PAS®

ICS Cybersecurity. Safety. Compliance.

ICS Cybersecurity and the Devil's Rope

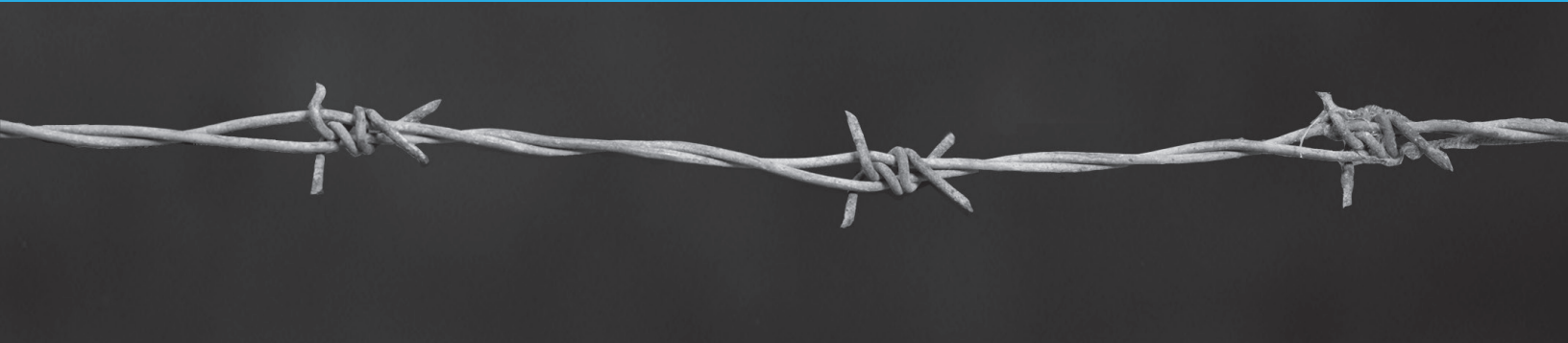


Table of Contents

Introduction

Near the end of the 19th century, the "Devil's Rope," or barbed wire, divided the West protecting the assets of farmers from ranchers who wanted to maintain their traditional way of life – an open range upon which their cattle could graze unfettered. Outlaw groups were recruited to cut fences and reestablish open access to land and public water sources. This did not sit well with farmers, who turned to lawmen for help. This conflict grew and eventually became known as the great Fence Cutter War.

Fast forward to the present time. We've erected an array of perimeter-based protection to safeguard not farmland, but industrial cyber assets. However, a new breed of fence cutters – nation state threat actors and malicious insiders – have successfully breached our best defenses, putting safety, reliability, and ultimately profitability of our nation's critical infrastructure at risk.

Why have our best efforts to secure industrial facilities fallen short? The answer is that we've taken an IT-centric versus a production-centric approach to industrial control system (ICS) cybersecurity. This has left the systems responsible for safety and production vulnerable to malicious attacks or unintended incidents.

Securing ICS is certainly a challenge, as the endpoints that matter most are highly complex and proprietary. Unfortunately, industrial facilities don't often have an accurate, comprehensive inventory of all their systems. Also, despite the existence of known vulnerabilities within ICS assets that exist on process control networks (PCNs), companies today still struggle with vulnerability identification and management.

How can you secure what you cannot see? And further, how can you know when a vulnerability on an ICS puts safety and production at risk?

This paper examines how the "Devil's Rope" of today has left our critical infrastructure vulnerable. It also discusses current ICS vulnerability management challenges, as well as how to address them by taking a more production-centric approach to managing vulnerabilities on Level 2, 1, and 0 ICS assets.

ICS Vulnerability Management Challenges

New research from SANS shows that ICS cybersecurity has become a significant concern – 67 percent of survey respondents reported that they consider the threat to ICS to be either high or severe/critical (SANS Securing Industrial Control Systems, 2017). This fear is born from successful attacks such as the Ukrainian power grid attack in December 2015, the Industroyer/CrashOverride malware attack one year later in December 2016, and a new campaign of attacks targeting energy companies in the spring and summer of 2017 by a group called Dragonfly 2.0. Each showed the ability and will to shut down power.

ICS vulnerabilities present attackers with additional options to compromise operators. However, despite the existence of known vulnerabilities on systems within PCNs, industrial companies are still struggling with ICS vulnerability identification and remediation.

ICS Vulnerabilities Don't Get the Attention They Deserve

Automation systems are vital infrastructure for most industrial processes. As these systems become more advanced and connected, they become increasingly attractive targets. For example, a recent report from Kaspersky Lab highlighted that almost 40 percent of monitored ICS assets faced an attack at some point in the first of half of 2017 (Threat Landscape for Industrial Automation Systems in H1 2017).

Industrial attacks are garnering more public attention. Despite the growing media hype around vulnerabilities in critical infrastructure though, far too often ICS vulnerabilities do not receive similar attention, typically due to the following reasons:

- Vulnerability exploits under-reported
- False sense of security
- More disclosures than capacity to investigate

Vulnerability Exploits Under Reported

Given that ICS assets are high consequence targets, they are attractive to threat actors. Yet, many ICS asset owners pay insufficient attention to ICS vulnerabilities even when exploits may exist in the wild.

Some Successful ICS Vulnerabilities Exploited in the Wild				
Vulnerability	Attack	Exploited	Disclosed	Known Victims
Siemens Simatic S7 DLL loading mechanism vulnerability	Stuxnet	July 2009	June 2010	NEDA Industrial Group, Natanz, Iran
Siemens WinCC insecure SQL Server authentication	Stuxnet	July 2009	June 2010	NEDA Industrial Group, Natanz, Iran
GE Cimplicity Path Traversal	Attributed to the Sandworm Team	January 2012	June 2012	Various
Moxa UC-7408-LX Plus unauthenticated firmware	Attributed to the Sandworm Team	December 2015	May 2016	Kyivo-blenergo Energy Distribution Facility, Ukraine
IRZ RUH2 3G unauthenticated firmware	Attributed to the Sandworm Team	December 2015	May 2016	Prykarpattya-oblenergo Energy Distribution Facility, Ukraine

Disclosure is a tricky thing. While we have some awareness of who has received audit fines and certain attacks do make the public forum, it is unclear how well companies are preparing for the next attacks. We do know that there are intrinsic challenges to overcome if the battle is to be won.

False Sense of Security

Most ICS asset owners rely on traditional corporate IT practices and solutions, such as network segmentation, firewalls, and air gapping – the modern-day IT version of the "Devil's Rope" – to deny threat actors access to industrial assets. However, they underestimate just how accessible and at risk their assets actually are.

As little as 15 years ago, control systems were stand-alone assets, unconnected to IT networks or the outside world. IT and ICS networks were isolated from each other using different protocols to communicate.

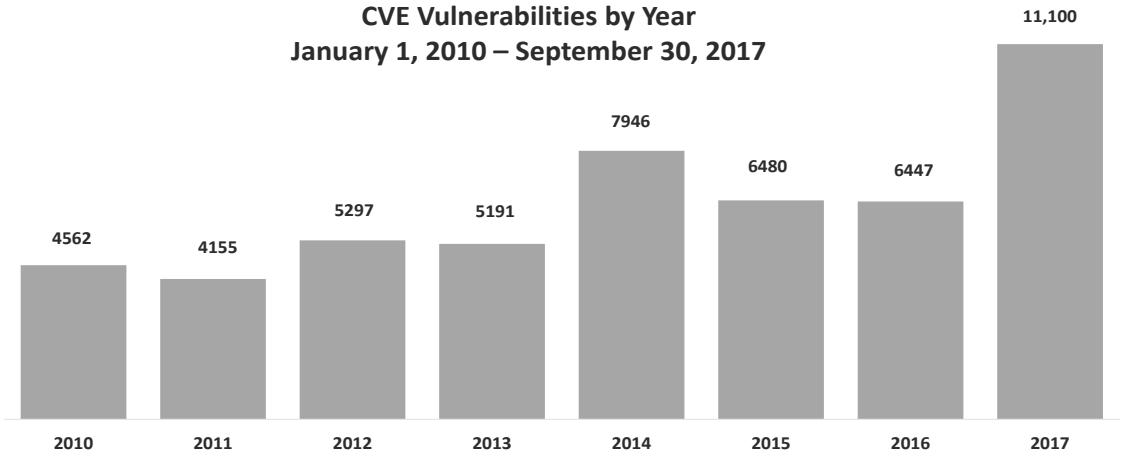
However, the nature of control systems and their connections to IT systems and the Internet has changed. While in the past, control systems were typically custom-built air-gapped systems, today they are IP-addressable and connected. ICS and IT systems increasingly connect and communicate, and more ICS are remotely accessible than ever before.

A 2016 report from Kaspersky Lab, Industrial Control Systems and Their Online Availability, illustrates this trend, as well as the vulnerability risk Internet exposure presents to ICS assets. The research showed 220,558 ICS components could be accessed from the Internet. Even more concerning, this same study found that 92 percent of these ICS assets had vulnerabilities.

As the report demonstrates, far too often hidden ICS asset connections to the Internet serve as an open door into the heart of industrial controls. Threat actors are skilled at finding and exploiting these gaps in perimeter security in their quest to control or damage systems maliciously. Network segmentation has offered modest protections and limited broad-based exposure, but cybersecurity professionals should not assume perimeter security solutions alone can protect their ICS assets.

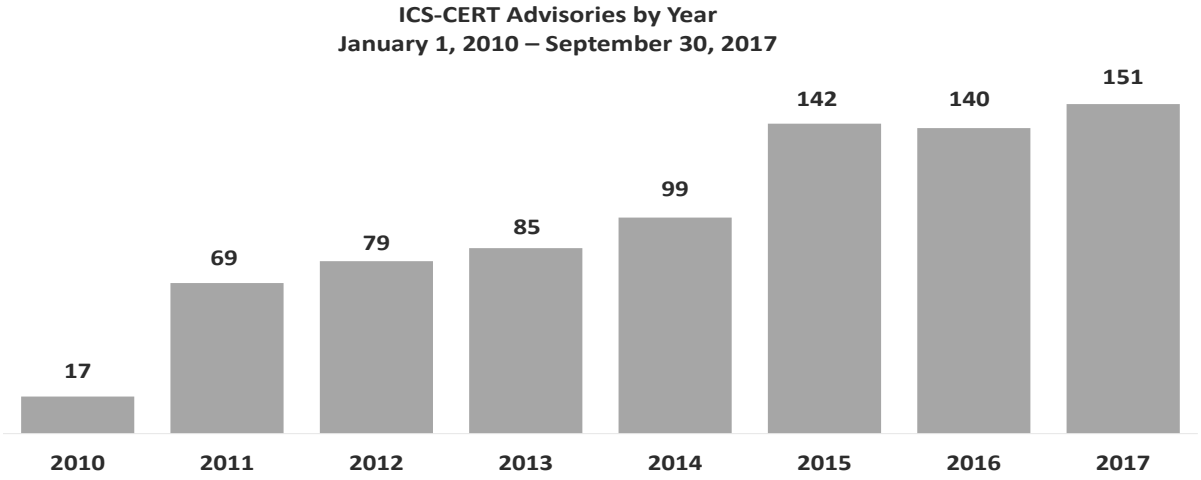
More Disclosures Than Capacity to Investigate

Vulnerabilities are tracked in the NVD using CVE identifiers. Since their launch in 1999, the number of CVEs has grown steadily. More than 51,268 CVEs were published between January 2010 and September 30, 2017. 11,100 CVEs were published within the first nine months of 2017 alone – a new record.



Traditionally, automation vendors were reluctant to publish discovered vulnerabilities. Some feared that if they were overly transparent regarding vulnerabilities, other vendors would use this information against them. Many preferred to fix vulnerabilities quietly as they worked on an updated version of the product, then asked their customers to upgrade if a vulnerability was publicly disclosed.

After Stuxnet made headlines in 2010, however, it became clear that Level 1 and 0 ICS vulnerabilities could impact industrial facilities. The number of publicly disclosed vulnerabilities began to increase greatly with ICS-CERT advisories for Level 1 and 0 ICS assets increasing sevenfold since 2010 (ICS-CERT Year in Review: Industrial Control Systems Cyber Emergency Response Team 2016).



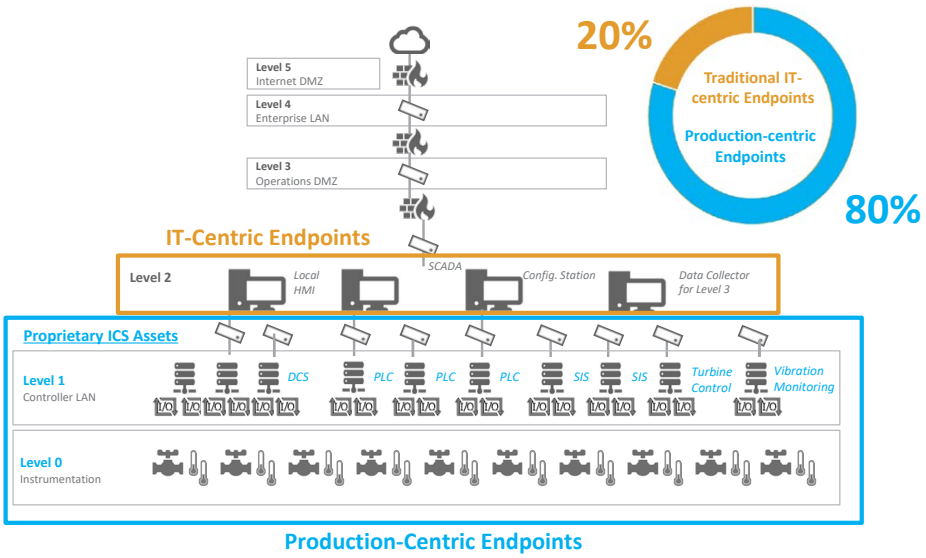
Many of these vulnerabilities have likely been lurking for years, only coming to light now due to an increased awareness of ICS cybersecurity risk.

Limited Visibility into ICS Vulnerabilities and Risks

Given the sophistication and effectiveness of recent industrial compromises, identifying and remediating known vulnerabilities is one of the best ways to reduce risks to the critical infrastructure. However, despite the existence of known vulnerabilities within systems that exist on PCNs, industrial companies today still struggle to identify ICS vulnerabilities and risks in a timely manner.

When it comes to securing OT assets, most approaches have been IT-centric. This has led to limited success with focus on securing Level 2 endpoints, such as workstations. This approach has also worked for securing routers and switches on the PCN, as these types of devices can avail themselves of the same types of security controls implemented on corporate IT networks. However, these Level 2 endpoints make up only 20 percent of industrial endpoints.

The remaining 80 percent of industrial endpoints are Level 1 and 0 production-centric endpoints including Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), and turbine controls. They also include smart field instrumentation and the sensors that directly connect to process equipment.



Level 1 and 0 assets are invisible to most cybersecurity professionals, as most of the tools used for vulnerability assessment today were not built to support the proprietary architectures and protocols used by ICS endpoints in multi-vendor process control environments. Because Level 1 and 0 assets are invisible or opaque, and because vulnerabilities on Level 2 endpoints are more readily understood and accessible, organizations focus on Level 2 vulnerability management.

However, 80 percent of endpoints in industrial environments are Level 1 and 0 endpoints. These are the endpoints that matter most in industrial environments.

At the end of the day, most organizations do not have a clear view into all the different endpoints running in their facilities. When automation system vendors publish vulnerability bulletins, managers do not easily know which systems and versions they have. And even when they do know that they have a system with a known vulnerability running, they typically cannot quickly tell if the vulnerability still exists, or if it has been remediated. This means they do not know with any degree of confidence whether the endpoint is secure, or if it is vulnerable to exploitation.

OT cybersecurity professionals must do a better job of gathering and maintaining an evergreen inventory of all the assets in the facility and assessing these assets against known vulnerabilities. You simply cannot secure what you cannot see.

Vulnerability Investigation Is Manual and Research-Intensive

Compiling the vulnerability management data needed to remediate vulnerabilities effectively in industrial facilities today is a manual and extremely research-intensive process.

OT cybersecurity professionals must monitor many different vulnerability sources, including (but not limited to) the NVD data feed, ICS-CERT alerts and advisories, Microsoft® security advisories, and automation vendor security bulletins – all of which contain information about vulnerabilities that can pose risk to industrial facilities.

When a new ICS-CERT advisory or automation vendor bulletin is published, OT cybersecurity professionals send enterprise-wide emails asking asset owners to determine if systems running in multiple facilities across the enterprise are vulnerable, and if so, to send back their remediation plans and timelines.

Asset owners within each site must sift through spreadsheets and data collected in many different siloed proprietary automation vendor products to find answers. Figuring out what needs to be done to address a vulnerability and what the consequences of vulnerability remediation will be on production requires painful research. In most facilities, there are simply not enough staff in place to stay current with the rapidly evolving OT threat landscape. Many asset owners in facilities lack sufficient cybersecurity knowledge and expertise. Timely, accurate responses from busy asset owners are difficult.

OT cybersecurity professionals must have a more automated, efficient way to assess their production-centric endpoints against the latest vulnerability advisories from Microsoft, ICS-CERT, and the automation vendors. When new vulnerabilities are published, staff need to know applicability immediately – not weeks, months, or years later. They need to understand the risk level a specific vulnerability presents, and what remediation actions they need to take to prevent a threat actor from exploiting vulnerabilities and negatively impacting production or safety.

Limited Visibility into Vulnerability Remediation Effectiveness

Obtaining timely, accurate information on the state of vulnerability remediation activities is difficult in most industrial environments. There are a variety of different automation system brands and models running in an industrial facility – many times 30 or more. Vulnerability remediation tracking and reporting processes still rely on spreadsheets of manually entered information. Such data are error-prone and quickly out of date. And even when accurate, vulnerability management workflows cannot be triggered from data stored in emails and spreadsheets. The state of vulnerability management today means the following is difficult:

- Creating an enterprise-wide view of OT vulnerabilities and remediation states
- Determining if a vulnerability has been remediated or mitigated by a compensating control
- Determining how long vulnerability remediation activities take to complete

- Identifying which facilities are proactively meeting corporate policies regarding vulnerability remediation on critical assets, and which facilities are less proactive or need additional assistance with vulnerability remediation activities

OT cybersecurity professionals must have a better way to manage vulnerability remediation activities and obtain visibility into vulnerability remediation states. Without a continuous view into vulnerability remediation activities and states, OT cybersecurity professionals run the risk of assuming their facilities are more secure than they are in reality.

Manual, Inconsistent Patch Management

Many organizations have well-established patch and vulnerability management capabilities for their IT-centric endpoints. However, far too many organizations still struggle to assess, implement, and validate patches. This puts ICS assets at risk.

Consistent, systematic patch management is an essential requirement for a secure facility. It reduces the attack surface, improves the overall security of OT systems, and reduces vulnerability risk. However, according to the SANS Securing Industrial Control Systems, 2017 report, patching is a problem in most industrial environments. Only 46 percent of respondents regularly apply vendor-validated patches.

Patch management is a significant challenge, and a major burden, for staff. OT systems are highly proprietary, complex systems, implemented with very specific hardware configurations and operating system versions. Due to precise configuration specifications for automation systems, software or configuration changes can cause systems to malfunction and negatively impact process reliability and safety. Patches for OT systems must be thoroughly tested by both the vendor of the industrial control system and asset owners or automation engineers prior to implementation. Due to concerns over uptime requirements, asset owners must plan and schedule ICS updates months in advance. Revalidation may also be required as part of the update process.

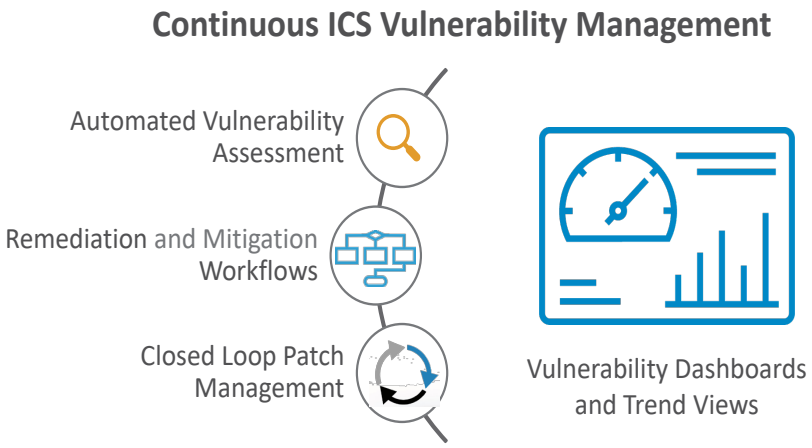
The SANS Securing Industrial Control Systems, 2017 report strongly recommends "establishing a fully-staffed, closed-loop program to manage testing and implementation of patches." Implementing a closed-loop patch management process provides the following benefits:

- Improves operational efficiency by coordinating disparate patch management ownership functions between IT and OT
- Improves visibility into the current state of patch management activities across assets, facilities, and the business unit
- Reduces risk by better protecting the organization from headline-grabbing safety incidents and production outages

Solution: Continuous ICS Vulnerability Management

Obtaining a complete view of the vulnerabilities that reside across the myriad of proprietary automation vendor systems is daunting. However, failure to manage OT vulnerabilities effectively leaves industrial endpoints exposed, and can negatively impact production, safety, reliability, and profitability.

PAS has used its more than two decades of expertise in the power and process industries, in combination with its long history of automation vendor platform independence, to deliver continuous ICS cybersecurity vulnerability management for Level 2, 1, and 0 industrial systems. PAS Cyber Integrity™ provides comprehensive ICS vulnerability management for complex, multi-vendor industrial power and process environments. Only Cyber Integrity gives the centralized ICS vulnerability insight from a sole source of truth that OT cybersecurity professionals need to protect critical industrial infrastructure effectively.



Automated Vulnerability Assessment

Cyber Integrity automates vulnerability assessment and identifies which ICS assets may have vulnerabilities that put production systems at risk. Cybersecurity teams can see all vulnerabilities across the entire enterprise, or filter to display vulnerabilities by facility, unit, area/zone, or individual asset. Results include the NVD Common Vulnerability Scoring System (CVSS) risk rating for each vulnerability.

Cyber Integrity also provides on-demand vulnerability assessment queries that run against the Cyber Integrity inventory of managed assets for quick assessment of control system vulnerabilities and cyber risk exposure. Results from on-demand queries can be imported into other automation system vendor management consoles that integrate with Cyber Integrity.

Remediation and Mitigation Workflows

A systematic approach to vulnerability mitigation or remediation enables improvements to overall OT security in industrial facilities in a cost-effective way. Industrial facilities that follow good vulnerability management practices prevent incidents by reducing the risk of OT vulnerability exploitation. Reducing the attack surface not only reduces the risk of an unplanned outage, it also better protects the organization from headline grabbing safety incidents and production outages.

Vulnerability remediation workflows in Cyber Integrity give a continuous view into the state of vulnerabilities in the OT environment by enabling documentation, inventory-matching, and reporting on existing vulnerabilities, as well as visibility into the risk associated with the vulnerability and the current state of vulnerability remediation. Workflows are highly customizable to meet the unique needs of an organization. For example, personnel can define vulnerability remediation workflows for mitigating a specific vulnerability across a group of assets, or to mitigate multiple vulnerabilities across a single asset or group of assets. Personnel can also define workflows for remediating vulnerabilities via patching or other methods, such as implementing a compensating control or performing a system upgrade.

Closed-Loop Patch Management

Organizations that implement Microsoft software patches on a prompt basis reduce the risk of OT vulnerability exploitation. Cyber Integrity patch assessment capabilities give a centralized, unified view into current Microsoft patch currency across all managed cyber assets. Cyber Integrity provides highly customizable patch management workflows designed to document and ensure that all proper steps are followed during the various stages of the patching process, including appropriate patch evaluation, testing, implementation, and verification. Summary views show which systems have patches applied, as well as which systems still need patching.

Vulnerability Dashboards and Trend Views

Customizable vulnerability management dashboards within Cyber Integrity give asset owners, facility staff, OT and IT cybersecurity professionals, and the executive leadership team visibility into the data they need to make informed vulnerability remediation and cyber risk management decisions. Vulnerability trend views display trends over time and can help answer the following types of questions:

- How many critical vulnerabilities have been identified this year compared to the number of vulnerabilities identified during the same period last year?
- How long does it take each facility or unit to mitigate or remediate critical vulnerabilities and reduce risk?
- Which facilities are consistently meeting mandates to address ICS vulnerabilities over time, and which are not meeting mandates?
- Am I compliant with vulnerability management standards?

Summary

There is no question that safety, reliability, and profitability within critical infrastructure facilities face a growing, worldwide threat from cyber attacks. Outlaws are bent on cutting companies' cyber versions of the "Devil's Rope." Unfortunately, many ICS asset owners lack an accurate understanding of their true risk – particularly from industrial control system vulnerabilities.

Exploitation of vulnerabilities in industrial networks can lead to significant consequences. Level 1 and 0 ICS vulnerabilities exist in organizations today, but they are difficult to identify and remediate using current methods. This leads organizations to focus on Level 2 vulnerabilities instead. However, Level 1 and 0 vulnerabilities are what matter most in industrial environments as they have the greatest influence on production and safety. Automating discovery and elimination of these vulnerabilities should be a top priority for ICS cybersecurity teams and one of the best defenses in a fence cutter war with no end in sight.

Additional Resources

For more resources and information on how PAS can help you manage and protect your industrial control systems, visit cyber.pas.com.

About the Authors

David Zahn

Chief Marketing Officer and 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 B.A. in Economics and Managerial Sutides from Rice University as well as an MBA from the McCombs School of Business.

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. Prior to PAS, under his leadership, NetIQ entered the SIEM market culminating in a Garner 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 a B.S. (cum laude) in Computer Science from Virginia Tech, and a B.B.A. from the University of Houston.

About PAS

PAS is the leading provider of software solutions for ICS cybersecurity, process safety, and asset reliability to the energy, process, and power industries worldwide. PAS solutions include industrial control system cybersecurity, automation asset management, IPL assurance, alarm management, high performance HMI™, boundary management, and control loop performance optimization. PAS solutions are installed in over 1,100 facilities worldwide in more than 70 countries. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.