ICS Cybersecurity: Protecting the Industrial Endpoints That Matter Most

Scott Hollis
Director, Product Management
&
David Zahn
CMO and General Manager, Cybersecurity Business Unit

Table of Contents

Industrial Cybersecurity Challenges

Endpoint detection and response (EDR) is one of the vogue technologies in industrial control system (ICS) cybersecurity today. Before EDR adoption became popular, industrial process and power generation companies focused primarily on process control network (PCN) perimeter defenses, such as firewalls, to keep the bad guys out. Cybersecurity professionals understand that perimeter defenses have limitations – particularly when you consider the insider threat – but they are an integral component of a defense in depth strategy. If a firewall is overcome, then additional layers of protection, such as EDR, must exist to protect critical systems.

In fact, this is a movie we've seen in corporate information technology (IT), where protectors of the realm realize that they are one properly worded, payload-enabled email away from an attacker circumventing their best perimeter security technologies. This is precisely why antivirus software, application whitelisting, and intrusion detection are so commonplace today.

The problem with EDR in a PCN is that EDR implementations have focused on only a small subset of the cyber assets found within an industrial process facility. Because most of the EDR solution vendors sprang from the corporate IT side, they are architected for IT-based systems, such as workstations, servers, routers, and switches. It is imperative that these systems are addressed, but they comprise only 20 percent of the cyber assets that exist in a PCN. The remaining 80 percent are found within the proprietary industrial control systems.

In the classic Purdue Model, the proprietary systems are those that reside in Level 1 and Level 0, where you find controllers, safety systems, and smart field instruments. These industrial endpoints comprise 3rd Party Modules, Com Modules, Control Level Firewalls, Controllers, Foundation Fieldbus Devices, Hart Devices, IO Cards, Operator Stations, Profibus Devices, Wireless Devices, and Wireless IO Modules. These are the most important endpoints in an industrial facility as they have primary responsibility for production and safety – the two most significant drivers of ICS cybersecurity investment today. In fact, if you turned off all the other systems in an enterprise – the accounting, email, reporting, SCADA, and other systems – the industrial facility would continue to run. The refinery would still produce gasoline, the power plant would still generate electricity, and the manufacturing facility would still stamp out parts.

> "Protecting information alone isn't enough, and ensuring the confidentiality, integrity and availability of that information isn't enough. Leaders in risk and cybersecurity from core to edge must now assume the responsibility of providing safety for both people and their environments..."
>
> Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change, Earl Perkins, Research VP & Christian Byrnes, Managing VP

Yet, it is these endpoints – again, the most important ones in an enterprise – that EDR has not traditionally covered. Part of the reason is that many organizations do not know all the systems they have. They obviously have insight into major systems like distributed control systems, but they may not know every programmable logic controller, and they certainly do not track detailed configuration data on IO cards, firmware, control logic, and more. This is clearly not acceptable from a cybersecurity perspective. Imagine NASA's Mission Control Center relying on extensive security to prevent intruders from getting access to the mission command center, but not knowing all the control systems on a booster rocket or lacking any information about how they are configured. This is essentially the situation that exists in most industrial process facilities today.

With cyber incidents and reported vulnerabilities on the rise, industrial cybersecurity leaders must deploy proactive industrial EDR across the entire PCN. Failure to reduce industrial endpoint attack surfaces (e.g. insecure configurations, missing patches, vulnerabilities) increases the risk of malicious changes or unintended misconfigurations.

This paper will examine how endpoint detection and response should extend to proprietary endpoints, what security controls have the greatest effect on reducing risk for these cyber assets, and what best practices apply.

More About the Endpoints That Matter the Most

Proprietary control systems, which include distributed control systems (DCSs), programmable logic controllers (PLCs), safety instrumented systems (SISs), advanced programmable controllers (APCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and more, are at the heart of industrial process operations. They are highly complex and most facilities have a variety of vendor systems in production use. It is common for plant managers to describe having "one from every manufacturer" in their facilities and certainly this is the case across an enterprise. Because these systems are proprietary, there are no common protocols to interrogate them for configuration information. In fact, significant architectural differences can occur from one product to another within a single vendor product line. So, deciphering one vendor's proprietary control system does not necessarily give insight into another.

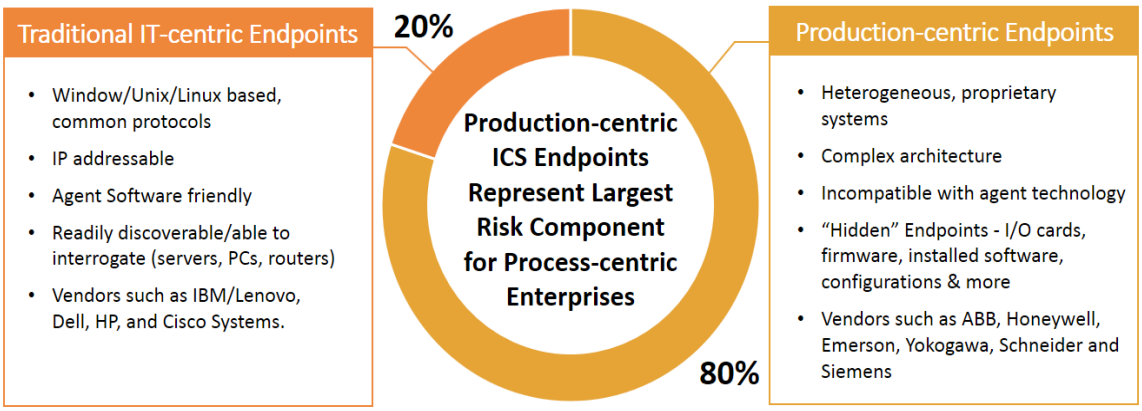


Figure 1: Traditional IT-centric Endpoints vs. Production-centric Endpoints

Sensitivity to process preservation drives cybersecurity decisions within a process control network. For instance, putting agents on proprietary ICS not only invalidates support, but it also violates process control engineering best practices. The prevailing mantra that "if it ain't broke, don't fix it" is always in play. This means that systems can contain known vulnerabilities with available patches for extended periods of time or possibly forever. It is considered acceptable to implement security controls in front of these systems to reduce risk versus upgrading and possibly degrading system performance.

Now, contrast this to the IT-centric systems that also exist in a PCN. There are different flavors of vendors, but standard protocols, such as WMI and SNMP, give cybersecurity professionals the ability to gather configuration information and, ultimately through analysis, understand whether an unauthorized change has occurred. These systems – the ones that comprise Level 2 and above of the Purdue Model – are more easily secured as agents and typical endpoint security controls are permitted.

ICS Vulnerabilities and Cyber Incidents Are Increasing

The threats to a PCN come from two vectors – external and internal. External actors have shown increasing willingness and capability to penetrate layered defenses to gain access to control systems. In its 2015 Global State of Information Security Survey, PWC cited that nation-state supported attacks had risen over 108 percent over the prior year. In December 2015, 225,000 Ukrainians experienced such an incident first hand when they lost power; a similar attack was repeated a year later – almost to the day.

Nation-State Supported
225K Ukrainians Lose Power

- **Impact**: 225,000 Ukrainians lose power due to outsider cyber attack
- **Weaponization**: BlackEnergy3 establishes network presence
- **Access**: Credentials harvested and remote access tools used to access PCN
- **Execution**: Substation breakers opened via VPN access into SCADA systems
- **Amplification**: Malicious firmware updates; master boot records/logs erased
- **Extension**: Telephonic DOS attack

Internally generated incidents are significant and in some ways more dangerous; as the malicious insider has detailed knowledge of the security controls, understands how to produce a desired outcome, and has authorized access.

Not all unauthorized change is malicious. An engineering mistake can generate similar outcomes to an attack. In IBM X-Force Research's 2016 Cyber Security Intelligence Index, the number of incidents attributed to malicious insiders was 44.5 percent, and inadvertent ones were 15.5 percent. Although rarely making the public eye, insider-based incidents have affected facility operations (see anonymized "Fired Employee" example).

Fired Employee
Production Shutdown

- **Impact:** Mill loses production after "insider" cyber attack
- **Profile**: Attacker was a recently fired System Administrator
- **Access**: Fired employee retained access to internal plant systems
- **Execution**: Distributed and quality control systems updated from home
- **Recovery**: "Significant" lost production time investigating and recovering systems

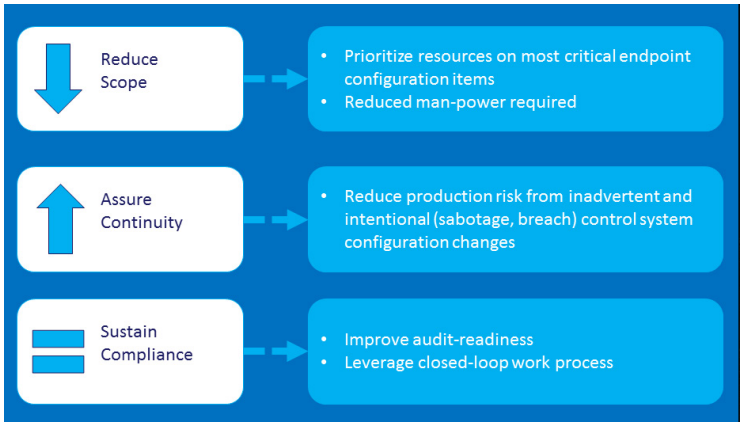
Although social engineering is still the most successful tool for penetraing an organization, once inside the network, vulnerabilities provide avenues for exploit. Per recent ICS-CERT reports, ICS endpoint vulnerabilities exist across all manufacturers. The vulnerabilities primarily comprise buffer overflows, hardcoded credentials, and cross-site scripting. The most recent reports show a 110% increase in reported ICS endpoint vulnerabilities. Vulnerabilities increase risk when not identified and sufficiently addressed.

Figure 2: Reported Cybersecurity Attacks, 2010 to 2015

It's All About the Baselines

Change is a constant in any industrial process facility. At the ICS configuration level, the number of changes can quickly soar into the thousands. It is why solely relying on checksums for change detection is ineffectual. The likelihood for change on any given day is high, and checksums do not tell engineers or cybersecurity personnel what changed. Any investigation is like searching for the proverbial needle in a haystack.

Not all change is created equal. Certain changes are important from an engineering perspective while others are important from a security tracking or audit one. Given the potential for high volumes of change, configuration management best practices dictate establishing one or many baselines.



A configuration management baseline is different than traditional definitions of baselines. In this definition, a baseline is merely a subset of configuration data deemed important to track. An initial baseline establishes the as-is configuration of a system. With each new collection of configuration data, the new data snapshot is compared to an existing baseline with differences indicated.

Depending on the risk profile of a cyber asset, specific workflow-based procedures are initiated for detected changes. For instance, if a change is identified on a configuration parameter of a historian, an incident response protocol will require investigation, but that will not necessarily have the same priority as a configuration change on an SIS. The SIS is deemed more operationally critical, and therefore demands greater urgency. Typically, the risk profiles of cyber assets come from a risk assessment process performed periodically.

Managing Change

Change investigation will have two potential outcomes. First, the change was authorized, and the baseline is updated to reflect the newly accepted configuration. Thus, the most recent baseline reflects a good working state – despite potentially long-running investigations into certain changes. Second, the change was unauthorized, and engineers must revert the changed configuration to its previous state. In this case, unauthorized changes may require additional steps such as work process updates, training, and other measures to prevent future occurrences. In both cases, automating the change detection, investigation, and remediation steps via workflows creates electronic breadcrumbs that provide evidence to compliance and audit processes.

To help illustrate this process, imagine an engineer has a work order to update a field instrument that controls flow rate into a highly volatile chemical process. While making configuration updates, the engineer mistakenly updates the high range (PVEUHI) of the instrument from 1004 to 1104.

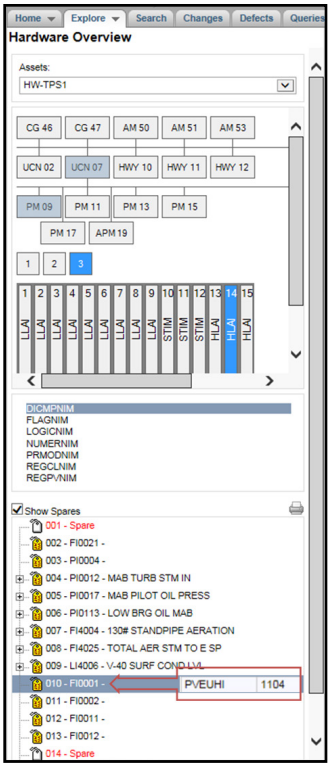


Figure 3: Hardware Overview

A robust configuration management process has range values defined as part of a critical asset baseline. After the engineering error, the change is flagged, and an incident response protocol initiates an investigation. The investigating engineer will have detailed information not only on the changed value, but also data such as the asset's location and what other systems are connected to it. The engineer can immediately assess whether the change is appropriate, or as in this case, remediate. Personnel can verify the value is restored to its previous state as the next configuration import will flag a change to this same field.

If internal or regulatory compliance standards require evidence of unauthorized change investigation, this is merely a simple report. Alerts and policies can help further lock down monitoring of critical configurations. Lastly, if governance or compliance groups require tracking of a different set of configuration values, those are different baselines managed in similar fashion to the previous example.

Network-Based Technologies: A Quick Word

Some organizations have turned towards deep packet inspection (DPI) to detect and manage change. DPI is roughly the same technology utilized for intrusion detection by today's corporate IT. Typically, DPI is deployed on a span/mirror port where it deciphers traffic to identify malicious activity.

Although this technology has a place in a defense in depth strategy, there are limitations to its inventory and configuration management capabilities. First, DPI gathers detailed configuration data only as traffic is generated and changes occur; thus, it is unable to detect the current configuration settings of all devices on the ICS network. This leaves gaps in both current ICS settings as well as device inventory. Second, DPI does not monitor most of the communications below Level 2. This means changes that occur between Level 1 devices, and Level 1 to Level 0 devices, are opaque. Finally, were a change detected, visibility into what changed, what the state was before the change, and the impact it has on other interdependent systems is limited.

Again, DPI is an important component to a layered defense; detecting anomalous traffic reduces risk. However, configuration management best practices require that sites have the ability to collect "as-built" control strategies from Level 0 and Level 1 devices including tags, properties, custom programs, graphics, inter-system connections, and more. This gives engineers a digital reference model of their entire control infrastructure on day one, making them more efficient and productive at their jobs.

Endpoint-Based Technologies

Endpoint-based technologies are proactive – they see what is "actually happening" on production-centric endpoints. Personnel can see before and after states of configuration values. And, it does not matter what communication protocols they utilize, since the endpoint-based solution is viewing the actual configuration data.

With endpoint-based technologies, personnel can see physical changes, such as new IO cards. They can see firmware changes made locally by a serial connected maintenance laptop, as well as register/tag changes resulting from an input that came from a wrong address. They can also see newly loaded SIS ladder logic with a misconfigured bypass condition.

With ICS configuration data, personnel know exact details of what they have – such as product version, model, service-pack or patch revision. With this knowledge, they can immediately know if a specific patch is applied. They can know the risk from the latest ICS-CERT vulnerability advisory with a simple query. They can know if configuration settings violate organizational policy or safe ranges.

Finally, endpoint-based technologies can back up configuration data. During the process of inventory and configuration data collection, automation software can store configuration files locally and offsite.

Closing the Loop on Vulnerabilities and Patch Management

Managing Microsoft security patches and reported ICS-CERT and US-CERT vulnerabilities is a required aspect of any proactive cybersecurity strategy intent on reducing the industrial endpoint attack surface. It is realistically only possible to accomplish once there is visibility into all industrial endpoints across PCNs. Too many organizations have patch and vulnerability management capabilities only for their IT-centric endpoints, yet little for the production-centric ICS endpoints. There simply are not enough resources available to do it manually, and manual efforts are error-prone.

There are two key capabilities needed. First, it is important to identify which vulnerabilities and security patches are applicable to the industrial endpoints in an organization. It is impossible to do manual research on all of them; there are over 80,000 on US-CERT and over 1,600 on ICS-CERT. Research time is drastically reduced when key inventory data (i.e., manufacturer, model, and version number) informs a simple query.

Second, with patches and vulnerabilities identified enterprise-wide, personnel can determine where to apply patches and where to apply additional security controls. A risk assessment process usually guides these decisions as factors such as likelihood of exploit and impact are captured here.

As an example, consider a published advisory on ICS-CERT for Emerson DeltaV DCS Controllers (see Figure 4), which are Level 1 devices. If an organization is monitoring these advisories, it tends to rely on an email asking each facility for a response on whether it is impacted. Not surprisingly, response rates are often well below 100% and not always accurate.

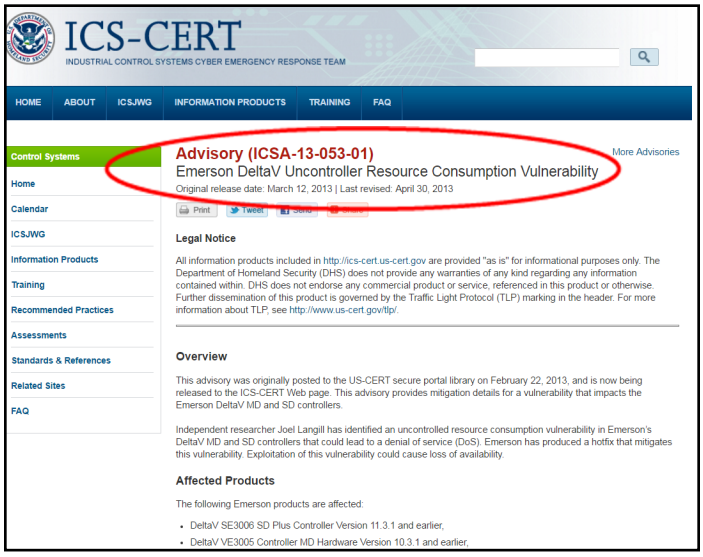


Figure 4: ICS-Cert Advisory for Emerson DeltaV MD and SD Controllers

The advisories themselves require careful analysis to understand impact and criticality. Inside each advisory is an "Affected Products" section, which contains details about the vulnerability, its operational risk, mitigation steps, and more. This is relatively straightforward to evaluate for a single vulnerability; but, scalability becomes an issue when this process is manual across the thousands of vulnerabilities and multitude of ICS endpoints.

Automation provides a way to access applicability and risk as well as drive appropriate actions. Pre-defined workflows will track patch testing, implementation, and mitigation actions to give full visibility into progress.

PAS Solution

PAS Cyber Integrity™ is a best-in-class, endpoint-based cybersecurity software that covers all major industrial control systems. Cyber Integrity leverages the Integrity software platform that has over 200 man years of investment deciphering and integrating control system configuration data into a single repository. The solution provides automated inventory, configuration, patch, vulnerability, and compliance management as well as backup and recovery preparedness.

Cyber Integrity aggregates and contextualizes configuration databases, programs, and user interfaces, which facilitate risk management for the variety of vendor control systems in a single industrial process facility or across multiple facilities. It simplifies the visualization and management of actionable information improving operational reliability, security, and safety.

Cyber Integrity monitors and detects unauthorized changes centrally automating investigation, remediation, and mitigation steps through polices and workflows. It also automates the steps behind closed-loop patch and vulnerability management processes as well as speeds recovery in the event the system is damaged or lost. Using Cyber Integrity, industrial facilities gain automated, normalized inventory data across all IT- and production-centric endpoints in the PCN. The software presents a unique and holistic view of control system assets beyond the reach of traditional IT-centric or vendor-specific solutions.

Cyber Integrity Benefits

- Hardens industrial control endpoints against cyber threats
- Enables internal and regulatory compliance
- Reduces compliance and operational efforts by up to 90%
- Prevents unplanned downtime due to unauthorized changes
- Manages across all major control system manufacturers

Summary

To assure effective industrial cybersecurity that minimizes industrial endpoint attack surfaces, organizations must employ proactive, endpoint-based protection that is purpose-built for PCNs. Organizations should ensure that they see and manage production-centric endpoints in addition to IT-centric endpoints. Inventory, configuration, patch, and vulnerability management as well as configuration backups are must-haves to protect industrial endpoints and identify changes that could indicate compromise. And, once deviations or potential compromises are identified, incident workflows should automatically drive remediation efforts through to resolution.

With most Boards of Directors now focusing attention on cybersecurity risk reduction, industrial cybersecurity leaders must focus on securing the endpoints that matter most – proprietary ICS endpoints that control production. Failure to reduce attack surfaces on these cyber assets will result in malicious changes and unintended misconfigurations that impact reliability, safety, brand, and ultimately the bottom line.

Next Steps

For additional insight into production-centric proprietary ICS endpoint visibility consider reading this white-paper: ICS Cybersecurity - You Cannot Secure What You Cannot See

To learn more about how you can overcome internal obstacles through automation to ensure that industrial facilities are protected, view this webinar: How Do We Move to a Production-Centric Cybersecurity Model?

About the Authors

Scott Hollis

Director of Product Management

As Director of Product Management at PAS, Scott has more than 20 years of experience in security and performance management. Under his leadership NetIQ entered the SIEM market culminating in Gartner leadership designation. He subsequently led the creation of the industry's first true multi-tenant, single instance, log management SaaS platform at Alert Logic. He has held senior positions at various sized organizations ranging from privately held venture-backed technology start-ups to publicly traded Fortune 100 companies including BMC Software, NetIQ, Alert Logic, Quest Software (now a Dell company), Zenoss, and Tenable Network Security. He has a B.S. (cum laude) in Computer Science from Virginia Tech, and an M.B.A. from the University of Houston.

David Zahn

Chief Marketing Officer and the General Manager of the Cybersecurity Business Unit

David Zahn is the Chief Marketing Officer and the General Manager of the Cybersecurity Business Unit at PAS. David has more than 24 years of enterprise software and services experience within startup and high-growth companies in oil & gas and IT. Prior to PAS, David was Vice President of Marketing at FuelQuest and Vice President of Marketing at Avalara. He is a frequent speaker at industry events, and has a BA in Economics and Managerial Studies from Rice University as well as an MBA from the McCombs School of Business.

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.