Industrial Network Infrastructure to Support Cybersecurity Strategies

PANDUIT™

Table of Contents

Incorporating Security into Your Physical Network Planning

Industry 4.0, or the Industrial Internet of Things (IIoT), has ushered in a new era of digital transformation for the manufacturing sector. While the adoption of digital technologies has driven substantial growth and efficiency, it has also heightened the risk of cyber threats.

According to a recent IBM report, **X-Force Threat Intelligence Index 2024**, manufacturing is the most-targeted industry by cybercriminals. The report found that manufacturing accounted for 25.7 percent of all reported cyber incidents during the previous year.

Threats today come from a variety of sources from cyberattacks, to ransomware, malware, even social engineering, but also from insider attacks. A survey by cybersecurity insiders found that 52 percent of respondents considered insider attacks more difficult to detect and prevent and 38 percent about as difficult as external threats.[1]

After an incident, enterprises needed an average of: 50 days to resolve an insider's attack and 23 days to recover from a ransomware attack, with average data breach costs rising from $3.86 million to $4.24 million.[2]

What these stats bring to light is that cybersecurity threats extend beyond internet-based attacks and require physical network planning as part of a defense in depth strategy. Common threats are unauthorized and intentional access to vulnerable network connections, USB connections and network equipment, as well as the potential for incidental cyber threats from workers while maintaining equipment.

50 DAYS
to resolve an insider's attack

23 DAYS
to recover from a ransomware attack

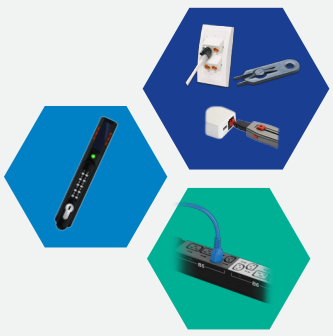
[1] 2020 Insider Threat Report (cybersecurity-insiders.com)
[2] 2024 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends | PurpleSec

Physical layer planning provides a best-in-class execution plan for the network and can reduce vulnerabilities, enable controlled access to equipment to deter insider threats and contribute to more effective services to and management of network hardware. Panduit offers a variety of solutions to manage and strengthen your network security and provide disaster recovery solutions in the physical layer, from micro data center cabinets designed to house industrial demilitarized zone (iDMZ) and security hardware, to industrial distribution frame and zone enclosures to physically segregate the network, to equipment hardening and access control (in select enclosures) and locking solutions, to physical port lock-ins and block-outs for RJ-45, USB, and LC fiber ports and adapters to deter access from unauthorized personnel.

Network Infrastructure for Cybersecurity Strategies

Physical Protection

Infrastructure is your first line of defense against a cyberattack. Limit access to critical systems and protect physical ports.



Asset Visibility

You cannot protect what you cannot see. Panduit solutions provide greater visibility into your network infrastructure to more effectively protect, prevent, contain, and detect cyberattacks.

Disaster Recovery

A business continuity plan with a disaster recover site should be a part of your cybersecurity strategy, to get your network and operations working again quickly after an attack.

Physical Protection – Port Security

Infrastructure is your first line of defense against a cyberattack. Physically protecting ports limits unauthorized access to critical systems by blocking ports.

Panduit offers a variety of devices that provide physical port security. The entire line of innovative copper products supports all of today's most common IP applications including Power over Ethernet (PoE) and wireless technologies.

Some of these items, like keyed jacks and patch cords for UTP applications, and faceplates, can be included in the initial design. We also offer jack block-out and lock-in devices for Ethernet and USB port solutions that can be installed any time. Panduit port security solutions provide exceptional value, guaranteed future reliability, and a secure foundation for your network's growth.

Network Security Devices

Network security devices reduce unauthorized access to existing network installations. These devices save time and money associated with network downtime, data security breaches, infrastructure repair, and hardware replacement due to theft. Block-out devices snap into modules and is released with the enclosed removal tool. SmartKeeper offers one master key that controls multiple block-out devices. The lock-in device is a versatile design that is compatible with most existing patch cords, faceplates, patch panels, and other IP devices.

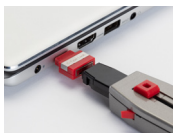
Block-out and Lock-in Devices

Part Number	Description	Color
SMARTKEEPER		
SKRJ45RD-X	RJ45 A block-out device	Red
SKUSBA-V	USB Type A block-out device	–
SKUSBC	USB Type C block-out device	
SKMKEY	Master Key	
BLOCK-OUT DEVICES		
PSL-DCJB	Ten RJ45 jack module block-out devices and one removal tool	Red
PSL-LCAB	Ten LC duplex adapter block-out devices and one removal tool	
PSL-USBA**	Five USB Type 'A' block-out devices and one removal tool	
PSL-USBB	Ten USB Type 'B' block-out devices and one removal tool	
LOCK-IN DEVICES		
PSL-DCPLE	Ten Standard RJ45 plug lock-in devices, one installation/removal tool	Red
PSL-DCPLRE	Ten recessed RJ45 plug lock-in devices, one installation/removal tool	
PSL-DCPLSE	Ten super recessed RJ45 plug lock-in devices, one installation/removal tool	
FLCCLIW-X	LC duplex lock-in clip and removal tool	White

Visit panduit.com for color and package options.
**Add -L to end of part number for bulk packages of 50 pieces with 5 removal tools to reduce single-use plastic


SKRJ45RD-X

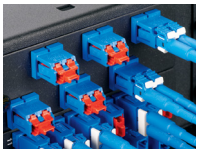

SKUSBA-V


SKUSBC


SKRJ45 SKUSBA-V SKUSBC


SKMKEY


PSL-DCJB


PSL-LCAB


PSL-USBA**


PSL-USBB


PSL-DCPLE, PSL-DCPLRE and PSL-DCPLSE


FLCCLIW-X

Keyed Connectivity

Keyed copper and fiber cabling systems allow the design of secure, modular, end-to-end connectivity for communication and computing elements from the data center to the workstation. The keyed functionality increases network security integrity by providing positive and negative keying features that distinguish network connections mechanically. Up to multiple color-coded keys visually distinguish connections to prevent unintentional connection to network infrastructure for increased security, allowing multiple networks to be managed without the risk of interchanging access and limiting network access to unauthorized users.

Mini-Com® Keyed Copper Jack Modules

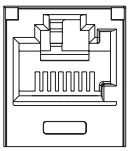
Keyed jack type is indicated by jack color. Select a patch cord (below) of the same color as the jack to match the keyed configuration.

Part Number	Description	Keyed Type and Color*
UTP KEYED JACK MODULES		
CJK6X88TGBU	Category 6A, RJ45, 10 Gb/s, 8-position, 8-wire universal UTP keyed jack module	Blue*
CJK688TGBU	Category 6, RJ45, 8-position, 8-wire universal UTP keyed jack module	

*For standard jack module colors and keyed configurations other than Blue, replace BU suffix with BL (Black), RD (Red), YL (Yellow), GR (Green), or OR (Orange). Each color represents a different keyed configuration.

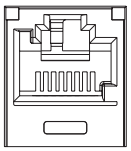
CJK6X88TGBU

A – Black



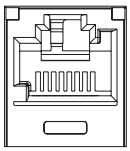
CJK688TGBL

B – Red



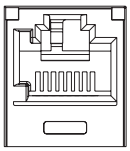
CJK688TGRD

C – Green



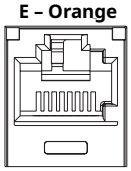
CJK688TGGR

D – Yellow



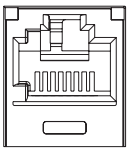
CJK688TGYL

E – Orange



CJK688TG0R

F – Blue



CJK688TGBU

Keyed Copper Patch Cords

Keyed patch cord type is indicated by patch cord color. Select a jack (above) of the same color as the patch cord to match the keyed configuration.

Part Number	Description	Length^	Keyed Type and Color*
UTP KEYED PATCH CORDS			
UTPK6A3BU	Category 6A, 10 Gb/s UTP stranded CM patch cord with TX6™ PLUS Keyed Modular Plug on one end and TX6™ PLUS Non-Keyed Modular Plug on the other end	3 feet	Blue*
UTPK6A1MBU		1 meter	
UTPKSP3BU	Category 6, UTP solid CM patch cord with TX6™ PLUS Keyed Modular Plug on one end and TX6™ PLUS Non-Keyed Modular Plug on the other end	3 feet	
UTPKSP1MBU		1 meter	

^For standard foot lengths (3, 5, 7, 10, 14) or standard meter lengths (1, 2, 3, 5, 7, 10) change the length designation in the part number to the desired length. For example, the part number for a Category 6A, UTP, keyed, Blue, 14-foot patch cord is UTPK6A14BU.
*For standard cable colors and keyed configurations other than Blue, replace BU suffix with BL (Black), RD (Red), YL (Yellow), GR (Green), or OR (Orange).

Keyed UTP Copper Patch Cords

Water/Tamper Resistant Faceplate

Part Number	Description
CFPWR4CIG	Single gang water resistant faceplate made of high impact material, meets IP-56 protection, includes gaskets to prevent water damage and two types of screw options to secure hinged cover to base. Requires adhesive labeling. International Gray

CFPWR4CIG

Physical Protection – Enclosures

Most plant floors are built as an open floor space for maximum flexibility for production equipment. As a result, network equipment often is mounted in open spaces and is far less protected and secure than telecom rooms in an office space.

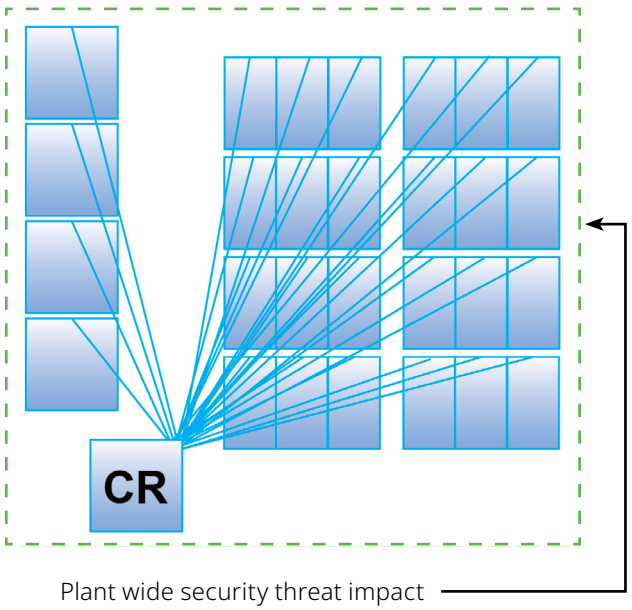
Intelligent PDUs and lockable enclosures are part of a defense-in-depth approach to physical network security that enables remote monitoring and troubleshooting while limiting physical access to IT equipment. IDF enclosures are engineered to deploy and protect 19" rack mount switches along with power distribution capabilities to protect and monitor critical IT equipment. The IDF solutions in mild steel include standard keyed locks and can be configured to include an intelligent PDU, as well as temperature and door sensors.

Benefits of Zone Architectures

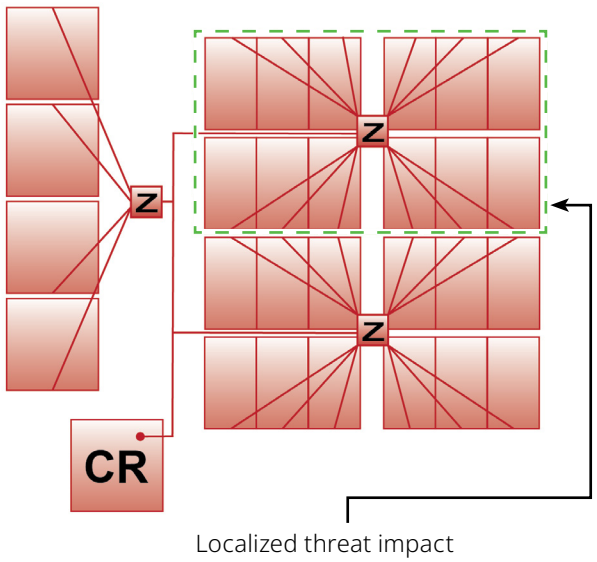
Industrial Distribution Frames and Zone Enclosures enable switch and cabling deployment in a zone architecture for greater uptime and localized security strategies:

- Physically segments the network nodes/switch layer
- Overlays perfectly to manufacturing cells
- Keeps local traffic local by access layer switch

Centralized Cabling
Home runs from each node back to the control room



Zone Cabling
Provides for reduced home-run wiring and easy moves, adds, and changes



IDF Enclosures

Ordering Information

Part Number	Enclosure Type	Switch Deployment	Security
IDFP482430 (Partially Pre-Configured)	4/12 Steel	Two access and up to three distribution	Locking handle, standard locking door latches
IDFE482430 (Enclosure only)			

Power Distribution Units

Ordering Information

Region	Part Number	iPDU Series	Input Current per Phase	Form Factor	Input Plug Type	Apparent Power (kVA)	Outlet Count	Outlet Configuration
NA	**P08D09M**	Monitored Input	15	1U	5-15P	1.4	8	(8)5-20R
	P08D10M		20		5-20P	1.9		
	P08D11M				L5-20P			
	P16D12M		30	2U	L5-30P	2.9	16	(16)5-20R
	P16D14M				L6-30P	5		(12)C13, (4)C19
INTL	**P12D36M**		16	1U	IEC60309-316P6	3.7	12	(12)C13
	P16D37M		32	2U	IEC60309-332P6	7.4	16	(12)C13, (4)C19
	P08G10M	Monitored Switched per Outlet	16	1U	IEC60309-316P6	3.7	8	(8)C13
NA	**P16E19M**	Monitored Switched	30	2U	L6-30P	5.0	16	(12)C13, (4)C19
INTL	**P08E25M**		16	1U	IEC60309-316P6	3.7	8	(8)C13

Order both enclosure and PDU part numbers. Partially pre-configured includes 26 RU enclosure with fiber enclosure, patch panels, cable managers, grounding and bonding and back panels, DIN rail.; Other enclosure sizes and styles available at panduit.com.

Power Distribution Units

A power distribution unit (PDU) helps manage mission-critical network power needs. Intelligent PDUs monitor power and environmental conditions to protect your systems and data. As noted in the table above, the suggested PDUs for use with IDF enclosures fall into three types:

- Monitored Input
- Monitored Switched per Outlet
- Monitored Switched

Asset Visibility

Panduit copper and fiber patch cables include *Rapid*ID labels

Managing the security of OT and Industrial Control Systems requires visibility of the connected hardware (and software) in the network. You cannot protect what you cannot see. The *Rapid*ID solution from Panduit helps enhance visibility into your network infrastructure, to more effectively prevent, contain, and detect cyberattacks.

The *Rapid*ID™ Network Mapping System automates labor-intensive and error-prone cable documentation, resulting in a faster, easier way to place and trace cables and patch cords. Using pre-labeled patch cords and a handheld scanner, *Rapid*ID allows you to quickly and simply document your network, thus improving visibility and reducing downtime in the event of an attack. *Rapid*ID reduces the time and cost of patch cord documentation by up to 50 percent.

*Rapid*ID makes the documentation process less painful and reduces human error by eliminating the need for manual data entry.

Several software options are available to support *Rapid*ID, including a free desktop version, along with Pro and Pro+ versions with greater capabilities.

The *Rapid*ID solution includes:

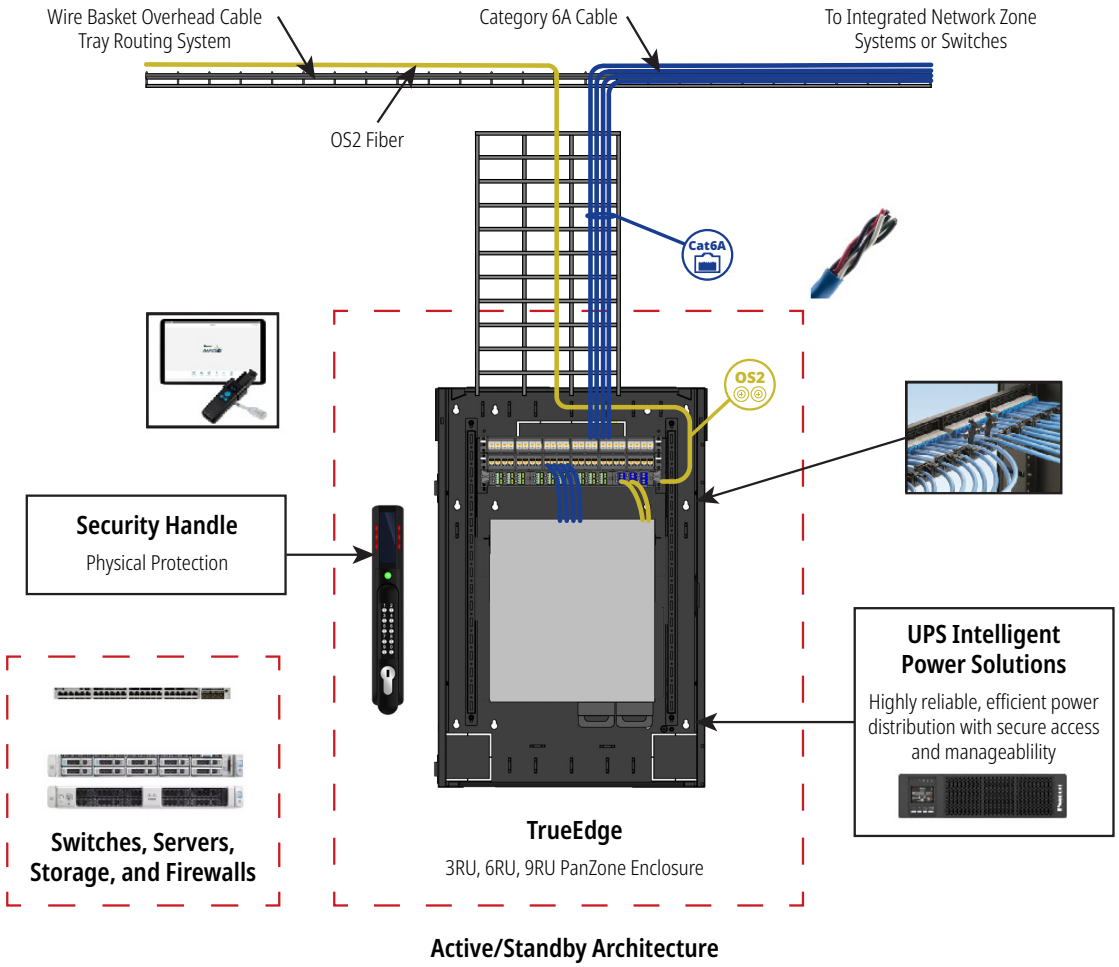
- Pre-labeled copper and fiber patch cords
- Bluetooth-enabled third-party barcode scanner compatibility
- *Rapid*ID pre-printed unique identifier label rolls

Get started with *Rapid*ID

Disaster Recovery Solutions

A business continuity plan with a disaster recovery site should be a part of your cybersecurity strategy. This self-contained site is key to quickly getting your network back online and operations flowing after a cyberattack.

Disaster Recovery Architecture



Active/Standby Architecture

The disaster recovery site can be a compact network equipment enclosure or industrial distribution frame, which is configured to enable fast switch-over and recovery of critical production centers.

An ideal solution for small to medium-sized businesses is a Panduit TrueEdge enclosure, equipped with intelligent UPS, access control, and *Rapid*ID compatible patch cords.

True Edge Enclosures

Zone enclosures provide accessibility and flexibility to reconfigure network distribution. Each zone enclosure serves as a main distribution point for a particular zone.

Keyed lockable features prevent unauthorized access. They can be upgraded with an optional combination lock that eliminates the need for a physical key.

The TrueEdge Vertical Wall Mount Enclosure allows up to 36 inches of active equipment depth to be mounted in a low-profile application. This low-profile wall mount enclosure houses traditional horizontal equipment vertically on a wall while minimizing network infrastructure investment by eliminating a rack or cabinet. It has a premium static load rating of up to 400 pounds and best-in-class thermal ratings to eliminate equipment failure.

- Scalable — offering a variety of configurations for servers, switches, and edge computing
- Strong — able to withstand optimum load capacity for deployments of server and switch configurations
- Configurable — offered in 3 RU, 6 RU, and 9 RU sizes, allowing customization to fit the needs of the application

Disaster Recovery Solutions

Size	TrueEdge	UPS Small	UPS Medium	Free Rack Units	Security Handle	*Rapid*ID Pro+ Subscription	Devices
DISASTER RECOVERY SMALL							
Small	6RU	1-2kVA	3kVA	4	Yes	Available	Mixed switches, servers, storage
Parts:	WME6BL	U01N11L (1KVA Li) U02N11V (2KVA VRLA)	U03N11L (3KVA Li)		ACF05 + ACF20		
DISASTER RECOVERY MEDIUM							
Medium	9RU	3kVA	3+3kVA (6kVA)	5	Yes	Available	Mixed switches, servers, storage
Parts:	WME9BL	U03N11L (3KVA Li)	U03N11L (3KVA Li)		ACF05 + ACF20		

UPS

An Uninterruptible Power Supply (UPS) provides excellent electrical performance, intelligent battery management, enhanced intelligent monitoring, secure network functions and long lifespan for lithium units. Additionally, they comply with ENERGY STAR 2.0, EMC and safety standards.

Output capacities can range from 1/2/3kVA, 5/6/10kVA to 10/15/20kVA with lead acid (VLRA) or Lithium-Ion battery types. These UPS solutions are integrated for use with the DCIM software that combines power and environment monitoring along with cabinet access, asset tracking, and connectivity management.

Zone Enclosures

Zone enclosures provide accessibility and flexibility to reconfigure office spaces. Each zone enclosure serves as a main distribution point for a particular zone. Keyed lockable features prevent unauthorized access.

Wall Mount Cabinets include keys to secure front and rear doors and side panels, they can be upgraded with optional combination lock that eliminates the need for a physical key.

PanZone® TrueEdge Wall Mount Enclosure

Part Number	RU	Height in. (mm)	Width in. (mm)	Depth in. (mm)	Load Capacity lbs. (kg)
WME3**	3	42.0 (1067)	28.5 (724)	9.5 (241)	200 (91)
WME6**	6			14.8 (376)	300 (136)
WME9**	9			20.0 (508)	400 (181)

**Colors: Black (BL) and White (WH)

WME6BL

TrueEdge: NEMA-Rated Low Profile IDF

Part Number	RU	Height in. (mm)	Width in. (mm)	Depth in. (mm)	Load Capacity lbs. (kg)
IDFLP6	6	42.0 (1067)	28.5 (724)	14.8 (376)	300 (136)

IDFLP6

Smart Rack Security Handle

Part Number	Description
ACF05	The Smart Rack Security Handle with dual frequency (125 kHz and 13.56 MHz) card reader and integral humidity sensor operates with the Panduit iPDU and UPS. All handles feature the base tumbler (TU020X) pre-installed at the factory.
ACF06	The Smart Rack Security Handle with dual frequency (125 kHz and 13.56 MHz) card reader, integral humidity sensor, and keypad for dual authentication operates with the Panduit iPDU and UPS. All handles feature the base tumbler (TU020X) pre-installed at the factory.
ACF20	Smart Rack Security Handle Harness for use with ACF05 and ACF06 to optimize cable routing in enclosures

ACF06

Codes, Standards, Regulations, and Organizations in Security

- ASIS ESRM, Enterprise Security Risk Management
- ASIS PAP.1, Security Management Standard: Physical Asset Protection
- ASIS SA, Security Awareness
- AVIXA RP-C303.01, Recommended Practices for Security in Networked AV Systems
- IEEE 802.1AE™, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security
- ISO 22301, Security and Resilience – Business Continuity Management Systems – Requirements
- ISO 31000, Risk Management – Guidelines
- ISO 31010, Risk Management – Risk Assessment Techniques.
- ISO/IEC 27001, Information technology – Security techniques – Information security management system – Requirements
- NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security
- ISA/IEC 62443 Series of Standards: Automation and Control Systems Cybersecurity Standards

We have the knowledge and experience to help you make the most of your infrastructure investment.

panduit.com/industrial

Let's connect
panduit.com/contact-us

PANDUIT®
infrastructure for a connected world