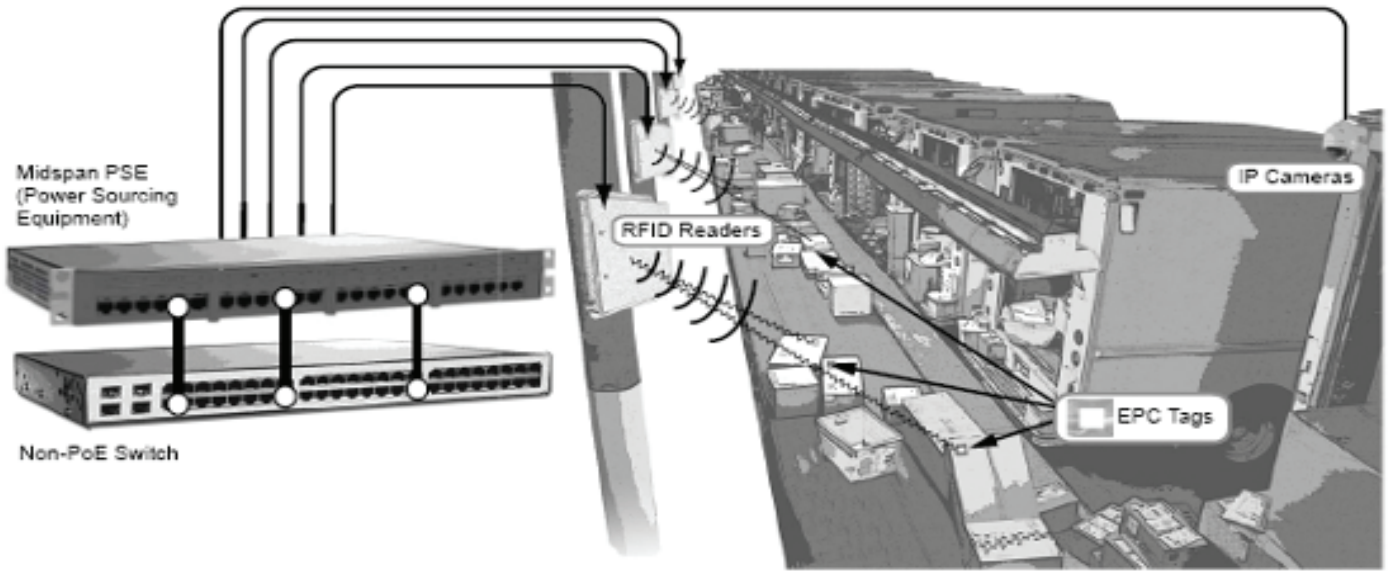


Figure 4.10-4. PoE enabled RFID readers track assets through shipping & receiving via Electronic Product Code (EPC) tags which respond with detailed product, container and location information. PoE cameras provide additional security to correlate asset movement and human interactions.

4.10.2 Installing

Distance requirements for PoE deployments are currently limited to 100m, in accordance with TIA/EIA specifications for Category 5e and Category 6 copper cabling limits.

Wiring schemes for RJ45 connectors on cables carrying PoE are not affected by PoE deployments, and should be terminated under conventional RJ-45 procedures and in accordance with TIA/EIA-568A and -568B.

For existing PoE installations, the specified current and power limits were designed to maintain cabling temperature rise of less than 10°C degrees and a maximum cabling temperature lower than 60°C (i.e., the sum of ambient temperature and expected temperature rise in cabling). Most fixed-direction network surveillance cameras and RFID readers can run on the 15.4 W of power provided under the current IEEE 802.3af standard using existing Category 5e or 6 cabling. Therefore, in most cases, these lower power levels do not present significant concerns regarding the heat rise over twisted-pair bundles.

However, devices such as room sensors, electronic door locks, and other building controls may require up to 25 W per device to operate. These devices would be powered over twisted pairs in conformance with the upcoming PoE-Plus standard, and the amount of heat generated in cable bundles at these higher power levels must be addressed.

Under PoE Plus, the maximum power transmitted over any individual cable bundle should not exceed 5,000 W up to an ambient temperature of 45°C. At temperatures from 45-60°C it is recommended to reduce the power output and or power consumption (i.e., de-rate the system) until the ambient temperature falls back to 45°C.

The de-rating process can include several strategies such as reducing the number of cables in the bundle, or improving the mix of PoE / PoE Plus powering to reduce the number of powered endpoints on a particular cable span. Also, higher performing cables with lower DC resistance (e.g., Category 6 and 6A) tend to generate a lower temperature rise and therefore have fewer associated bundling constraints.

4.10.3 Testing

Fluke has updated the firmware in their DTX-1800 series cable tester to support PANDUIT DPoE™ 1GIG™ Power Patch Panels. The new DTX V1.41 firmware supports two-pair (1,2) & (3,6) PoE channel and permanent link testing over Category 5e and Category 6 twisted-pair cabling as well as AC Wire Map testing, and is available on the Fluke website at: http://www.flukenetworks.com/fnet/en-us/products/DTX+CableAnalyzer+Series/Downloads.

Unlike traditional DC testing methods, testing capabilities are being introduced that utilize AC signals to perform Wire Map measurements that are not blocked by Power over Ethernet (see Figure 4.10-5). This technique provides visibility of each wire in the cable to ensure that the wire pairs are correctly connected and that power will be properly supplied to powered devices.

Category 5e and Category 6 channel and permanent link testing for the DPoE™ 1GIG™ Power Patch Panel can be done by configuring the Fluke DTX-1800 series cable analyzer as follows. Once the configuration settings are set, the DTX-1800 series cable tester is ready to perform any necessary testing. Two examples of expected test results are shown in Figure 4.10-6.

(NOTE: The DPoE™ 1GIG™ Power Patch Panel should NOT be powered during testing.)

The Agilent WireScope Pro N2640A also is capable of testing through midspan PoE devices.

With the V1.41 firmware installed, go to SETUP >> highlight Twisted Pair, hit Enter >> on following screen, hit the right arrow to go to tab 2>> highlight AC Wire Map, hit Enter >> highlight Enable, hit Enter.

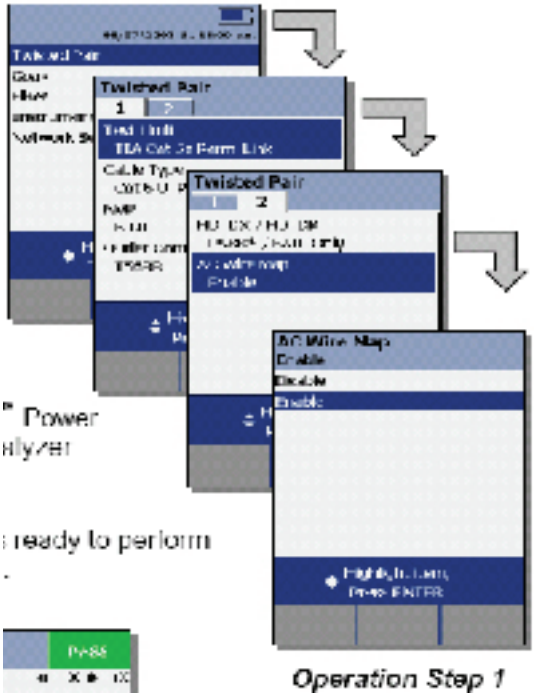


Figure 4.10-5. AC Wireman Testing Procedure

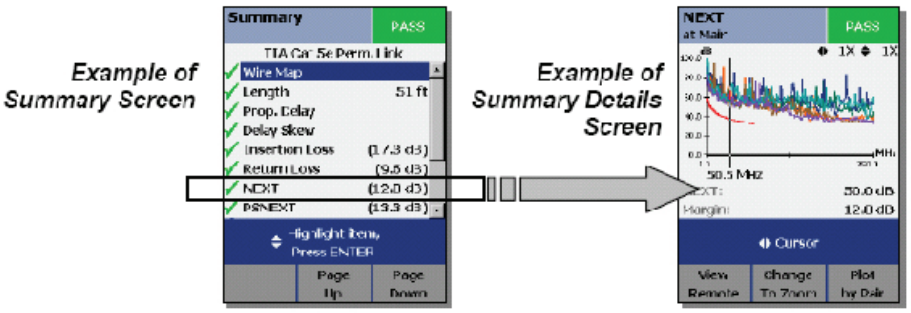


Figure 4.10-6. Example PoE Test Results from Fluke DTX-1800 Series Cable Analyzer

4.10.4 Documenting

Component Labels for *DPoE*™ Power Patch Panel

Suggested Label Solutions for TIA/EIA-606-A Compliance				
Patch Panel Part Number	Laser/Ink Jet Desktop Printer Label	TDP43MY Thermal Transfer Desktop Printer Label	*PanTher*™ LS8E Hand-Held Printer Label	*Cougar*™ LS9 Hand-Held Printer Label
Patch Panel on Page D.3	UILJ6	—	UILS8BW	UILS8BW

Component Labels for *DPoE*™ Power Midpsan

Suggested Label Solutions for TIA/EIA-606-A Compliance				
Patch Panel Part Number	Laser/Ink Jet Desktop Printer Label	TDP43MY Thermal Transfer Desktop Printer Label	*PanTher*™ LS8E Hand-Held Printer Label	*Cougar*™ LS9 Hand-Held Printer Label
DPOE8S2XG	UILJ4	—	UILS8BW	UILS8BW
DPOEPL8BU	UILJ4	—	UILS8BW	UILS8BW

Building a PoE Solution

DPOE24UIXG

ULTIMATE ID

Part Number	Part Description	No. of Rack Spaces^	Std. Pkg. Qty.
DPOE24U1XG	24-port UTP 1 GbE 10/100/1000 patch panel supporting IEEE 802.3af-2003 and legacy PoE power protocols. Includes Element Manager software CD, rack mount screws, grounding strap and lug.	1	1

^One rack space = 1.75" (44.45mm).
Strain relief bars for mounting can be found on page B.55.
Power supply and/or power system sold separately.

DPOE8S2XG

DPOE8KIT

DPOEWM8B

DPOEPL8BU

DPOESHELF

Part Number	Part Description	No. of Rack Spaces^	Std. Pkg. Qty.
DPOE8S2XG	8-port STP 10/100/1000 midspan supporting IEEE 802.3af-2003 and legacy PoE protocols. Option for table top mounting, wall bracket, or 1 RU shelf. Includes Element Manager software CD.	1	1
DPOE8KIT	Compact 8 midspan kit includes individual unit, 120 watt power supply, and 15 A conductor power cord.	1	1
DPOEWM8B	Wall mount bracket for DPOE8S2XG.	1	1
DPOEPL8BU	8-port passive patch panel module.	1	1
DPOESHELF	1 RU shelf for DPOE8S2XG.	1	1

^One rack space = 1.75" (44.45mm).
Power supply and/or power system sold separately.

DPoE™ Power System

- Offers 48 volt DC power that is scalable from 500 watts to 3,750 watts
- Utilizes high efficiency power supplies that can be hot swapped for upgrades or replacement without taking the entire system down
- Provides consistent powering across a wide range of devices and application needs
- Offers a low profile, one rack space design
- Emits 35% less heat compared to other power supply systems
- Increases reliability with problem fault isolation

DPOEPWRCU

DPOEPWRR500 / DPOEPWRR1250

Part Number	Part Description	No. of Rack Spaces^	Std. Pkg. Qty.
DPOEPWRCU	Power system chassis. Utilized for supplying power to single and multiple power patch panels when equipped with the appropriate *DPoE*™ Power Rectifiers.	1	1
DPOEPWRR500	500 watt power rectifier supplies power for multiple power patch panels. A combination of three rectifiers will support four to seven panels. Used with DPOEPWRCU.	—	1
DPOEPWRR1250	1250 watt power rectifier supplies power for multiple power patch panels. A combination of three rectifiers will support up to fourteen panels. Used with DPOEPWRCU.	—	1

^One rack space = 1.75" (44.45mm).
Power system chassis requires proper A.C. country specific power cord (CORD-A for Australia, CORD-E for Europe, CORD-S15 for United States, CORD-J15 for Japan or CORD-U for United Kingdom) must be ordered separately.

4.11 Connected Building Solutions

Enterprises today require the spaces they occupy to be designed to support a wide variety of building systems and cutting-edge communications technologies. Traditional building systems such as lighting, security, HVAC, structural health monitoring, and energy management now must co-exist with IP-based voice, data and video communication technologies.

The terms “Intelligent” or “Connected” Building have evolved to reflect these changes in building systems design and construction. Once used to denote structures with automation features that offered improved control over various building systems, today’s Connected Buildings are designed with extensive system convergence and interoperability in mind.

A connected building has the ability to share or leverage data between disparate systems to achieve a more efficient process. This is accomplished by reducing energy operation cost and providing a comfortable safe work environment. Linked facility and network systems are now built directly into the building fabric, generating and sharing data over a single platform to enhance the efficiency and effectiveness of the building as a whole.

Some examples of an industrial connected building include the following:

1. In the event that a plant’s main power-feed experiences a phase loss, the alarm message can be communicated through the switchgear control via a communication protocol like modbus. This message can be sent to a middleware platform where a software policy can be written to send an e-mail alarm messages to the facilities group, local service provider, and even the industrial machines’ HMI.

2. Facilities HVAC systems can share temperature and humidity information between the HMI or to the facilities control operators interface, which can be beneficial for critical machining processes. Other data points such as start/stop/status of a machine or machine maintenance schedules can be maintained.

3. Remote access for system status, control, alarming, logging, trending.

4. Card Access control and security. The card access system can be set up so that an employee has to scan their ID on a machine in order to have the machine power up. These ID credentials can ensure that the employee has been trained and authorized to use this equipment.

Installation

The phases to a successful installation of information technology cabling in industrial environments include:
Phase 1: Design – the selection of cabling components and their configuration. A Unified Physical Infrastructure (UPI)-based solution should be considered.
Phase 2: Specification – the detailed requirement for the cabling, its accommodation and associated building services addressing specific environment(s) identified within the premises together with the quality assurance requirements to be applied.
Phase 3: Implementation – the physical installation in accordance with the requirements of the specification.
Phase 4: Operation – the management of connectivity and the maintenance of transmission performance during the life of the cabling.

Multi-Technology Cable Bundle to Physically Converge Systems

Connected Building Solutions are based on running a multi-technology cable bundle along shared pathways in order to extend the reach of a physically converged infrastructure to all devices and systems. By capturing and transporting all operational and services data over a physically converged infrastructure, it becomes possible to implement facility-driven policies that support business requirements and tenant/customer demands. Most systems can be physically converged through shared conduit, cable trays, and building pathways; others will converge through a switched IP network.

The physical layer provides the foundation for key building and enterprise systems to communicate both locally and remotely. PANDUIT Connected Building Solutions complement Cisco and Rockwell Automation logical network architecture solutions by allowing building systems to converge and extend the reach of the IP-based network to all devices within an enterprise. Connected Buildings can interface and share information through a common gateway or middleware (see Figure 4.11-1); the gateway uses various drivers to normalize the data to be converged or integrated for a more efficient process.

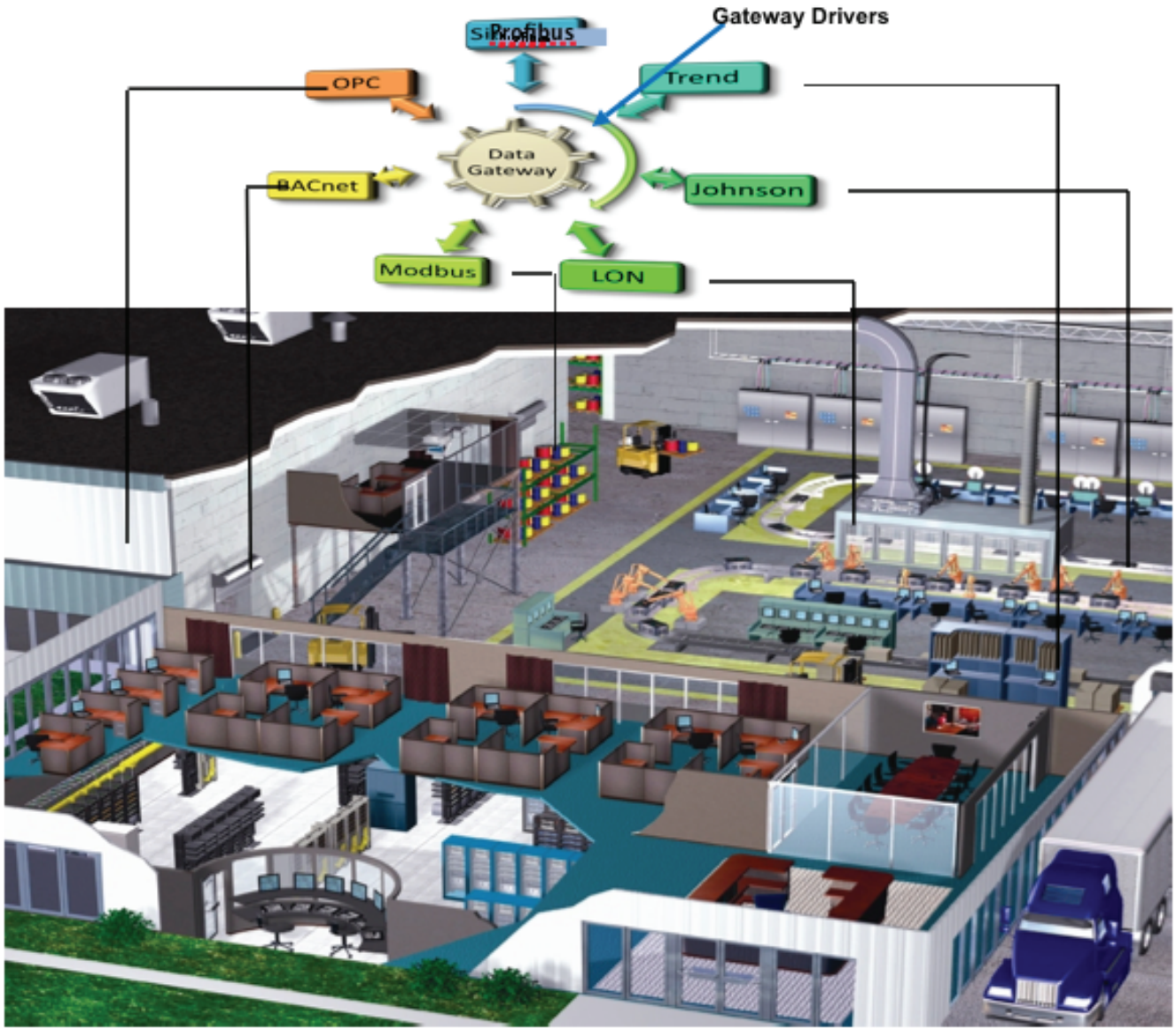


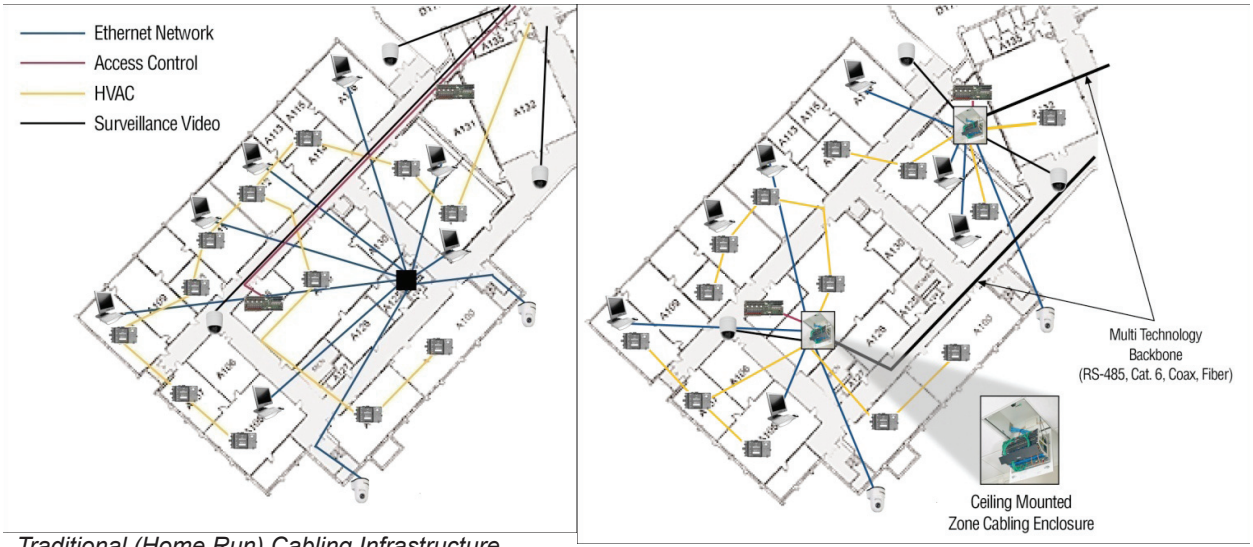
Figure 4.11-1. By capturing and transporting all operational and services data over a physically converged infrastructure, it becomes possible to implement facility-driven policies that support business requirements and tenant/customer demands.

Common processes that might be integrated include:

- Facilities Common communication protocol LON or BacNet
- Fire/Life/Safety Common communication protocol RS485/232
- Industrial Controls Common communication protocol Modbus or SCADA RS-485/232
- Energy Management Common communication protocol LON or BacNet
- Card Access Common communication protocol RS232 or TCP/IP

parate pathways, leading to inefficiencies in specification, installation, and maintenance. Network cabling becomes easier to locate, manage and maintain as each additional building system is routed within the same pathways and enclosures. Managed cabling also helps eliminate abandoned cable in ceilings, making the workplace run more efficiently and safely.

Physically converged infrastructures also contribute toward larger corporate sustainability initiatives. Basic green



Traditional (Home Run) Cabling Infrastructure

Converged ("Zone Cabling") Infrastructure

Figure 4.11-2. Connected Building Solutions deploy all building systems along common pathways to multiple zones where systems connectivity is required.

"Zone Cabling" Architecture

A highly effective way to layer intelligence throughout a building is to logically distribute cabling runs using "zone cabling" architecture for all building networks. Zone cabling enables automated building systems to be converged with Ethernet cabling pathways as they are being designed. This converged multi-technology backbone is comprised of Category 5e/6/6A copper, optical fiber, coaxial, RS-485, and other fieldbus cabling. These systems are converged within a common pathway and then terminated within zone enclosures distributed throughout the building (see Figure 4.11-2).

The zone cabling enclosures become network consolidation points, allowing all cables to be managed and patched in a single enclosure. This architecture differs from dedicated cabling runs typically used in building systems, in which multiple lengthy and redundant cabling routes along dis-

objectives include reducing consumption of non-renewable resources and creating healthy environments. To support these objectives smart lighting subsystems, indirect lighting, daylight harvesting, and modern under-floor HVAC are used to improve occupant comfort and achieve energy efficiencies throughout the building thus shrinking the organization's carbon footprint. These solutions also add value by enabling green performance and LEED certification for building stakeholders, which differentiates buildings from the competition in a business climate where environmental stewardship is increasingly valued.

Further information on the *PANDUIT* Connected Building Solution is available in the following documents:

- Introduction to Connected Building Solutions
- Unified Physical Infrastructure: Introduction to the UPI Vision
- Managing Physical Security Risk in the Infrastructure

Section 5
Network and Security Services

Network and Security Services are designed to support a project or system throughout its lifecycle while assisting the customer with reaching necessary reductions in design and implementation costs, increase uptime and reduce future maintenance costs.

5.1 Network Services

The Network lifecycle phases include the following:

- Assess
- Design and Plan
- Implement
- Audit
- Manage and Monitor

5.1.1 Assess

Network Assessments are a group of offerings that evaluate the current condition of a designed or implemented network via documentation review or on-site network analysis. Assessments can help the customer determine whether the network is able to meet the functional requirements needed to achieve production and business goals. It accomplishes this by evaluating the network, documenting design or implementation issues, and offering resolutions to prevent or fix these issues. An assessment can be used to learn about potential problems that could result in future unplanned downtime.

Customers can improve Return On Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Improving Revenue via Increased Uptime by discovering inefficient and problem-ridden designs or implementations before problems escalate to devastating downtime
- Reducing Project Costs by ensuring that networks are correctly designed to meet the highest performance capabilities
- Improving Productivity through efficient network architecture and design

Network Design Assessment offers a review of existing design documentation (network layout, Bill of Material (BOM), cable schedules, configuration plans) to ensure that the specified components, network architecture and network configuration scheme will meet the functional requirements. The deliverable is a summary of observations, issues, and resolutions. This can be used to ensure that all vendor designs will interconnect without any issues, to verify that the design is within your specific requirements or to offer third-party review.

On-site General Assessment is a one day review of the network's installation, configuration and information. The deliverable is a summary of findings with a rated criticality and high level path forward.

On-site Comprehensive Assessment focuses on customer needs (issue, upgrade, expansion). It can include operational tests, physical media testing, or issue identification. The deliverable is a summary of observations, issues, and resolutions that will assist in preventing downtime by bringing your network up to optimal condition.

5.1.2 Design and Plan

Good network design and planning form the foundation upon which performance and reliability are built. That foundation can help customers realize the value of manufacturing convergence and negate the potential impacts of improper implementation. Network design services enable them to achieve production and business goals and foster manufacturing convergence by enabling the following:

- Integration of business and manufacturing systems
- Remote access and support
- Visibility and integration of technologies and communications
- Fewer networks to maintain
- Foundation for more innovative business models

The design process begins with customer collaboration which includes assessing the network design expectations, business objectives, and identifying functional and informational requirements. Once the specific expectations and requirements are determined, a detailed specification is created. This is the basis for the network topology design and it will ensure that the network design best meets the needs for the system.

(continued on next page)

Customers can improve Return On Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Reducing project costs by ensuring that networks are correctly designed to meet current and future performance and information sharing requirements
- Increasing network availability and uptime to ensure production application and control system stability
- Improving productivity by ensuring that networks are designed to meet production goals and are available when production is scheduled

Network Design Development offers a range, from a design framework document that can be implemented by a network or IT specialist, to a full design package - any sub-set in between. The required deliverables are determined by customer collaboration at the onset.

Network Migration Development offers design assistance that focuses on upgrading an existing network which typically begins with an assessment. The deliverable includes a hardware and media path forward based on customer requirements and current status of the network.

Network Standards Development offers assistance to customers requiring plant-wide or corporate-wide standards for network consistency. The deliverable includes recommendations to be incorporated in a standards document based on blend of industry standards and customer requirements

5.1.3 Implementation

Network implementation services help customers realize the benefits of manufacturing convergence through improved network efficiency, reduced operational costs and increased manufacturing productivity. Network infrastructure Implementation is the foundation for a highly operational network and includes not only the media that transmits the traffic but the hardware that controls the flow of traffic as well as the software that sends, receives and manages the traffic. A network implementation that follows industry standards increases the opportunity of achieving the necessary performance and reliability and can negate the impacts of improper implementation.

Network implementation services, similar to design services, help customers to achieve production and business goals and foster manufacturing convergence by enabling the following:

- Integration of business and manufacturing systems
- Remote access and support
- Visibility and integration of technologies and communications
- Fewer networks to maintain
- Foundation for more innovative business models

The implementation process can consist of turnkey solutions working with our partners that offer guaranteed network installation to simple system configurations.

Customers can improve Return On Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Reducing project costs by ensuring that networks are correctly implemented to meet current and future performance and information sharing requirements
- Increasing network availability and uptime to ensure production application and control system stability
- Improving productivity by ensuring that networks are implemented to meet production goals and are avail able when production is scheduled

Network Installation includes a range of offerings from equipment procurement to complete media and hardware installation services.

Network Configuration includes hardware and software setup for network devices. Optional deliverables can include configuration data and/or backup and restore procedures.

5.1.4 Audit

A Network Audit confirms whether networks are installed according to governing body and/or customer standards. State-of-the-art network diagnostic tools are used to conduct installation and operational tests to validate system implementation and to ensure that performance is within standards outlined by TIA/EIA, ODVA, CNI or an appropriate governing body. Installation testing validates the installation of new networks and prevents commissioning problems. Operational testing is an operational evaluation that tests system performance to ensure reliable communications and verify critical operating parameters. All test results and performance data are completely documented as a baseline for future reference.

Customers can improve Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Improving Revenue via Increased Uptime by discovering inefficient networks and preventing a problem that would cause a shut-down
- Reducing Project Costs by ensuring that networks are correctly designed and implemented to meet the highest performance capabilities
- Decreasing Downtime by discovering potential problems within your network before problems escalate

Network Design Audit consists of comprehensive installation and operational network tests, measurements and analysis based on governing body standards (ODVA, TIA/EIA, and ControlNet International). The deliverable is a report documenting all findings, measurements, analysis, and remediation suggestions.

5.1.5 Manage and Monitor

Manage and Monitor Services are a group of offerings that help customers maintain the network to achieve their expected production and business goals. Offerings range from continuous monitoring or ad hoc diagnostic monitoring to periodic visits or emergency response. These network management offerings can help improve network uptime when customers do not have the resources, tools and technical knowledge internally.

Customer can improve Return On Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Improving Revenue via Increased Uptime by discovering inefficient and problem ridden designs or implementations changes before problems escalate to devastating downtime
- Improving Productivity by efficiently managing the net work architecture and design
- Improving availability by quickly determining the issue and resolving

Remote Monitoring ranges from continuous surveillance to ad hoc diagnostic monitoring of your network infrastructure and activity.

Incident Response is a customer-initiated engagement that can include network trouble shooting, repair, or analysis.

Onsite Support includes annually or regularly scheduled network assessments to analyze any changes to the system and their effects.

5.2 Security Services

Network & Security Services are designed to support a project or system throughout its lifecycle and to assist the customer to reach necessary reductions in design and implementation costs, increase uptime and reduce future maintenance costs. The security lifecycle phases include the following:

- Assess
- Design & Plan
- Implement
- Audit
- Manage and Monitor

5.2.1 Assess

Security Assessments can improve automation asset reliability by determining potential risks to the production process and by developing procedural and technical countermeasures to reduce these risks. Industrial Automation and control assets, similar to traditional IT systems, are vulnerable to many security issues such as unauthorized modifications, intellectual property theft, and malware such as viruses, worms and trojans. Any compromise of these systems can impact production, quality, regulatory compliance, and even safety. To reduce risks to the business, Rockwell Automation's Security Services focus on identifying potential threats to automation assets and developing cost-effective countermeasures to protect the production process

Customers can improve your Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Increasing Uptime by lowering risk of network failures and security compromises
- Increasing Performance by protecting against unauthorized changes that reduce efficiency
- Increasing Quality by tracking and traceability improvements and reducing risks of modifications that affect product quality
- Increasing System Reliability by maximizing usage of current assets and providing additional security controls to improve security at the lowest overall cost of ownership

Policy Assessments are conducted via interviews with key personnel to identify vulnerabilities associated with existing security policies, procedures or overall program. The deliverable will include a "path forward" plan to continuously improve security by introducing human-based security controls.

Design Assessments are a full architecturally-based analysis of customer's infrastructure with documentation provided by the customer. With this analysis, their infrastructure will be compared to their existing security requirements and various industry security standards, which will result in recommendations for their network and information infrastructure in the controls environment

On-site Operational Assessments are an analysis of customer's manufacturing infrastructure including interfaces to the business infrastructure. Security will be evaluated with respect to industrial control networks and integration strategies with business infrastructures. The deliverable will be a report detailing observed vulnerabilities, issues, and resolutions.

On-site Risk Assessments help identify customer assets and their values, vulnerability and threats. The deliverable will quantify the probability and business impact of those threats and provide possible solutions and the cost of the countermeasure.

On-site Vulnerability Assessment will identify system vulnerabilities. The deliverable will be a report detailing observed vulnerabilities, issues, and resolutions.

5.2.2 Design and Plan

Security design and planning services can help customers realize the value of manufacturing convergence and negate the impacts improper design. While manufacturing convergence has many benefits, it can cause negative impacts due to environmental, architectural, maintenance, and consequence of failure differences between manufacturing and IT enterprises.

Security design services enable them to achieve production and business goals and to foster manufacturing convergence by enabling the following in a secure manner and reducing the associated risks:

- Integration of business and manufacturing systems
- Remote access and support
- Visibility and integration of technologies and communications
- Fewer networks to maintain
- Foundation for more innovative business models

Customers can improve Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Increasing Uptime by lowering risk of network failures and security compromises
- Increasing Performance by protecting against unauthorized changes that reduce efficiency
- Increasing Quality by tracking and traceability improvements and reducing risks of modifications that affect product quality
- Increasing System Reliability by maximizing usage of current assets and providing additional security controls to improve security at the lowest overall cost of ownership

Security Program Development is the overall encompassing offering that steps customers through the development of a Security Program which can include some or all of the following services.

Security Policy Development is a collaborative effort with the customer to assist in creating their security policy. The deliverable includes recommendations to be incorporated in a standards document based on blend of industry standards and customer requirements.

Security Design Development offers a range from a design framework document that can be implemented by a network or IT security specialist to a full design package or any subset in between. The required deliverables are determined by customer collaboration at the onset.

Business Continuity Planning (BCP) helps minimize the effects of necessary resources that are no longer available or functional to a customer trying to conduct business. The BCP engagement entails collaboration with the customer to develop new business continuity plans or review the existing business continuity plans stemming from an existing business impact analysis; to identify continuity risks, evaluate existing preventive controls; to develop mitigation and recovery strategies and to develop and document roles, responsibilities and actions within the contingency plans.

Disaster Recovery Planning and Incident Response Planning for the controls environment will fall under and support the larger BCP supporting the overall Security Program. While Disaster Recovery Planning entails how to recover, Incident Response Planning entails what to do when it occurs.

5.2.3 Implementation

Security Implementation services can help customers realize the value of manufacturing convergence and negate the impacts of improper implementation. While manufacturing convergence has many benefits, it can cause negative impacts due to environmental, architectural, maintenance, and consequence of failure differences between manufacturing and IT enterprises.

Security implementation services enable them to achieve production and business goals and foster manufacturing convergence by enabling the following in a secure manner and reducing the associated risks:

- Integration of business and manufacturing systems
- Remote access and support
- Visibility and integration of technologies and communications
- Fewer networks to maintain
- Foundation for more innovative business models

Customers can improve Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Increasing Uptime by lowering risk of network failures and security compromises
- Increasing Performance by protecting against unauthorized changes that reduce efficiency
- Increasing Quality by tracking and traceability improvements and reducing risks of modifications that affect product quality
- Increasing System Reliability by maximizing usage of current assets and providing additional security controls to improve security at the lowest overall cost of ownership

Security Program Implementation takes the design and development documents to the next level – implementation. The overall program implementation includes implementing the security design, policies and procedures.

Security Configuration is the configuration of network devices and security appliances including firewall and switch security configurations (firewall rule sets, ACLs, etc)

Non-Production Penetration Testing can only be done in a lab or an offline production environment. It includes reconnaissance, asset identification, vulnerability discovery and exploitation and attacking in scope targets.

System Hardening reviews Vulnerability Assessment data and implements system changes to prevent network and application-based attacks, essentially addressing risks identified in the assessment stages.

Security Policy Training creates awareness throughout the organization of the desired security changes and helps enforce accountability for new security policies.

5.2.4 Audit

Security Audits are based on customer and/or known standards and verify whether a security program is implemented as expected, whether implemented by Rockwell Automation or not. Industrial Automation and control assets, similar to traditional IT systems, are vulnerable to many security issues such as unauthorized modifications, intellectual property theft, and malware such as viruses, worms and trojans. Any compromise of these systems can impact production, quality, regulatory compliance, and even safety.

To reduce risks to the business, Rockwell Automation's Security Services focus on identifying potential threats to automation assets and developing cost-effective countermeasures to protect the production process. While auditing, Rockwell Automation offers remediation to meet standards that are currently not met.

Customers can improve Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Increasing Uptime by lowering risk of network failures and security compromises
- Increasing Performance by protecting against unauthorized changes that reduce efficiency
- Increasing Quality by tracking and traceability improvements and reducing risks of modifications that affect product quality

- Increasing System Reliability by maximizing usage of current assets and providing additional security controls to improve security at the lowest overall cost of ownership
- Regulatory compliance

Security Audits evaluate existing infrastructure against customer security design or policy or against a known and accepted standard or government requirement. Compliance examples include items such as the NERC CIP standards, ISA SP-99, NIST 800-53, NIST 800-82, etc.

5.2.5 Managed Security Services

Managed Security services can help customers realize the value of manufacturing convergence and can also negate the impacts of improper implementation. While manufacturing convergence has many benefits, it can cause negative impacts due to environmental, architectural, maintenance, and consequence of failure differences between manufacturing and IT enterprises.

Security implementation services enable them to achieve production and business goals and foster manufacturing convergence by enabling the following in a secure manner and reducing the associated risks:

- Integration of business and manufacturing systems
- Remote access and support
- Visibility and integration of technologies and communications
- Fewer networks to maintain
- Foundation for more innovative business models

Customers can improve Return on Net Assets (RONA) and Overall Equipment Effectiveness (OEE) by:

- Increasing Uptime by lowering risk of network failures and security compromises
- Increasing Performance by protecting against unauthorized changes that reduce efficiency
- Increasing Quality by tracking and traceability improvements and reducing risks of modifications that affect product quality
- Increasing System Reliability by maximizing usage of current assets and providing additional security controls to improve security at the lowest overall cost of ownership

Remote Monitoring can be offered in conjunction with our InSite team or can be implemented in an ad-hoc, non real-time fashion to diagnose long-term potential security and network issues.

Incident Response includes management, coordination and resolution services that entail assessing / verifying security incidents and providing guidance on further action as necessary.

On-site support and disaster recovery assistance offers support when a customer's Disaster Recovery Plan has been implemented once a business continuity impacting event has occurred. This response could range from technical support to managing the disaster recovery actions.

Appendix A

***PANDUIT* Copper Cabling System Technical Information**

Appendix A-1

PANDUIT® TX6ATM 10GigTM UTP
Copper Cabling System
Conduit Fill Capacity Table

TX6A™ 10GIG™ UTP Copper Cable										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area		Max. No. Cables Using 40% Fill Rate
		Internal Diameter		Area-.79D² Total 100%		Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0683	44	3
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0683	44	5
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0683	44	8
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0683	44	12
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0683	44	19
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0683	44	28
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0683	44	43
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0683	44	58
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0683	44	75
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0683	44	118
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0683	44	170

PANDUIT® TX6™ 10Gig™
Shielded Copper Cabling System
Conduit Fill Capacity Table

TX6000™ Plenum Shielded (PSP6004**) Cable										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (Plenum)		Max. No. Cables Using 40% Fill Rate (Penum)
		Internal Diameter		Area-.79D² Total 100%		Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0683	44.1	3
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0683	44.1	5
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0683	44.1	8
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0683	44.1	12
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0683	44.1	19
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0683	44.1	28
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0683	44.1	43
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0683	44.1	58
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0683	44.1	75
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0683	44.1	118
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0683	44.1	170

PANDUIT® TX6™ PLUS UTP
Copper Cabling System
Conduit Fill Capacity Table

TX6000™ Category 6 Plenum (PUP6004**) Cable										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (Plenum)		Max. No. Cables Using 40% Fill Rate (Penum)
		Internal Diameter		Area-.79D²	Total 100%	Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0426	27.5	4
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0426	27.5	8
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0426	27.5	14
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0426	27.5	19
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0426	27.5	31
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0426	27.5	45
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0426	27.5	69
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0426	27.5	93
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0426	27.5	120
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0426	27.5	189
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0426	27.5	273
TX6000™ Category 6 Riser (PUR6004) Cable**										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (Riser)		Max. No. Cables Using 40% Fill Rate (Riser)
		Internal Diameter		Area-.79D²	Total 100%	Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0452	29.2	4
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0452	29.2	7
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0452	29.2	13
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0452	29.2	18
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0452	29.2	29
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0452	29.2	42
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0452	29.2	65
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0452	29.2	88
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0452	29.2	113
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0452	29.2	178
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0452	29.2	257
TX6000™ Category 6 CM (PUC6004) & LSZH (PUL6004**) Cables**										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (CM & LSZH)		Max. No. Cables Using 40% Fill Rate (CM & LSZH)
		Internal Diameter		Area-.79D²	Total 100%	Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0397	25.6	5
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0397	25.6	8
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0397	25.6	15
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0397	25.6	20
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0397	25.6	34
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0397	25.6	48
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0397	25.6	75
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0397	25.6	100
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0397	25.6	129
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0397	25.6	203
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0397	25.6	293

TX6500™ Category 6 Plenum (PUP6504**) Cable										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (Plenum)		Max. No. Cables Using 40% Fill Rate (Plenum)
		Internal Diameter		Area-.79D² Total 100%		Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0551	35.6	3
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0551	35.6	6
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0551	35.6	10
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0551	35.6	14
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0551	35.6	24
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0551	35.6	35
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0551	35.6	54
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0551	35.6	72
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0551	35.6	93
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0551	35.6	146
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0551	35.6	211
TX6500™ Category 6 Riser (PUR6504) Cable**										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (Riser)		Max. No. Cables Using 40% Fill Rate (Riser)
		Internal Diameter		Area-.79D² Total 100%		Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0555	35.8	3
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0555	35.8	6
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0555	35.8	10
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0555	35.8	14
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0555	35.8	24
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0555	35.8	34
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0555	35.8	53
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0555	35.8	71
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0555	35.8	92
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0555	35.8	145
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0555	35.8	209

PANDUIT® TX6TM PLUS Shielded Copper Cabling
Conduit Fill Capacity Table

TX6000™ Category 6 CM Shielded (PFC6004**) and LSZH Shielded (PFL6004**) Cables										
Conduit Trade Size Inches (mm)		Internal Conduit Area						Cable Area (CM &LSZH)		Max. No. Cables Using 40% Fill Rate (CM &LSZH)
		Internal Diameter		Area-.79D² Total 100%		Area 40% Fill				
		inches	mm	inches²	mm²	inches²	mm²	inches²	mm²	
3/4	(21)	0.82	20.9	0.53	345	0.21	138	0.0688	44.4	3
1	(27)	1.05	26.6	0.87	559	0.35	224	0.0688	44.4	5
1	(35)	1.38	35.1	1.50	973	0.60	389	0.0688	44.4	8
1	(41)	1.61	40.9	2.05	1322	0.82	529	0.0688	44.4	11
2	(53)	2.07	52.5	3.39	2177	1.35	871	0.0688	44.4	19
2-1/2	(63)	2.47	62.7	4.82	3106	1.93	1242	0.0688	44.4	28
3	(78)	3.07	77.9	7.45	4794	2.98	1918	0.0688	44.4	43
3-1/2	(91)	3.55	90.1	9.96	6413	3.98	2565	0.0688	44.4	57
4	(103)	4.03	102.3	12.83	8268	5.13	3307	0.0688	44.4	74
5	(129)	5.05	128.2	20.15	12984	8.06	5194	0.0688	44.4	117
6	(155)	6.07	154.1	29.11	18760	11.64	7504	0.0688	44.4	169

Ca-