White Paper

March 2015

Control Panel Security

Identifying and Mitigating Security Risks

PENTAIR
Hoffman
DESIGN WITH CONFIDENCE™

www.pentairprotect.com

PANDUIT®
building a smarter, unified business foundation
Connect. Manage. Automate.

www.panduit.com

Introduction

Businesses rely on data streams from electrical and electronic enclosures, networking cabinets, and human machine interface (HMI) systems to run their operations, so network managers are increasingly concerned about equipment access and network security. The ability to assess and mitigate potential risks that derail the performance of these enclosures or systems is vital to a company's operational success.

Mission-critical information, control panel components, and confidential or classified data require varying degrees of protection depending on the storage environment. Therefore, the system owner must consider the following factors when choosing a control panel security solution:

1. The **value** of the information or equipment
2. The **risk** level of the control panel environment
3. The **cost** to protect the information or equipment
4. The **functionality** of components needing EMI protection and/or emitting Wi-Fi signals

Facilities managers are generally responsible for determining basic security needs for industrial enclosures and purchasing and maintaining electrical enclosures and control panels for their sites. These responsibilities require that only authorized personnel have access to the control panels, equipment, and information. Unauthorized access not only causes security concerns, but can force a shutdown of operations or power, causing extensive downtime and costs associated with handling the breach.

Whether addressing the loss of valuable information due to data breaches, equipment loss due to theft, damage from vandalism or accidents, or equipment downtime and network failures caused by technicians' mistakes or cyber-attacks, security plays a crucial role in the operation of any business. While many of these risks may not be preventable even with the best security measures, implementing a well-designed physical infrastructure security system can limit the impact and severity of an occurrence. A layered approach to controlled access allows businesses to cost effectively mitigate the expense of lost or stolen information, or the cost of injury from unintentional access.

Technology advancements have modernized access points and control panel design, allowing better security and innovation to protect the contents, both physically and virtually. Touch screens are replacing push-button systems and biometric locks are becoming more common. Using technology to limit access also allows the control panel engineer to modify access without replacing the physical hardware.

This white paper is the last in a series of eight papers on the topic of control panel optimization. The intent is to help identify and mitigate control panel security risks by providing case studies relevant to various applications and discussing the importance of isolating security layers and solutions for these issues. For access to the other white papers and more information on Panduit or Pentair Equipment Protection (manufacturers of the Hoffman brand of enclosure), please visit www.Hoffman-Panduit.com.

Securing the Industrial Network Physical Layer

In the past, stand-alone control systems provided "security through obscurity" without requiring the Internet. With the rapid growth of industrial Ethernet and EtherNet/IP, remote access into control systems has become essential to enable more productivity for companies. The drive to connect factory and enterprise networks is a reality and with more factory equipment to monitor, robust security strategies are required to feed real-time data to the business.

Industrial network security is often governed solely by company policy. An exception is applications within critical infrastructure, where network security is mandated by government agencies. U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience defines 16 critical infrastructure sectors and maintains sector-specific strategies for cybersecurity. The security threat not only comes from Internet connections but can come from within. As many as two-thirds of economic espionage cases involve company insiders. Internal threats include:

- The disgruntled employee intentionally stealing information or sabotaging systems
- Any outsider (contractor, etc.) with inside access to the plant
- Someone with access to the parking lot and the ability to use widely available programs to map wireless networks (e.g., InSSIDer.com) from a laptop
- Non-malicious intent, such as someone charging an iPod or smartphone, which could inadvertently introduce viruses or malware into the industrial network

All connections within the physical infrastructure must be protected and access to unused and open ports should be restricted to maintain the highest possible network reliability.

Risk vs. Cost

Losing vital customer or company information can cause significant damage to a business. According to a study performed by the Ponemon Institute and Symantec Corporation in 2013, US companies reporting data breaches had an average of 28,765 records compromised. In some cases, these breaches cost the companies over $20 million. The study also showed that the majority of data breaches now occur via malicious attacks (Figure 1). These calculated attacks have a higher cost per capita than human error breaches, so creating layers of protection for data and equipment is crucial. Besides the measurable costs of a data breach, the intangible aspects could incur additional costs. Every company needs to determine whether the price of protecting its brand reputation and instilling consumer confidence outweighs the risk of ineffectively protecting equipment and information.

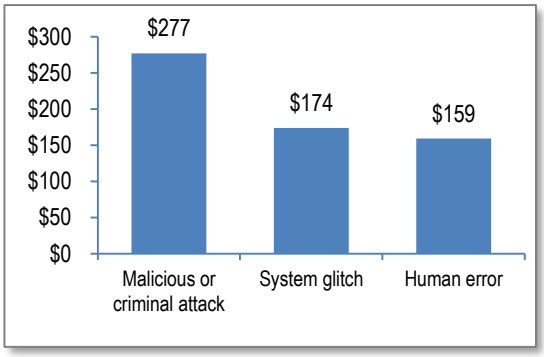

Figure 1: Per capita cost for three root causes of data breach (Figure 6, 2013 Cost of Data Breach Study: United States).

Cost of Downtime vs. Cost of Protection

Research has shown that 59 percent of Fortune 500 companies experience a minimum of 1.6 hours of downtime per week. These companies average over 10,000 employees with wages typically over $50/hour per employee. While a server or network interruption will not affect every employee, these outages translate into significant productivity losses, excess expenses, and lost revenue (Figure 2). Even with insurance for such outages, most policies cover only the lost revenue, not additional expenses. Therefore, it is important that facilities managers take the proper steps to protect and limit access to equipment because the cost of protection is lower than the cost of equipment downtime. The layers of protection to prevent downtime may start externally at the physical enclosure or can be integrated within the enclosure and components.

Brokerage Service	$6.48 million
Energy	$2.8 million
Telecom	$2.0 million
Manufacturing	$1.6 million
Retail	$1.1 million
Health Care	$636,000
Media	$90,000

Typical Hourly Cost of Downtime by Industry (In US Dollars). *Source: Network Computing, the MetMeta Group and Contingency Planning Research.*

Figure 2: Lost revenue by industry.

For example, due to the large amount of money exchanging hands, casinos in Las Vegas use security cameras to help prevent crime. This “eye in the sky” helps detect suspicious behavior and allows casino owners to protect their assets. Unauthorized access to security cameras, whether to the controls or to the power source, puts millions of dollars at risk. A criminal's ability to shut down the system can cripple a casino’s ability to regulate and prevent illegal behavior on the gaming floor. As a result, casino owners use multiple layers of security for physical enclosures to prevent thefts from occurring through unauthorized access, and employ sophisticated security protocols for software and operations.

Occurrence vs. Severity

One mistake can have catastrophic consequences if the enclosure does not have leveled layers of access to prevent accidental changes or entry. Therefore, additional security may be required when workers need regular access for maintenance, but do not need access to vital controls or sensitive data within the same enclosure. In these situations, defense contractors or utility applications may use an enclosure within an enclosure to properly secure controls and ensure employee safety. These enclosures have security that prevents entry by non-maintenance personnel and may have additional enclosures inside that can only be accessed by employees with proper clearance or certifications.

Some nuclear plant applications use enclosures within enclosures to manage access to their controls. These applications require entry and maintenance by low-level clearance employees, but also include high-level controls within the enclosure. By limiting the initial access to the basic controls, with a second layer of security required to access the additional contents, nuclear plant operators can prevent security issues and accidents.

Functionality – The Control Panel Location

The rising value of scrap metal and copper has created an increase in theft and damage to enclosures and control panels. While any control panel in a public area is at risk, those located in impoverished neighborhoods, and areas with high crime rates are most susceptible to theft, causing system downtime and added costs, if not properly secured. Other at-risk locations include those without adequate lighting, sites hidden from view, and remote areas where traffic is rare.

August 2014 - Vandals were able to cut locks and damage equipment using a bolt cutter at a community well site on Graham Island in remote Queen Charlotte, British Columbia. The vandals tampered with the automatic control panel and aeration system, along with a well pipe, making the water unsuitable for use. The village repaired the equipment, but had to shift capacity to other wells that do not operate as efficiently, costing the tiny town valuable resources and money. In this case, different locking mechanisms and security measures could have prevented intrusion to the enclosure and controls, even if the vandals were able to gain access to the facility.

Damage to a control panel or enclosure is not limited to criminal activity. Applications involving heavy machinery, vehicles, or other powerful, moving parts create an additional risk. These potential sources of destruction do not take much effort or time to harm the enclosure so anticipating risks and providing additional security by selecting the appropriate material and location is crucial for protecting the control panel.

Other common security issues occur on the shop floor, at schools, and through company network systems. Technician mistakes, theft and vandalism, and viruses, malware, or computer worms all create security risks that companies should consider when choosing equipment protection methods.

Shop Floor – Technician Mistakes

Multiple people may need to access the panel for building management or automation systems applications. These systems control and monitor a facility’s mechanical and electrical equipment, such as ventilation, lighting, power, fire, or security. Allowing a technician access to all of the systems, instead of limiting access to areas requiring service can be a costly mistake if the settings of another system are inadvertently changed.

Schools – Theft, Hacking, and Vandalism

The location of enclosures and control panels is important to operational success at a school. Students seeking to avoid a class may try to shut down lighting, pull fire alarms, or activate other controls. Control panels can also be compromised by poor placement or inadequate durability. Potential hazards to school control panels include students with heavy backpacks, crowded hallways, and inexperienced drivers on school grounds. In addition, unsecured enclosures and equipment are vulnerable to data theft, security breaches, manipulation, and equipment theft.

Company Network – Viruses, Malware, and Worms

With the proliferation of portable USB devices, iPods, mobile phones, and other technology entering the workplace, employees may unintentionally expose an organization's data and customers to theft and malware such as viruses, worms and Trojan horses when they charge infected devices. Data can easily be copied or compromised, which places a company's network, data, and records at risk without safeguards in place.

Solutions – Controlled Access in Layers

To mitigate most security risks, it is necessary to have multiple defense measures that protect control panel components. Creating layers and different levels of security, and integrating them into a single system enhance the system's effectiveness and allow facilities managers and network managers to feel confident that controls and data are secure. There are six layers of enclosure security. See Figure 3.

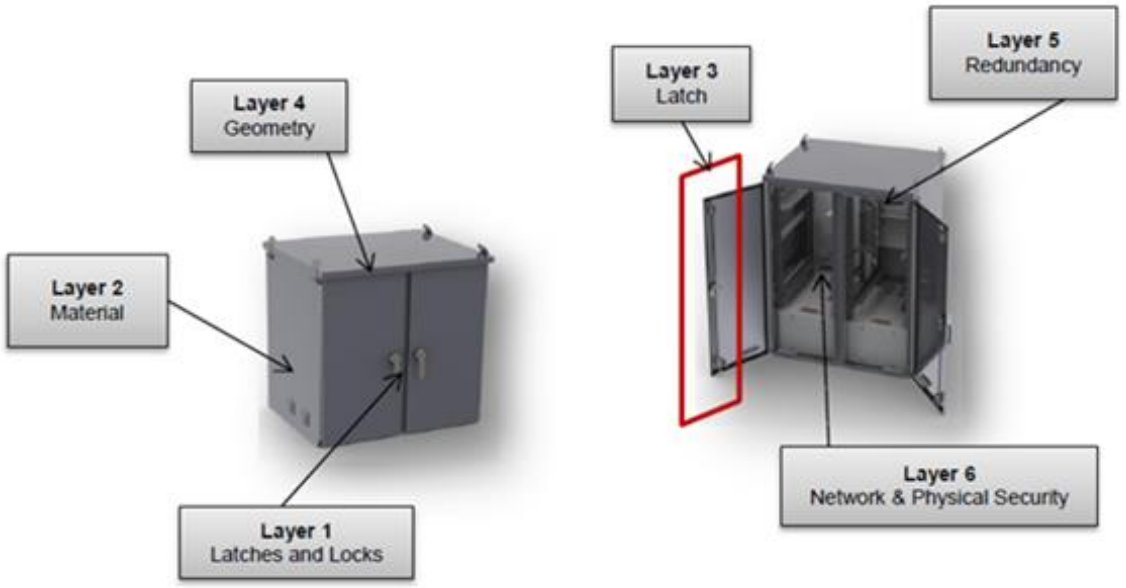

Figure 3. Six layers of security.

Layer #1 – Locks, Keys, or Biometrics

The first layer is the latches and locks that allow entry into the enclosure. The security level of the locks depends on the level of desired access. Enclosures with external, unprotected hinges and locks are twice as likely to be a target for tampering. Placing the hinges inside the enclosure and using recessed or flush mount locks instead of protruding latches and padlocks reduce the risk of tampering or damage. Using different lock and key styles also increases equipment security.

Many enclosures include a **standard key configuration** so technicians can open multiple enclosures using the same master key. This saves time because the technician is not required to try multiple keys while performing maintenance or repairs.

While this capability is convenient, it allows anyone with knowledge of the lock type to use a generic key to gain access, including hackers who know the brand and model enclosure that a company uses. To minimize this possibility, Hoffman offers cylinder lock kits that fit in pre-drilled or punched holes and are available with two key configurations. See Appendix, #1.

Securing an enclosure may be as simple as replacing a standard key hole with inserts that have alternative key shapes, such as square bits, triangular holes, and Daimler or Fiat shapes. **Changing the shape of the key** prevents entry with standard keys and tools, forcing the user to know what lock is installed beforehand and to have the matching key. See Appendix, #2.

Using **unique house keys** with the enclosure provides additional security by limiting access to only those given a key. A company may use the same house key for all enclosures, and can configure the key for specific company needs. Therefore an outsider cannot gain entry to the enclosure with a generic key. If the company wants to limit access further, each enclosure can have its own key. Unique house keys may increase maintenance times, but they are important for applications that hold sensitive data or for controls the company does not want falling into the wrong hands. Hoffman provides many lock and key solutions configured to fit a company's security requirements.

One of the most basic security measures, which requires a tool such as a screwdriver to open an enclosure, can deter unintentional access. **Screw cover enclosures** increase the time required to open an enclosure, decreasing the window of opportunity for would-be thieves. While this method allows access to anyone with the proper tools, it may be a successful deterrent in heavily traveled areas or where security personnel can visually monitor the location. Hoffman offers screw cover enclosures rated for Type 1, 3R, 4, 4X, and 12 applications. See Appendix, #3.

Combination locks are also a suitable choice to prevent unauthorized entry into an enclosure. These locks eliminate the need to carry a physical key and allow a technician to share access with multiple people. Since they are embedded into the enclosure or latch, combination locks are more secure than external locks. Hoffman offers multiple combination lock solutions for indoor applications. See Appendix, #4, #5.

Facilities managers may feel that a **padlock** provides enough security to prevent thieves and vandals from gaining access. Padlocks are best used for applications in locations with high traffic, or where area monitoring is possible or suspicious behavior (such as someone cutting the lock or hammering the mount) would be noticed. These applications use mounting kits or knobs to hold the padlock in place so the cover cannot be opened. Hoffman offers a padlocking wing knob, along with handles and latches designed for use with these types of locks. See Appendix, #6.

Instead of using mechanical lock components that are limited to a single, finite combination, a **key pad** uses software that allows access when the correct code is entered. This technology lets the user change the code periodically, increase the length of the code to make it more secure, or allow multiple codes to track who is accessing the contents and when the access occurs.

Fingerprint, hand, and eye scanners are the next generation of security mechanisms that can prevent unauthorized access to equipment. While still in the infancy stage for use with electrical enclosures or control panels, these high-tech devices use recognition software to identify the user before access is granted. Recent improvements have decreased the size of the touch screen and memory needed to allow these scanners to operate, so the variety of applications using recognition technology has dramatically increased. See Figure 4.

Figure 4. Fingerprint scanner.

Electrical interlocks provide internal safety lock-out and prevent access to an enclosure while the equipment is energized. These locks detect energy flow within the enclosure and prevent a door handle from turning if engaged. Hoffman offers electrical interlocks for use with hinged enclosures that meet UL 508A standards. Interlock defeaters are offered if access to an enclosure is absolutely necessary, even if the interlock is engaged. Refer to the *Environmental Protection of Control*

Panels: Overview and Standards Compliance white paper on www.Hoffman-Panduit.com for more information.
See Appendix, #7.

Layer #2 – Type of Material

The second layer represents the material that makes up the enclosure. Steel, aluminum, and composite materials may all be ideal, depending on the application. The thickness of the enclosure material also should be considered. Since each material used for enclosure construction exhibits a variety of characteristics, there is no universal material choice. This section discusses the characteristics and capabilities that make some materials suitable for different applications.

Mild steel can be shaped and formed by manufacturers more easily than stainless steel because of its low level of carbon content. However, this durability reduces mild steel's security ability as compared to stainless steel. **Stainless steel's** robustness makes it very secure for constructing an enclosure, with little concern for accidental damage. **Aluminum enclosures** are lightweight compared to steel and are used in industrial applications ranging from telecommunication cabinets, and traffic control equipment, to waste water treatment facilities. The lighter nature of aluminum makes it less durable than stainless steel, but also less costly. Although less durable than stainless steel, aluminum has a robustness that allows it to be more suitable in harsh environments than its mild steel counterpart. Aluminum is less likely to rust and like mild and stainless steel, it provides security and modification options suitable for any customer application.

For other applications, **non-metallic enclosures** may be used. While non-metallic enclosures have been around for 40+ years, increased awareness and knowledge of the benefits have raised demand. Non-metallic enclosures can be modified more easily at a job site, but are weaker compared to their metal counterparts. A common misconception is that non-metallic enclosures are less secure or tamper resistant than metallic enclosures, but when properly locked, non-metallic enclosures provide the same level of security.

When selecting an enclosure, design/controls engineers should consider whether Wi-Fi signals should pass through it. If electromagnetic interference must be kept out or prevented from escaping the enclosure, then metallic enclosures may be excellent for electrical applications, but may not be suitable for wireless networking because they can impede performance. These types of applications still need security and protection; therefore non-metallic materials can be a better choice to help equipment retain optimal performance.

Fiberglass is the most popular non-metallic choice enclosure, but **polyester and polycarbonate blends** are also prevalent. It is easier to add windows to a non-metallic enclosure, reducing the necessity for physical entry and allowing technicians to use latching or locking devices that are more secure. See Appendix, #8, #9.

Many applications can be affected by electromagnetic interference (EMI) or radio frequency interference (RFI). High current devices generate magnetic fields that can create interference problems. This interference can also be caused by stray voltages or currents from one source affecting other electronic equipment. With some equipment located in highly sensitive areas, EMI/RFI can be a major issue. Therefore, shielding is often required to prevent interference. For more information on EMI/RFI and Electromagnetic compatibility (EMC) requirements, please see the white paper in this series titled *"Noise Mitigation for Control Panels"* and the white paper titled *"Optimizing Control Panel Layouts for Noise Mitigation in Factory Automation Systems."* Both papers can be accessed at www.Hoffman-Panduit.com.

Layer #3 – Internal Latching Types: Single-Point to Multi-Point

The third layer is the type of latch that the lock mechanism uses to engage with the enclosure body. The most basic system for keeping an entry point closed is a single-point latch, where the handle, lock or latch turns 90º to create a single obstruction between the door and the enclosure side that keeps the door from opening. See Figure 5. Single-point latches provide a good barrier for small enclosures and enclosures with a single door that is not easily pried open.

Figure 5. Single-point latch.

Multi-point latches have an additional mechanism that creates more security points to keep a door from opening. See Figure 6. Since equipment can take up a considerable amount of space within an enclosure, a three-point latch may not be ideal, whereas the compact design and reliability of a single-point latch produces a better solution to prevent door obstructions. Using a single lock with a connection point at the handle, three-point latching systems have bars or rods that move up or down from the handle. These rods move into grooves or holes at the top and bottom of an enclosure to create a barrier that prevents the door from opening. Three-point systems help prevent unauthorized access when the enclosure design causes a door to be more flexible, allowing someone to easily pry open a corner, even when the door is locked.

Figure 6. Point latch mechanism.

Tall enclosures and two-door enclosures frequently utilize three-point systems to create a more robust seal and secure the contents, while other enclosures may use multiple, single-point latches and latches on different sides of the enclosure door to create a multi-point system. Having a three-point latching system helps prevent vandals from damaging an enclosure and compromising the seal or watertight nature. Hoffman offers many free-standing or wall mount enclosures that take advantage of the added security that three-point latches provide. With ratings up to 4X, typical applications using these enclosures and locking mechanisms include the pharmaceutical, food and beverage, packing, water, petroleum, and chemical processing industries.

Layer #4 – Design Geometry

The fourth layer encompasses the enclosure design and pry points where a potential thief or vandal can use leverage or force to open a locked enclosure. Minimizing seams and gaps, hiding hinges, and using flush mount doors eliminate pry points for intruders. The Pharmapro enclosure from Hoffman has a flush mount design that does not protrude. See Appendix, #10.

Another aspect of enclosure design that can increase security is the type of hinge used. Continuous hinges are usually on the outside of the door and can be removed from a locked enclosure, but require the right tools and a significant amount of effort for removal. Lift-off hinges and doors are easy to remove once the enclosure is unlocked and open, but are not removable when the enclosure is locked. Hidden hinges, or hinges that open on the inside of the door can further decrease the chance of a break-in because there is no opportunity to remove pins or the cover unless the enclosure is open. The Hoffman Concept enclosure includes these features and is ideal for a variety of machine control applications. See Appendix, #11.

Adding windows can either help or hurt equipment security. Full visibility alerts would-be thieves to enclosure contents. However, if no valuable equipment is inside and crime is a problem for the area, a window may deter vandals from damaging the enclosure to determine the contents. Many enclosures have dangerous electrical loads or meters inside, so a window may also notify thieves of the danger within and discourage any access attempt.

Layer #5 – Redundancy

An enclosure within an enclosure, or redundancy, comprises the fifth layer of security. The designer can repeat layers 1-4 by creating another locked enclosure within the exterior enclosure. For example, a smaller locked enclosed section merged into the main enclosure provides entry to some sections of the enclosure, but not to others, depending on the security clearance level of the personnel.

Safety lock-outs are another form of redundancy used in enclosure security. They allow use of multiple padlocks on a single, secured power source or enclosure so entry is only available when all workers have removed their locks. This safety feature enables workers to place their dedicated locks on a power source and travel to a terminal along the power source's circuit without being concerned that another worker will reconnect the power.

Layer #6: Network and Physical Security

The final layer of security is a solution that deters unauthorized network access at the physical layer. With many industries and applications requiring intensified security along with conventional software measures, separating a data network with a physical layer of security controls user access and prevents illegitimate entry. Examples of physical infrastructure solutions that help control this access include lock-in and block-out devices that attach to network and data ports to deter unauthorized port access.

Physical network security devices are effective for maximizing physical network reliability and security. Only authorized personnel are allowed to access the unused ports or connections that the physical network security devices help to secure. These devices can be used on both copper and fiber network connections to secure the integrity of the network infrastructure.

Lock-in Devices and Clips

Lock-in devices and clips prevent the unauthorized removal of cables, wires, connections, patch cords, or other networking equipment from the hub to reduce network downtime, data security breaches, and hardware replacement due to theft. See Figure 7. These devices require a special tool to install or release the lock-in plug from the jack, preventing unintentional removal and reducing downtime caused by unplugged cables. Panduit offers the QuickNet™ lock-in device and other models designed for use with Opti-Core® and keyed LC patch cords.

For copper, lock-in devices are available in standard and recessed versions to address the various depths of RJ45 jacks. The versatile design works with most existing patch cords, faceplates, patch panels, IP cameras, and other IP devices. It is also compatible with VoIP phones, which helps prevent unauthorized removal. See Appendix, #12.

For fiber, lock-in clips limit access and prevent unauthorized removal of cables, other networking equipment, or critical connections. The LC duplex lock-in clip can only be used with Opti-Core® LC and keyed LC patch cords. The installation/removal tool allows connectors to be locked into or released from adapters in modules, FAPs, cassettes, or patch panels for enhanced physical security. See Appendix, #14.

Figure 7. Lock-in device (top); Lock-in clip (bottom).

Block-out Devices

Block-out devices provide a simple and secure method to control access to data and deter vandalism to jacks. The jack module block-out device saves time and money associated with downtime, data security breaches, hardware replacement, and infrastructure repair.

Similar to lock-in devices, block-out devices can only be installed or removed via special tools at the network jack. However, instead of keeping cables and other connectors in place, block-out devices protect the network by preventing access to the jack and data through a physical barrier that obstructs the entrance that a data cable needs for access. See Appendix I, #13.

SC adapter block-out devices work with SC adapters that are TIA/EIA-604 FOCIS-3 compatible. Each device blocks one SC connector space, keeping it secure and reducing the risk of damage to the SC adapter. The devices can be used in applications such as switch panels, switches, and wall jacks that use SC adapters.

USB Type 'A' block-out devices work with USB 2.0 and USB 3.0 Type 'A' ports. See Figure 8. There are two options available: a removable device and a permanent device. Each design blocks one USB Type 'A' port, keeping it secure and reducing the risk of viruses being loaded, and unauthorized data being removed through the USB port. These devices can be used in any data application, especially with computers, switches, and other hardware that use **USB Type 'A' adapters**. See Appendix, #15.

Figure 8. USB Type A block-out device.

USB Type 'B' block-out devices work with USB 2.0 Type 'B' ports. There are two options available: a removable device and a permanent device. Each design blocks one USB Type 'B' port, keeping it secure and reducing the risk of viruses being loaded and unauthorized data being removed through the USB port. They provide an economical method to block unauthorized access at a physical layer to USB Type 'B' ports in printers, industrial network equipment, and other hardware devices, reducing the risk of unintentional or intentional damage. See Appendix, #16.

Conclusion

Integrating the security element into the equipment and enclosures is essential because it allows design/controls engineers to create multiple layers of security that work together to protect the network and equipment without retrofitting or replacing components. Pentair's Hoffman branded enclosure solutions feature several design layers that deter unintentional access into an enclosure, each adding some amount of cost but adding a significant level of security. Physical security solutions that help control access to automation devices can be effective additions to other layers of security employed in contemporary control systems. Network accessories from Panduit such as block-out devices and lock-in devices offer a secure solution for network components, which saves time and costs associated with security breaches, network downtime, repairs, and hardware replacement due to theft. Together, Panduit and Pentair offer diverse and complete solutions for protecting equipment from intentional and unintentional security threats to add value to their customers' physical security needs.

Appendix - Solutions from Pentair Hoffman and Panduit

#1		**Cylinder Lock Kit** Hoffman offers cylinder lock kits that fit in pre-drilled or punched holes with two key configurations available.
#2		**Keys and Inserts** Hoffman offers keys and inserts for triangular, square, double bits, Daimler Benz, and slotted configurations.
#3		**Screw Cover Enclosure** Hoffman offers screw cover enclosures rated for Type 1, 3R, 4, 4X and 12 applications.
#4		**3-digit Combination Lock** The 3-digit combination lock-in handle from Hoffman can be easily changed and eliminates the need to carry around a key. A quarter turn of the handle opens and closes the cabinet. Maintains cabinet rating Type 12.
#5		**4-digit Net Series L-Handle Combination Lock** The combination L-Handle fits Net Series cabinet doors from Hoffman and offers a 4-digit combination lock with master key override that can easily be changed. Install using existing cam from standard handle.
#6		**Padlocking Wing Knob** The padlocking wing knob from Hoffman offers handles and latches designed for use with these types of locks. When the padlock is in place, the wing knob cannot be rotated and the cabinet is secured. It maintains the cabinet rating Type 3R, 4, 4X, and 12.
#7		**Electrical Interlocks** These interlocks from Hoffman are for use with hinged enclosures that meet UL 508A standards. Interlock defeaters are also offered if access to an enclosure is absolutely necessary, even if the interlock is engaged.
#8		**Ultrx Fiberglass Enclosure** This enclosure from Hoffman is an excellent choice when metal enclosures will impede performance, either through heat accumulation or when electromagnetic interference is an issue.
#9		**Polypro Enclosure** Designed specifically for Wi-Fi applications, Polypro polyester enclosures from Hoffman perform exceptionally well in applications where harsh chemicals, weather extremes, and corrosive environments demand toughness from a lightweight enclosure.
#10		**Pharmapro Enclosure** This 4X enclosure from Hoffman can keep controls safe while minimizing surfaces and angles intruders normally use to pry the box open or off its mount.
#11		**Concept Enclosure** This enclosure from Hoffman is designed with hidden hinges, continuously welded seams, corner formed doors, and a three-point latch system on larger models.

#12		**RJ45 Plug Lock-in Device** This lock-in device from Panduit secures connections to reduce network downtime, data security breaches, and hardware replacement due to theft.
#13		**RJ45 Plug Block-out Device** The innovative design of this block-out device from Panduit snaps into RJ45 jacks and is released with the removal tool, ensuring the safety and security of the network infrastructure.
#14		**LC Duplex Lock-in Device** This lock-in device from Panduit works with LC duplex adapters that are TIA/EIA-604 FOCIS-10 compatible. Each device blocks two LC connector spaces, keeping them secure and reducing the risk of damage to the LC adapter.
#15		**USB Type 'A' Block-out Device** This block-out device from Panduit blocks unauthorized access to USB Type 'A' ports to provide additional security from viruses being loaded and data being removed through the USB port.
#16		**USB Type 'B' Block-out Device** This block-out device from Panduit blocks unauthorized access to USB Type 'B' ports to provide additional security from viruses being loaded and data being removed through the USB port.

Referenced Resources

- http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf
- http://www.strategiccompanies.com/pdfs/Assessing%20the%20Financial%20Impact%20of%20Downtime.pdf
- http://www.haidagwaiiobserver.com/Article.aspx?Id=440
- U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience
- Environmental Protection of Control Panels: Overview and Standards Compliance White Paper
- TIA/EIA-604 FOCIS-3 Fiber Optic Connector Intermateability Standard, Type SC and SC-APC
- UL 508A – Industrial Control Panels

Disclaimer

The information contained herein is intended as a guide for use by persons having technical skill at their own discretion and risk. Panduit and Pentair disclaim any liability arising from any information contained herein or for the absence of same.

About Pentair Equipment Protection

Pentair Equipment Protection, a Pentair global business unit, is the leading provider of worldwide product and service solutions for enclosing, protecting and cooling electrical and electronic systems. Its industry-leading brand—Hoffman—provides a broad variety of standard, modified and engineered solutions to the commercial, communications, energy, general electronics, industrial and infrastructure markets.

About Panduit

Panduit is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, increased agility and operational efficiency. Panduit solutions give enterprises the capabilities to connect, manage and automate communications, computing, power, control and security systems for a smarter, unified business foundation. Panduit provides flexible, end-to-end solutions tailored by application and industry to drive performance, operational and financial advantages. Panduit global manufacturing, logistics, and e-commerce capabilities along with a global network of distribution partners help customers reduce supply chain risk. Strong technology

relationships with industry leading systems vendors and an engaged partner ecosystem of consultants, integrators and contractors together with its global staff and unmatched service and support make Panduit a valuable and trusted partner.