How to Protect Control Assets Before the Cybersecurity Egg Cracks

Table of Contents

A Vulnerable Target

The target is on the back of industrial control systems (ICS) within the power and process industries. The number of attacks, as reported by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), has increased sixfold since 2010. Control systems at industrial facilities present a more attractive target to hackers as they offer a greater opportunity to exert control over the plant and cause potentially catastrophic damage. The attacks are growing in sophistication as hackers become more knowledgeable about the proprietary systems at the center of plant operations.

ICS cybersecurity is a global concern. The Federal Office for Safety in Information Technology in Germany recently revealed that a steel mill suffered a massive blast furnace explosion as a result of a control system cyber attack. The attack prevented the normal shutdown of the furnace. While it is unclear whether the explosion was an intended result of the attack, it is clear to investigators that the hackers had intimate knowledge of the control system environment. Thankfully, no lives were reported lost.

Although malicious attacks make the headlines, control engineers understand that the greater threat still lies with inadvertent engineering changes to proprietary control systems. These occur on a more frequent basis and can have equally disastrous results. The problem is that such changes can go unnoticed for long periods as manual change management processes do not really detect them.

The challenge the industry now faces is hardening ICS cybersecurity before a potentially devastating attack or inadvertent engineering change occurs. In this paper, we will discuss the current state of cybersecurity in the industry and best practices for implementing a comprehensive ICS cybersecurity strategy.

Hard on the Outside, Soft on the Inside

Companies from every industry suffer from Denial of Service and other attacks that disrupt operations or at least prove a nuisance to IT personnel. There is a constant battle between hackers (black hats) and security professionals (white hats) to stay ahead of the other. Combatants have traditionally waged this battle at the network- or PC-level, which is where security solutions have proliferated. The war has now spilled into the operation technology (OT) side.

Within the power and process industries, security and compliance personnel have invested millions of dollars implementing security standards, such as intrusion detection and firewalls, to secure plants. They have invested similarly in physical security to ensure only authorized personnel have access to critical parts of the plant. In both areas, plants continue to invest in hardening the outer layer of their operational infrastructure with the intent of keeping bad people at bay.

What remains largely unaddressed are the configurations of the proprietary industrial control systems that are at the heart of plant safety and productivity. Today's solutions provide a measure of security by protecting the networked devices that sit above the control system. Until now, no solution has focused on hardening the proprietary configuration of control assets.

Various Attack Vectors

The subsequent diagram illustrates the variety of attack vectors that can circumvent today's physical- and IT-based security. They include infected USB devices, third-party software updates, or misconfigured firewalls. Any one of these can expose a plant to an attack that cedes control to malicious hackers.

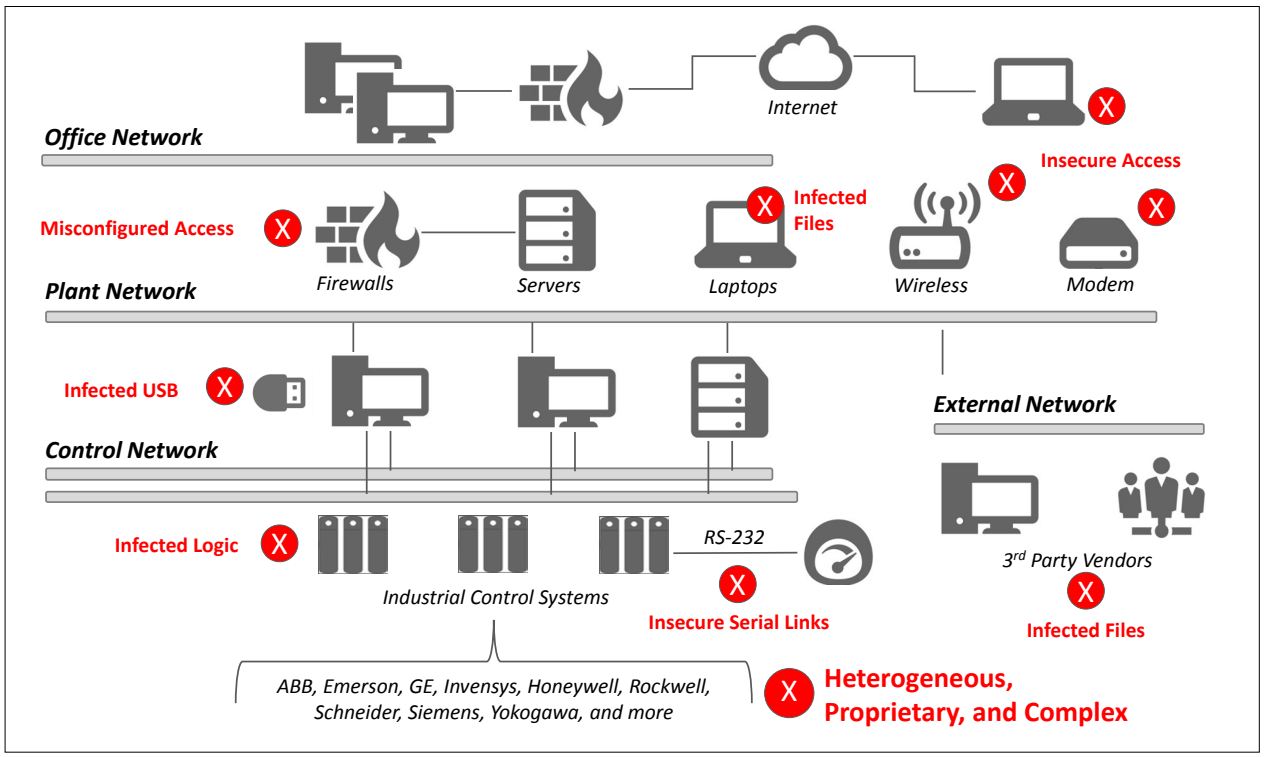


Figure 1: Various Attack Vectors

So, why are control systems, arguably the most critical assets in the plant, left vulnerable? IT professionals are versed in implementing solutions that manage IT asset configurations, ensure policy adherence, and monitor for unauthorized change. Why doesn't the control system have similar levels of protection? The following sections detail the four essential reasons why control systems continue to remain vulnerable.

1. Heterogeneity

Most plants have control systems sourced from multiple manufacturers. Although control system vendors offer various types of security offerings, none of them span all the assets in a plant or enterprise. The same holds true for vendor-supplied configuration management tools. As they are proprietary, technicians must manage configurations on each respective system and provide aggregated reporting. Best-in-class control system security demands consistent, centralized transparency and control over the myriad of assets in a plant. Heterogeneity of control systems within a plant makes this difficult to achieve with today's IT-focused solutions.

2. Proprietary

The internal configurations of control systems are proprietary. Automation vendors tightly control and protect the structure of their control and safety system configurations. No two systems – even those from the same automation vendor – have the same configuration structure or use the same set of tools to manage the configuration. Given that a typical power or process company may have more than 30 different process control, safety, and programmable logic controller systems, each with a unique and proprietary configuration structure, it becomes a daunting task to manage and protect these assets from cyber attacks in a consistent and effective manner.

Instead, many plants rely upon the tacit knowledge of individual system experts at each location to manage their respective systems. The methods used by the system experts are as different as the systems themselves, which can expose new security vulnerabilities. In fact, configuration management is often overlooked as a result.

Having highly proprietary, multi-generational, and multi-sourced control systems makes it untenable to rely on automation vendors to supply a common configuration management solution. According to the automation leader at a power generation company in the Southeast United States, they would have to use 30 different applications from more than 10 different suppliers in order to manage their automation assets. That would obviously defeat any goal of consistency and effectiveness, leaving the plants vulnerable.

3. Complexity

Internal configurations of control systems are highly complex and inherently difficult to manage. This complexity poses two distinct challenges. The first is the retention of the deep knowledge required by plant personnel to manage the systems properly. The second is the availability of a common configuration management application to facilitate critical operations, such as configuration change management and backup and recovery. In this light, proper configuration management becomes a difficult task.

The automation system is the primary platform for operational and safety improvement at power and process plants. It is not unusual to change the configuration of a control system on a weekly basis in order to improve or adapt to the changing conditions of a processing unit. Regardless of its rigor, a manual change management process without closed-loop feedback leaves control systems vulnerable to unwanted changes from either inside or outside actors. Unmanaged change to a control system can lead to dire consequences.

4. OT, Not Just IT

An industrial plant with a hardened IT layer, but a soft control system security environment at its core, is highly vulnerable to cyber threats. What is at risk goes beyond confidentiality of corporate information, as was the case with the 2014 Sony hack. At stake are personnel safety, economic loss, and even national security.

Even when there is corporate will to make control systems more secure and a strong set of IT controls in place, security personnel find that standard IT security approaches do not cover all the needs of control systems. Control systems lack connectivity, and system protocols are often unique for proprietary ICS systems. Frequent configuration changes make it difficult to understand normal operations automatically.

A hardened inner OT layer also provides critical protection when IT controls fail or are bypassed altogether. As an example, while normal maintenance practices involve controls engineers connecting laptops directly to OT devices, this bypasses most IT level controls including firewalls and intrusion detection systems.

Regulatory and Standards Bodies React

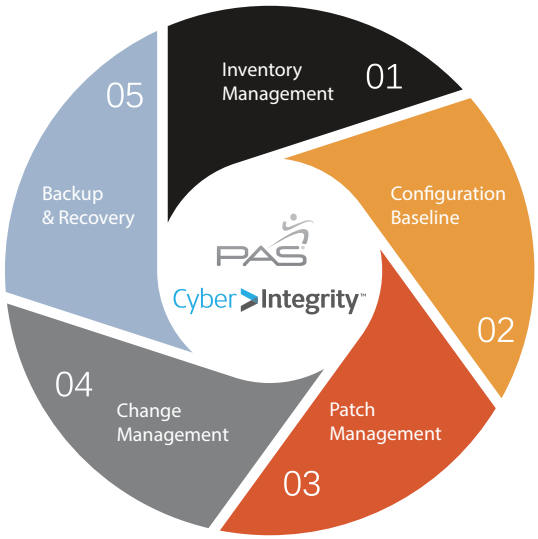
While companies continue to develop and enhance their own security standards, some face regulatory requirements depending on their country and industry. Nearly all regulatory environments include strong controls for inventory and configuration management of ICS infrastructure. For example, according to SANS, a cooperative security research and education organization established in 1989, inventory and configuration management represent the top two most critical security controls for effective cyber defense. The North American Electric Reliability Corporation (NERC) prescribes security controls with its Critical Infrastructure Protection (CIP) regulatory standards for the power industry, and the National Institute of Standards and Technology (NIST) does so with SP800-82 for a broader set of industries in the United States. Internationally, there is the ISA-99/IEA-62443 standard. Other country-specific standards such as the Ministry of Information and Communications Technology's (ictQATAR) Prime Minister's Decision No. (18) of 2013 are emerging as well.

Taking Control of Configuration Management in Control Systems

Configuration management of any control system involves five essential functions – asset inventory, configuration baseline, patch management, change management, and backup and recovery. If a cyber attack successfully circumvents the best laid perimeter defenses, recognizing the effect of an attack is an integral part of a multi-layered security approach that prevents damage before it occurs. Many companies perform these five functions today, but do so manually. Their approach is expensive, slow, and error prone – not a good combination when the goals are safety and productivity.

1. Inventory

It is all too commonplace for plant personnel to lack a single, up-to-date inventory of all control assets. Having this list is critical since any device connected to a control asset is a potential attack vector. It only takes one compromised system to wreak havoc on plant operations.



Determining the inventory of all proprietary control assets is difficult due to the various communication protocols used by different vendors. This differs from network-based IT systems in which nearly every asset is connected via Ethernet and is therefore "discoverable" via well understood tools that can scan the network. Few assets in a control system are connected via Ethernet and remain hidden from easy detection. It is necessary to use a combination of methods to collect inventory of such assets.

Additionally, there is important inventory information including details on control strategies, I/O cards, firmware, and installed software buried deep within the proprietary databases of the distributed control systems, programmable logic controllers, and remote terminal units. Best practices prescribe collecting this data and adopting an evergreen inventory policy. Automating inventory discovery is extremely difficult when dealing with the heterogeneous and proprietary configurations normally found within control systems.

2. Configuration Baseline and Policy Enforcement

Once the inventory of a plant is known, operations personnel need to establish a baseline configuration. The baseline configuration is the starting point for managing assets throughout their operational life. As change is a constant in any plant, the baseline provides a known good state for a particular asset. This ultimately provides a means to evaluate whether a change is operationally acceptable.

When building a configuration baseline, it is important to capture configuration policies as well. Configuration policies monitor for conditions outside of acceptable operational or security boundaries and alert personnel of a violation. Configuration policies permit Operations to manage groups of devices together, which results in more efficient change management processes.

3. Patch Management

Many plant environments today rely on spreadsheets and open-ended, manual processes to evaluate and manage patches. The result is a lack of consistency and visibility into patch application and vulnerability assessment. Workflow-driven automation allows companies to import patch information from Microsoft®, identify control assets affected, track vendor patch approvals, and drive testing, implementation, and mitigation activities. Doing so improves process efficiency and celerity. A closed-loop process also helps avoid regulatory fines and penalties, coordinates disparate patch management ownership functions, and provides visibility to all process stakeholders.

4. Change Management

As stated earlier, configuration change is constant in a plant. Device configurations are updated for a multitude of reasons. These reasons range from changes to the physical operating properties of the system, such as pressure or temperature, to firmware updates for a device. As a result, plant operators need to understand when a change has occurred and whether that change was authorized. Unauthorized changes, whether malicious or inadvertent, can cause reliability issues, physical damage to equipment, or injury to personnel. Plant operators actually have the opportunity to detect cyber attacks or inadvertent changes that affect control assets when they have a good baseline of all assets in a plant and proper change management.

5. Backup and Recovery

The best defense strategies must anticipate a breach that affects plant operations. Although a network breach can have significant consequences, one that affects a control system configuration can prove disastrous to a company. Having periodic backups and tested recovery processes accelerate returning to normal operations and minimize the impact to safety and productivity.

Hardened on the Outside and Inside

The PAS ICS Cybersecurity solution is the only offering in the market that provides centralized monitoring and management of control system configurations. PAS Cyber Integrity™ hardens control system security by capturing the inventory of all control assets in a plant, creating a baseline of situation-normal configurations, facilitating a closed-loop patch management process, detecting when a change occurs, initiating a response protocol when a change is unauthorized, and providing automated backup and recovery capabilities in case all else fails.

Cyber Integrity delivers the following benefits:

- Gain inventory visibility into IT and OT cyber assets,
- Reduces compliance efforts by up to 90 percent,
- Avoid regulatory fines and penalties from non-compliance,
- Prevent unplanned downtime due to unauthorized changes, and
- Manage across all major control system manufacturers.

Conclusion

It is no longer sufficient to rely only on hardened perimeter defenses and leave the core control system of a plant soft and vulnerable to attacks or engineering mistakes. Manual efforts are easily defeated and unscalable. The only answer is to achieve a level of control asset security that rivals the network and physical environments. Automated inventory, patch, and configuration change management are the right mechanisms to do so as it alone hardens the inside of the control asset egg.

Additional Resources

To learn more about implementing an ICS Cybersecurity strategy and the PAS methodology for doing so, please visit www.pas.com/cyber-security or email info@pas.com.

About PAS

PAS Global, LLC is a leading provider of software solutions for process safety, cybersecurity, and asset reliability to the energy, process, and power industries worldwide. PAS solutions include industrial control system cybersecurity, automation asset management, alarm management, high performance HMI, boundary management, and control loop performance optimization. PAS solutions are installed in over 1,100 facilities worldwide with more than 41,600 users. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.