AUTOMATION 2022

VOLUME 4

Cybersecurity & Connectivity

- Seven-Step OT Risk Assessment
- Reducing OT/ICS Cybersecurity Risk
- Mitigate Network Vulnerabilities
- The Good, the Bad, and the Ugly of OT Security
- Recovery Starts with Better Change Management
- Top 25 ICS Vulnerabilities

AUTOMATION.COM | ISA A subsidiary of the International Society of Automation

Introduction

AUTOMATION 2022 VOL 4

Automation 2022: Cybersecurity & Connectivity

As businesses travel their respective journeys toward digital transformation, they realize every day that securing their industrial control system (ICS) networks can be formidable. Operational technology (OT) systems continue to evolve rapidly. While modern OT and information technology (IT) systems and Industrial Internet of Things (IIoT) devices bring huge benefits to critical infrastructure and industrial organizations, they also bring new cybersecurity challenges.

Everything comes with risks. Cybersecurity attacks, vulnerability exploits, and digital espionage have crossed the boundaries into what were once considered off-limit targets. Our job as automation professionals is to recognize those risks and counter them head on.

This edition of AUTOMATION 2022: Cybersecurity & Connectivity shows you strategies and solutions for securing OT/ICS infrastructure. Discover the top 25 ICS vulnerabilities and how to counteract them, how to mitigate industrial network vulnerabilities, best practices for cybersecurity risk reduction, risk assessment strategies, and advice on how to build an appropriate cybersecurity plan.

Jack Smith, Contributing Editor

SPONSORS

About AUTOMATION 2022

The AUTOMATION 2022 ebook series covers Industry 4.0, smart manufacturing, IIoT, cybersecurity, connectivity, machine and process control and more for industrial automation, process control and instrumentation professionals. To subscribe to ebooks and newsletters, visit: www.automation.com/newslettersubscription.

AUTOMATION 2022 is published six times per year (February, April, June, August, October, December) by Automation.com, a subsidiary of ISA—the International Society of Automation. To advertise, visit: www.automation.com/en-us/advertise.

AUTOMATION.COM
groups/68581
automationdotcom
automation_com

International Society of Automation
Setting the Standard for Automation™
company/internationalsocietyofautomation
InternationalSocietyOfAutomation
ISA_Interchange

Renee Bassett, Chief Editor
rbassett@automation.com
Chris Nelson, Advertising Sales Rep
chris@automation.com
Richard T. Simpson, Advertising Sales Rep
rsimpson@automation.com
Gina DiFrancesco, Advertising Sales Rep
GDiFrancesco@automation.com

Table of Contents

AUTOMATION 2022 VOL 4
CYBERSECURITY & CONNECTIVITY

txOne networks

Keep the Operation Running

Purpose-built for OT Digital Safety

OT DEFENSES THAT SAFEGUARD OPERATIONS FROM KNOWN AND UNKNOWN THREATS

Industrial control systems (ICS) are intricate ecosystems where legacy and state-of-the-art devices work together to keep highly automated production processes in motion. But, this complex infrastructure is easily exploited. ICS vulnerabilities are being targeted in greater numbers, and cyber attacks spread fast - disrupting production, damaging assets, and putting lives at risk.

TXOne provides OT-focused cybersecurity solutions to protect both legacy and modern assets without the latency that interrupts productivity.

www.txone.com

Learn More >

Discover TXOne Networks' framework for OT digital safety with your free copy of The OT Zero Trust Handbook.

Use the Seven-Step OT Risk Assessment

Determine your level of cyber risk and knock out the threats with an OT Zero Trust approach.

By Austen Byers, TXOne Networks

A system controlling the fabrication of integrated circuits stopped abruptly during routine operations, destroying wafers worth $50,000. Another robot randomly swung its heavy metal arm around 180 degrees into an employee walkway. These were only accidents—imagine what a bad actor can orchestrate. To accurately decide which cyber defenses you need for optimum protection, it's important to first take a look at your risk within operational technology (OT) environments. Which devices are most vulnerable? What are the attack surfaces?

Gartner recently punctuated the wake-up call that connecting assets to the internet also opens the door to ransomware, trojans, worms, and other nasty malware assaults. In the Market Guide for Operational Technology Security, Gartner identified the "Oh Wow!" moment—a polite term for the instant one realizes that failing to invest in modern

cybersecurity is creating a self-inflicted threat. The moment a ransom demand arrives, it is already too late. What will be attacked next?

Users have a choice. Forego this scenario and combat the hacks by evaluating threats using this seven-step OT zero trust risk assessment toolkit.

Step 1: Take an inventory of OT assets

It seems simple, but without a comprehensive understanding of your machines, how do you know what's at risk and needs protection (figure 1)? Consider using tools that help streamline this process, such as portable security devices or endpoint applications that automatically inspect and inventory all types of OT devices from legacy, to modern, to air gapped.

Step 2: Evaluate OT security needs and tolerance

Remember that lessons learned from information technology (IT) may not apply to OT. IT cybersecurity assessments revolve around the CIA triad: confidentiality, integrity, and availability. Because IT systems are often used for company information, the highest priority is confidentiality. The opposite is needed for OT (table 1). Machines work all day, every day, 24 hours per day. Productivity is key. Safety is critical. Availability is the priority.

IT	Priority	OT
Confidentiality	1	Availability
Integrity	2	Integrity
Availability	3	Confidentiality

Table 1. CIA triad priorities for IT vs. AIC priorities for OT.

Detectability is also important. If you don't know that a threat exists, then you cannot respond. The environment also plays an important role. Inclement weather, hazardous materials, and rugged environments are realities that may not affect IT systems.

Users also must consider the criticality of an asset and the potential harm if misused. For example, what is the likelihood a controller could activate a robot arm to swing around 180 degrees? Would workers be

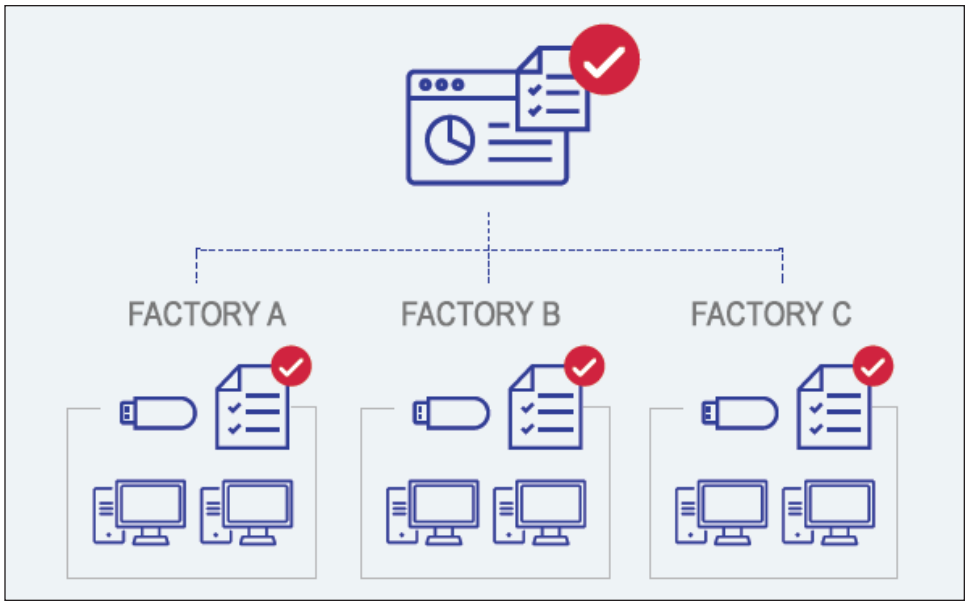


Figure 1. Portable security devices and endpoint applications can help inspect and inventory OT assets.

hurt? Would facilities or equipment be damaged? If a machine's output is altered in the slightest, would that be detrimental to quality?

Step 3: Assess threats

Hackers are constantly researching targets, developing or downloading hacking tools, looking for security holes, and attacking. Malware travels through networks disguised as regular traffic. Personnel walking onsite often carry hidden cyber threats within their laptops and USB drives. Each type of attack has a different threat level, and attackers often mix and match attacks.

"The goal of a risk assessment is to understand and quantify threats so you can prioritize and deploy your cyber defenses where and when they are needed."

Threat actors range from so-called "script kiddie" amateurs to state-employed professional hackers. Most corporate threats begin with threat actors dedicated to the field of cybercrime or cyber espionage who would like to use ransomware to extract payments. Professional threat actors work collaboratively as advanced persistent threat (APT) groups, which are the professionals of the cybercrime industry.[1]

Researchers ranked the most common types of cyber-attacks unique to an industrial control system (ICS) (table 2).

Cyber-attack	Description
Denial of control	Control systems are disrupted by delaying or blocking the flow of data, creating bottlenecks.
Control devices reprogrammed	Unauthorized changes to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers that change alarm thresholds, change equipment behavior, or prematurely shut down systems. Any of these could cause spills, fires, equipment damage, or other harm to workers and the environment.
Spoofed system status information	False data sent to control system operators could disguise attacks.
Control logic manipulation	Untested changes to software or configuration settings could produce unpredictable results.
Safety systems modified	Safety systems could be turned off or programmed to take incorrect actions that damage or destroy systems and threaten workers or the environment.
Malware injected into control systems	Viruses, trojans, worms, or other malware can disrupt production and may destroy equipment.
Copied from *Table C-8 in NIST Special Publication 800-82 Revision 2*.	

Table 2. Ranking of the most common types of cyber-attacks unique to ICS.

These attack vectors often involve expert knowledge of systems, and expert hackers even develop apps so that others can attack without understanding all the technical details.

Step 4: Analyze risks

Operational technology functions in the physical world. The key difference between OT and IT cyber-attacks are the safety consequences:

- Safety of your team and your community
- Safety of your property
- Environmental safety

When evaluating risks, consider what damage could occur if your sensors or actuators are hijacked (figure 2). Think about what happens when an attack propagates through connected systems. If your digital controllers stop functioning, what happens to your non-digital assets? When setting risk thresholds, safety considerations are critical.

OT zero trust risk analysis allows users to identify the most important risks so they can focus their budget and their team on responding to the most critical threats first. When a threat is identified, consider these questions:

- Which systems are vulnerable to the threat?
- What is the harm; i.e., can this threat attack my command controllers or other digital equipment?
- What are the physical ramifications of the threat?
- What if the threat cascades locally or beyond?

While investigating whether a threat should be added to your risk assessment, consider using the MITRE ATT&CK matrix to understand the details of the threat. This is a curated knowledge base for cyber threats against OT, whereby researchers have investigated common attack strategies for assets and systems that are routinely targeted.

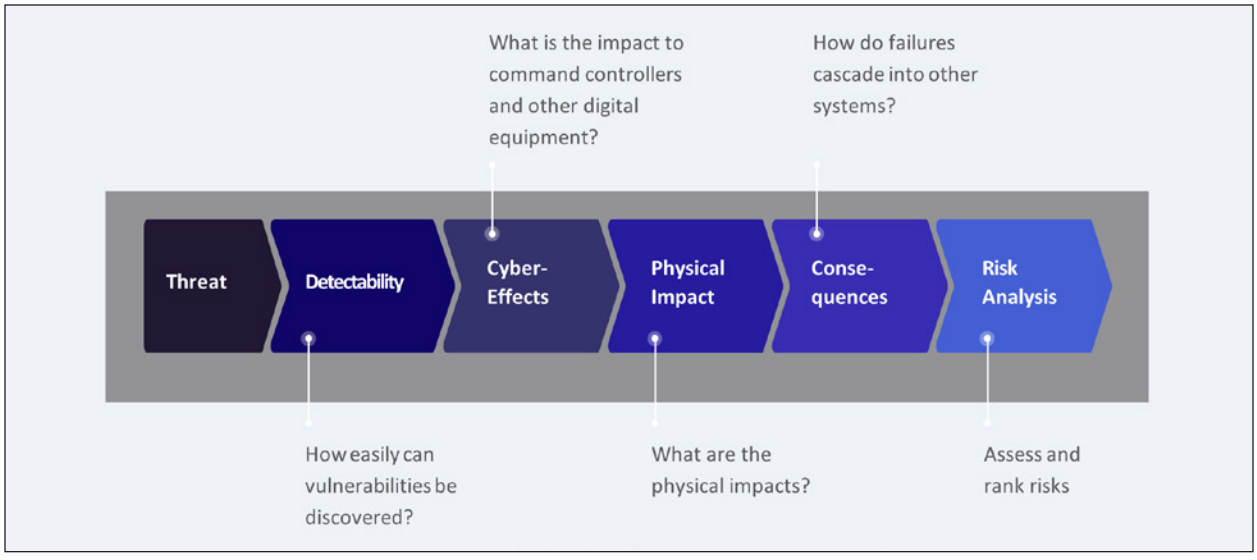


Figure 2. When evaluating risks, consider the damage that could occur and the impact on safety.

Take a deep dive into the technical process for assessing and managing cyber-risks when using OT zero trust. First, time is valuable. Rank cyber threats based on what is most critical so you can spend your time efficiently.

Step 5: Prioritize risks

The goal of a risk assessment is to understand and quantify threats so you can prioritize and deploy your cyber defenses where and when they are needed. You can use this to evaluate protections for safeguarding a single asset or your entire factory floor. We suggest adding risk scenarios to the threat assessment from Step 3 and the risk analysis from Step 4 to help with this.

To systematically rank and prioritize, assign a value to each risk vector. We use a 0 to 10 scale, but choose the quantification scheme that best reflects your situation and risk tolerance:

- Vulnerability severity: On a scale of 0 to 10, if this threat occurred, how severe would the damage be?
- Asset criticality: On a scale of 0 to 10, how important is this asset?
- Likelihood: On a scale of 0 to 10, how likely could the threat occur in your facility?
- Impact: On a scale of 0 to 10, what is the impact on productivity?
- Detectability: On a scale of 10 to 0, how will you know that you are under attack?

Compared to other scores, detectability scores are reversed. A low detection score is 10, meaning that you are more vulnerable because you cannot defend against what you don't know about.

To calculate the risk ranking, or risk priority, put the numbers from each risk vector into the following formula:

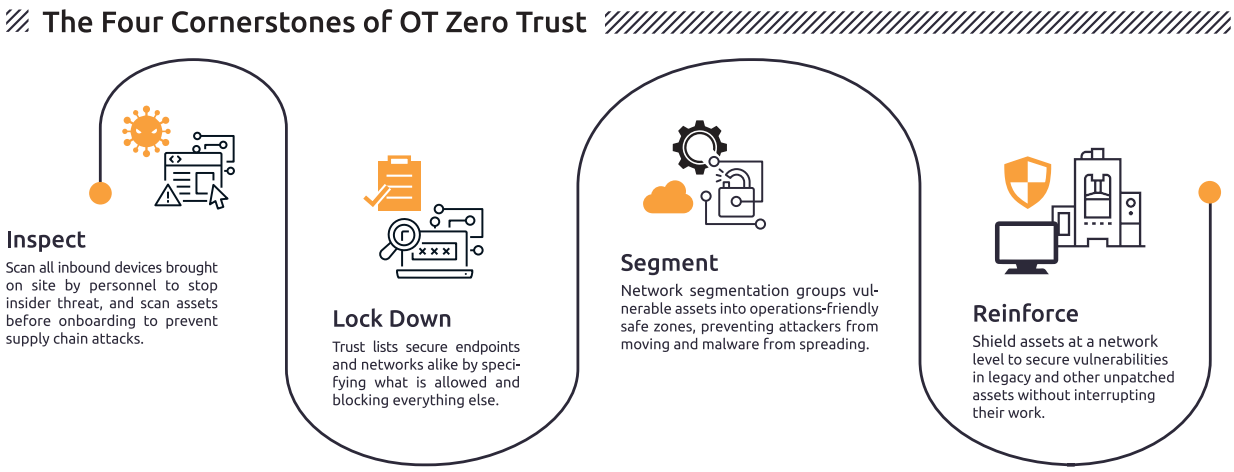
Priority = [severity + (criticality x 2) + (likelihood x 2) + (impact x 2) + (detectability x 2)] / 5

High-priority risks will be those with a risk ranking of 18 to 12. Medium risks are ranked from 12 to 6, and low risks have priority rankings under 6.

To quickly see which cyber defenses you need, sort by risk priority. You may even want to color-code your risk assessment (table 3). In this example, Risk 1. Denial of control has the highest priority. The vulnerability is severe, and the asset is critical. The likelihood this may occur is medium, but if it does, the impact is high. It might or might not be easy to detect. Red color coding is used to show high severity.

Risk assessment/cyber defense selection		
	Risk 1. Denial of control: Control systems are disrupted by delaying the flow of data and creating bottlenecks.	**Risk 2. Malware injected into control systems:** Viruses, trojans, worms, or other malware can disrupt production and might destroy equipment.
Vulnerability severity (Low 0; high 10)	10	1
Asset criticality (Low 0; high 10)	10	5
Likelihood (Low 0; high 10)	5	1
Impact (Low 0; high 10)	10	10
Detectability (Low 10; high 0)	5	5
Risk priority	14	8.6
Risk mitigation or response		
	Mitigation 1. Use a defense console to monitor status from all assets and report incidents.	**Mitigation 1.** Inspect devices to scan and destroy malware on modern endpoints and legacy or air-gapped devices.
	Mitigation 2. Segment the network so you can quarantine infected machines.	**Mitigation 2.** Reinforce protections with virtual patching.

Table 3. Prioritizing risk vectors.



Step 6: Monitor risks

Now that you have a good understanding of your risk priorities and what needs to be protected, you can find the solutions that best serve your needs to monitor and protect your OT network.

The four cornerstones of OT zero trust support continuous monitoring of your systems. We recommend ensuring that your OT strategy and tools cover each of the following cornerstones:

Inspect assets, take inventory, and destroy supply chain malware using portable security devices. These devices do not interrupt production so you can scan legacy and air-gapped assets, as well as perform routine or surprise inspections.

Lockdown assets by determining your trust policies so OT zero trust can enforce them. Your assets are armed with monitors that discern the situation and take the best course of action depending on what's happening at any given time.

Segment your network into zero-trust zones and only allow trusted messages from trusted devices to enter a zone. Once inside, only trustworthy messages can be sent outside.

Reinforce cybersecurity by using endpoint protection with machine-learning threat intelligence and virtual patching to reduce risks. Continually monitor your systems, assess threats, and activate your risk responses if needed. It is helpful to have all security devices report in real time to one cybersecurity defense console.

Step 7: Response to cyber incidents

Risk thresholds are unique to every company. For each risk you identify, you decide what response meets your comfort level. Risk responses are generally grouped into these categories:

- avoiding
- transferring
- sharing
- mitigating
- accepting the risk

The most important feature of any risk response is the ability of your system or your team to execute the response and stop the attack. OT zero trust locks down assets and monitors network traffic using trust lists that stop most attacks before they start.

ARM your organization with OT zero trust

While there is no guarantee of a risk-free world, this seven-step OT risk assessment is based on years of experience by industry leaders who have documented their findings in NIST and other standards, along with researchers who are solely dedicated to finding better ways to protect your operational technology.

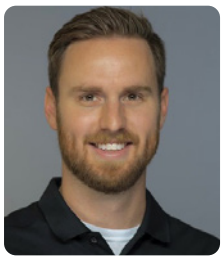
To quickly review the seven steps:

1. **Take inventory of your assets:** OT zero trust-based portable security devices automatically inventory every asset during an inspection, making it easy to confirm the defensive status of stand-alone assets, newly arrived onboarding assets, and any devices brought onto the work site.
2. **Develop a security plan to protect your assets:** Understand the needs and priorities of your OT environment and your unique tolerance for the unexpected to inform your cybersecurity plan.

3. **Assess threats:** OT zero trust-based threat intelligence is always working for you, finding new trends that detect and prevent malware from lurking in the shadows of your systems and network.
4. **Analyze risks to understand what is at stake:** OT zero trust matches up protections with your assets to put dependable, easily maintained defenses in place before your network gets hit and your assets are in danger.
5. **Prioritize risks:** Quantifying risks gives you a powerful weapon to prioritize and justify your budget for cyber defenses.
6. **Monitor risks:** OT zero trust is a valued technology partner following your lead using your criteria to carry out the critical mission of tackling the 24x7x365 challenge of safeguarding your systems.
7. **Respond to cyber incidents:** Forego the "Oh Wow!" chaos and prepare your team and your cyber defenses to respond with an OT zero trust methodology.

Using OT zero trust, ARM yourself with a tried-and-true process that is summarized in the NIST Guide to Industrial Control Systems (ICS) Security: continually **A**ssess risks, **R**espond to threats, and **M**onitor vulnerabilities.[2]

ABOUT THE AUTHOR



Austen Byers is technical director at TXOne Networks. He leads the company's efforts in providing design, architecture, engineering technical direction, and leadership. Byers is a sought-after thought leader in operational technology (OT) digital safety with more than 10 years in the cybersecurity space. He has spoken at numerous industry events as a subject-matter expert to provide insight into the state of industrial cybersecurity and the intricacies of OT breaches, and to provide strategies to help organizations keep their assets and environments safe.

Sources:

1. David P. Duggan, Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard, Categorizing Threat: Building and Using a Generic Threat Matrix (Albuquerque, New Mexico: Sandia National Laboratories Report: SAND2007-5791, 2007), 13.

2. Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams), Adam Hahn, SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security, (Gaithersburg, Maryland: U.S. Department of Commerce, 2015).

HEXAGON

Safeguard the industrial endpoints that matter most

PAS Cyber Integrity® is a powerful and scalable OT/ICS risk and endpoint management solution that provides the critical data and insight needed to make your industrial operations safer and more resilient.

Learn more »

Five Best Practices to Reduce OT/ICS Cybersecurity Risk

Consider these cybersecurity best practices to help users achieve an acceptable risk level for their facilities

By Chad Elmendorf, PAS Cybersecurity, Hexagon Asset Lifecycle Intelligence

Industrial control systems (ICSs) ingest and automate thousands of variables to control dangerous processes that commonly use high temperatures and volatile raw materials to produce the final output. The safety and reliability of these systems is paramount to meeting the industrial facility's health, safety, and environment (HSE) objectives, efficient production, and no unscheduled outages. These systems were never designed to be cyber-secure and for decades were considered air-gapped and unable to be reached by cyber attackers.

The evolution of OT/ICS risk

That is no longer the reality. With the adoption of digital transformation technologies to increase efficiency and lower costs, industrial facilities, which most often operate in these sectors, are now connected cyber/physical systems. Asset owner/operators are therefore operating a "connected plant" and have found that their critical systems are vulnerable to cyber-attacks. With the continuous drip of successful attacks on critical infrastructure making headlines, risk management has become a common topic in boardrooms around the globe, resulting in greater pressure placed on security and operations teams to ensure that defenses are put in place, and should a successful attack occur, consequences will be minimized to an acceptable risk level.

1 Best practice 1: See it, manage it

The foundation to any operational technology (OT)/ICS cybersecurity program is a full, in-depth asset inventory, which must include all the details of what systems and endpoints are running in the industrial environment. You must be able to "see it" before it can be protected. As unique as control logic is across various sites, asset inventory also comes in many different shapes and sizes.

> **"You may never experience an attack**, but to reduce risk, you must have a cybersecurity program that is built on the assumption that you will."

To effectively use asset inventory information throughout a cybersecurity program, knowing that a distributed control system (DCS) is communicating with a programmable logic controller (PLC) or a server is talking to a switch is not adequate to reducing risk. That level of detail is easily achieved by monitoring and analyzing the network traffic to build an inventory. This method provides a detection benefit but is also limited in that it can only provide asset inventory information down to Level 2 of the Purdue Model and therefore does not achieve a full inventory, as it cannot detect endpoints at Level 1 and Level 0, in addition to "islanded" assets that are operating in a closed, or "air-gapped," network but are still susceptible to attacks from insider threats.

What does an in-depth asset inventory look like (figure 1)? The technology must be able to provide detailed asset information,

including the manufacturer, model, version, and serial number for every piece of hardware, firmware, and software, whether connected to the network or not, across the industrial control system environment. To reduce cybersecurity risk in an ICS environment, asset inventory information must encompass every DCS and controller, input/output (I/O) cards, communication modules, and the version of the firmware loaded into each of these devices, as well as the same level of detail for PLCs, safety instrumented systems (SIS), and human-machine interfaces (HMIs), etc. The only method to achieve this level of visibility is to collect and analyze the native control system configuration files, which will enable you to confidently answer the important questions that are common in vulnerability management, asset lifecycle management, and asset migration planning, including:

- "Do I have that asset?"
- "How many are in the ICS environment?
- "Where are they?"

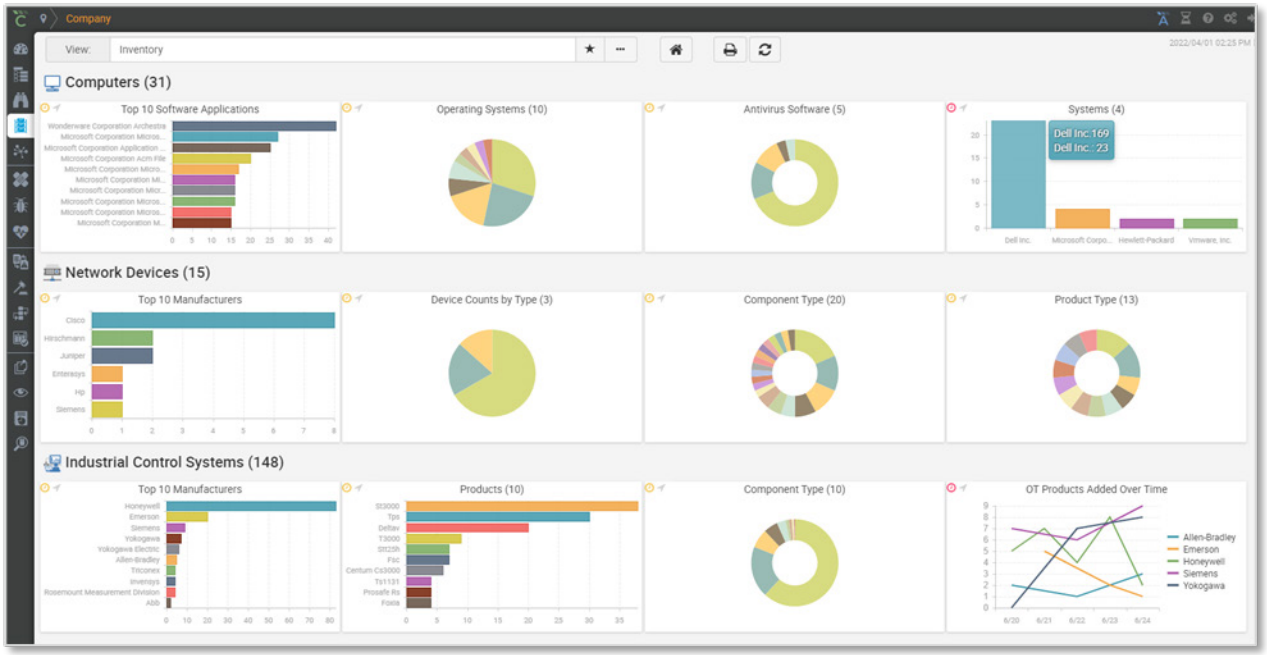


Figure 1. Summary view of inventory in a typical industrial control system.

In Hexagon's experience, working with customers around the globe, we have typically seen far more than 100 components per DCS, more than 45 for an SIS, and more than 40 for PLCs. In addition, for each computer, engineering workstation, operator station, etc., there may be considerably more than 450 inventory items. For refineries specifically, it's common to identify more than 6,000 inventory endpoints that must be managed and protected from cyber threats.

2 Best practice 2: Ensure configuration data integrity

Obtaining a comprehensive asset inventory is Step 1, but unplanned downtime can still occur. Using configuration analysis is a method to lowering risk and improving business resiliency with a proven track record of preventing and shortening unplanned downtime. Each industrial environment is unique. There are certain types of changes that may occur in the configuration files that can indicate a high probability of an imminent threat. To gain visibility into these indicators, software is available that automates the process of comparing configuration files and alerting on any changes that might impact safety and/or security of operating environments. This method provides the visibility to substantially reduce the consequences of a cyber or operational incident, and therefore the overall cybersecurity and safety risk in an industrial facility.

To ensure configuration data integrity, a baseline—or snapshot of the configuration as it stands today—of the "known-good" configuration of all assets must be generated and continually monitored for any deviations on a time-based cadence. A good configuration baseline tool allows ICS engineers to define different property values across asset types, asset criticalities, or different parties that are responsible for the asset operation. The configuration management tool can alert the relevant parties based on the type of deviation so that the mean time to respond is decreased. For example, the security system must be notified if certain registry settings are changed in a control system server, as it could indicate unauthorized credential access has been gained and settings within the control

system could be manipulated. Another example where ICS engineers need to be notified for immediate response is if suddenly the firmware version of several PLC cards changes.

A solid configuration management process must include an automated collection and comparison of asset configuration information to defined baselines. Simple file comparisons or notification of a download event isn't adequate for defining baselines because a single configuration file may contain normal operational values as well as security or system reliability information. One would expect that the process operation values will change on a regular basis, so alerting on those doesn't make sense. In addition, the responsible parties are likely different for a security change event compared to a system reliability event. So, the solution needs to understand exactly what changed in the file to alert the appropriate parties about acting. No action is required if these types of deviations aren't detected. However, if deviations are detected in the comparison, the changes must be assessed, verified, and either documented as a new baseline value or rolled back to the previous configuration.

3 Best practice 3: Evaluate risk based on the environment

Evaluating OT/ICS risk is a multidimensional challenge whereby several sources of information are needed to provide holistic context, including consideration of environmental, vulnerability, and temporal impact factors. Environmental information includes a comprehensive asset inventory and topology maps (figure 2) to show the entire environment and the connections between assets. Once a full view is achieved, assets can then be logically grouped to evaluate if a particular known vulnerability affects other assets in the environment. Logical grouping of assets further builds on the initial visibility needed to more effectively secure high-risk assets.

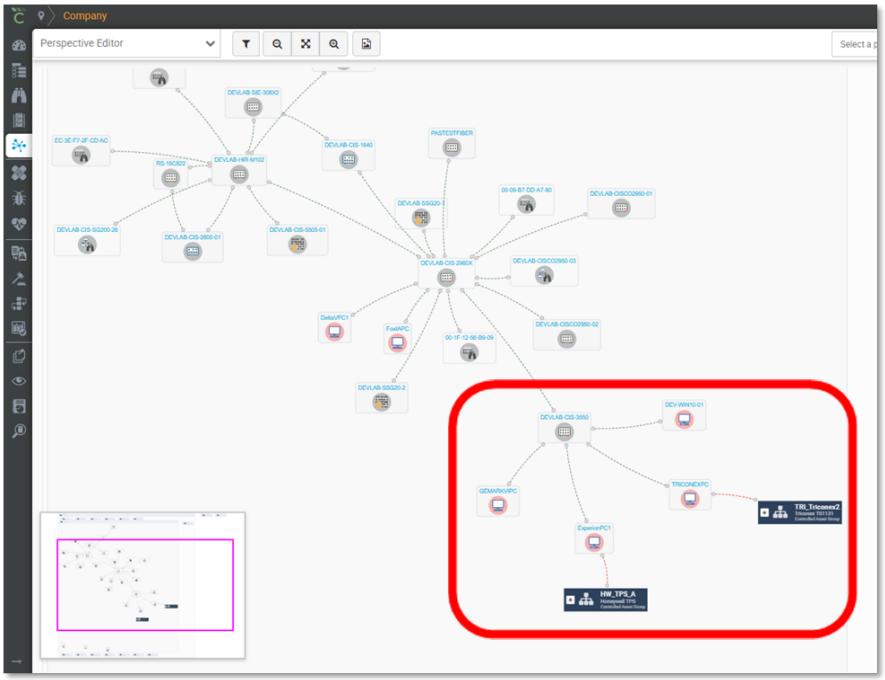


Figure 2. Topology map with various groupings.

Next, it is important to see the attack surface (figure 3) and know the vulnerabilities that exist within the asset inventory. This information can come from a source such as the U.S. National Vulnerability Database, known vulnerability exploits, and independent threat analysis. It's at this point where an automated process that ingests vulnerability data and runs it against the asset inventory to determine if the vulnerability that exists in the environment makes life a lot easier and helps to determine what mitigation is appropriate.

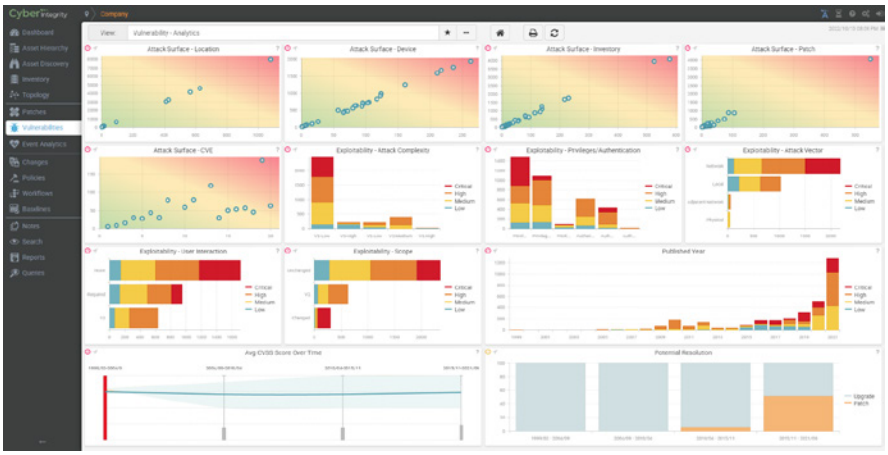


Figure 3. Example of an attack surface.

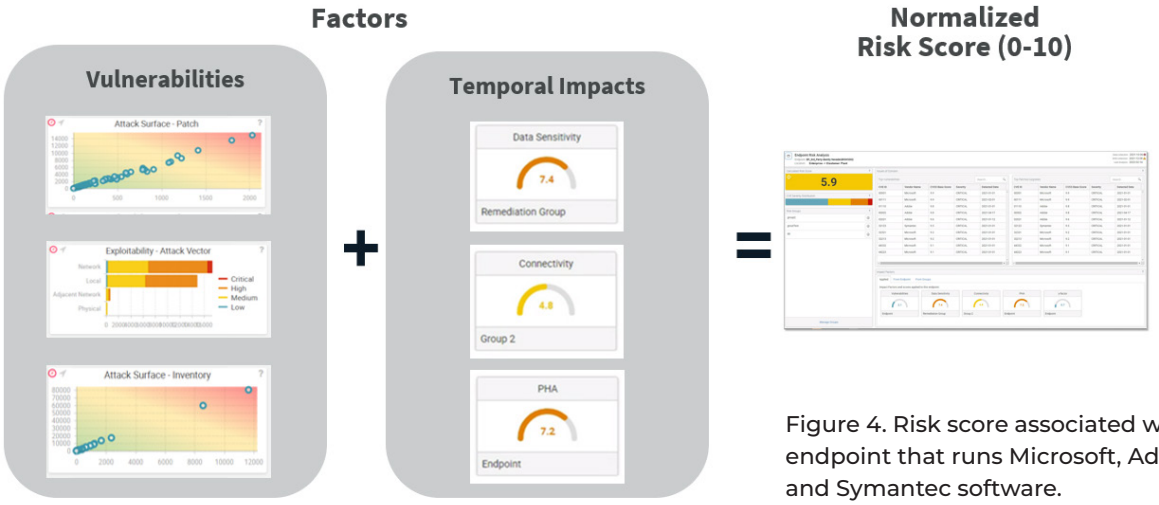


Figure 4. Risk score associated with an endpoint that runs Microsoft, Adobe, and Symantec software.

The third area of context required to evaluate and build a better risk score is incorporating temporal impact factors that are specific to a site-level OT/ICS environment or enterprise. Risk comes in many shapes and sizes, and by incorporating temporal impact scoring, users achieve a level of risk specificity that is unique to their environment. Impact factors can be sensitivity, connectivity, criticality, safety impact, and others. The key is that these are specific to your environment.

Assume a new vulnerability with a common vulnerability scoring system (CVSS) score of 8 gets published (figure 4) and you want to know what assets are affected. Incorporating temporal impact factors might change the risk score to 9 or move it down to 6.5. If it moves down, based on this increased level of context, there may be more important vulnerabilities to focus on first, or if it goes up, it may be prudent to move it to the top of the list for remediation/mitigation. The benefit is that you'll better understand which vulnerabilities are the most important and why, based on your specific environment.

4 Best practice 4: Use forensic analysis of configuration changes

There are many bad actors out there, and without spreading fear, uncertainty, and doubt (FUD), it's important to have a healthy respect for the threats that exist in our rapidly expanding connected

world. You may never experience an attack, but to reduce risk, you must have a cybersecurity program that is built on the assumption that you will. As an analogy, we may drive thousands of miles a year not thinking that we'll get into an accident, but we always, or should always, use the seatbelt just in case one occurs.

Playing this analogy out further, assume your plant has a fender-bender (i.e., incident). Knowing the severity and how it was caused allows steps to be taken so it doesn't happen again. With forensic analysis of configuration changes, you will be able to improve incident response by pinpointing the logic changes that occurred for more informed analysis. This information greatly aids incident responders in fully understanding the composition of the incident and decreasing the mean time to recover.

5 Best practice 5: Backup, backup, backup

Ransomware and other types of cyberattacks are increasingly common in OT/ICS environments, and we must assume that we'll be attacked. Again, not FUD, but healthy respect for the reality we live in. Therefore, your ability to recover from operational or cyber incidents, whether malicious or not, is critical to your business's success.

When considering your backup strategy, a "two is one, one is none" approach is recommended. A single trusted restore point or process isn't sufficient for critical OT/ICS cyber assets. If your industrial facility is attacked (or any serious event occurs that might force a shutdown, such as a catastrophic event like an earthquake or hurricane), being able to confidently restore your process back to the state that it was in before the cyber or operational incident is crucial to meet your recovery time objective, and maintain safe and profitable operations.

ABOUT THE AUTHOR

Chad Elmendorf is marketing director for Hexagon's PAS OT Integrity platform designed to secure complex, multi-vendor OT/ICS environments by reducing your attack surface, remediating vulnerabilities, strengthening cyber resiliency, and lowering enterprise risk. He holds a BS in Marketing and MBA from the University of Wyoming.

MOXA

Secure Your Network

EDS-4000/G4000 Series Industrial Ethernet Switches

Futureproof Your Network Resilience

- IEC 62443-4-2 certified for enhanced security
- Features 90 Watts PoE and 2.5 GbE connectivity
- Modular power design for easier maintenance

Get Started

Have Questions?
USA@moxa.com

How to Mitigate Three Common Industrial Network Vulnerabilities

By Felipe Sabino Costa, Moxa Technologies Inc.

Be aware of common system vulnerabilities in industrial networks that could be exploited during a cyberattack

Since industrial networks are primarily built and expanded to address growing business demands, it may be easy for administrators to overlook common system vulnerabilities. For example, when adding a device to a newly built or expanded network, do you know which industrial Ethernet switches have unlocked ports? Or do you simply connect new devices without a second thought?

Ignoring common system vulnerabilities in today's world could put your entire network at risk. The following scenarios summarize some common system vulnerabilities in industrial networks that may be exploited during the three main stages of a cyberattack: exploration, utilization, and attack. After examining the threats, tips will be provided on how to strengthen your industrial network security.

Stage 1 vulnerabilities: Exploration and infiltration

Recall the last time you logged onto your network. How complex was your password? Although weak passwords may be easier for busy administrators to remember, they are also easier for malicious actors to crack through a brute force attack. Making it easy for an attacker to guess your network login credentials is like putting the keys to your house in a location that is easy for a robber to find.

Figure 1. Ethernet switches act as gates through which information is sent and received on networks.

Attackers commonly exploit open ports on networks. For example, Ethernet switches (figure 1) act as gates through which information is sent and received on networks. If you leave the door open, intruders can walk right in. By scanning your network, hackers can identify open ports and infiltrate your network just like a burglar entering through an unlocked gate.

How to mitigate

One of the simplest ways to enhance your network security is to ensure that users create a sufficiently complex password to reduce the likelihood of an attacker guessing your credentials by brute force. For additional security, you also should consider a login failure lockout mechanism that limits the number of unsuccessful login attempts, which may indicate a brute-force attack. To protect your network from port scanning, you can create a whitelist of ports (figure 2) that are accessible through your firewall and also disable wide area network (WAN) pinging.

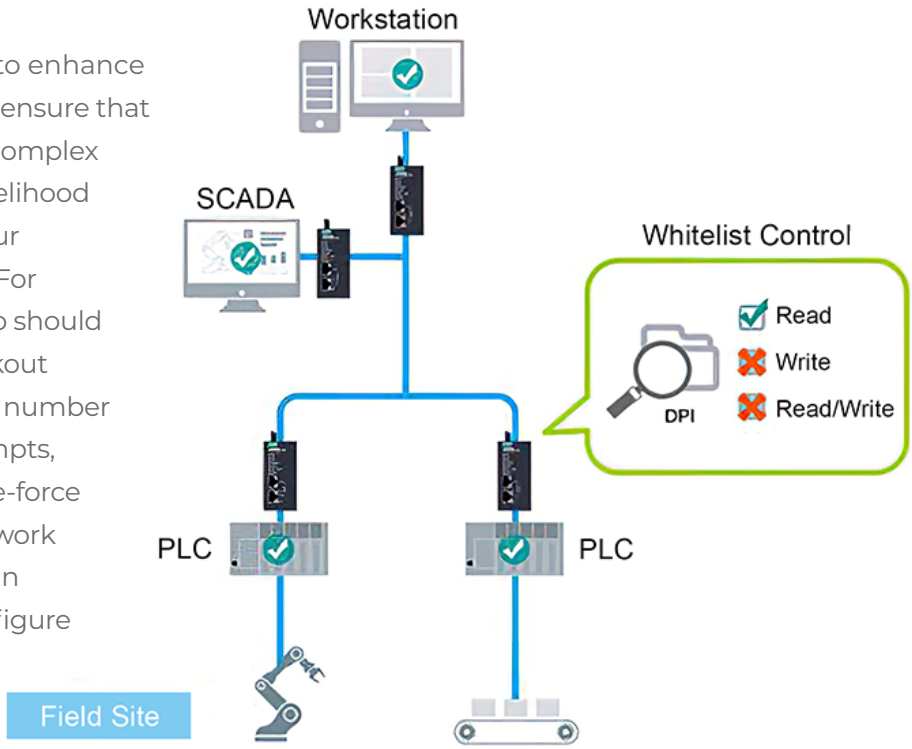


Figure 2. Deploying whitelist control powered by deep packet inspection can prevent hackers from injecting unauthorized commands.

Stage 2 vulnerabilities: Utilization and network control

During the second stage of a cyberattack, the malicious actor has already infiltrated the network and is using resources on the network for their own purposes. Even though they are not actively wreaking havoc on the network, they are secretly gathering information and laying the groundwork for a more harmful attack.

For example, a hacker may be using various scanning tools to learn about your network topology so they can find their next target and access or control more devices. The attacker can even use command injection to bypass authentication requirements or grant themselves higher levels of user privileges to execute prohibited commands and commandeer network devices for nefarious purposes.

How to mitigate

To limit the attacker's ability to move throughout your network and commandeer your devices, we recommend network segmentation (figure 3) and traffic control. For example, you should partition your network into smaller segments and control the communications that pass through these segments. In addition, deploying whitelist control to prevent command injection can also limit the severity of the security breach.

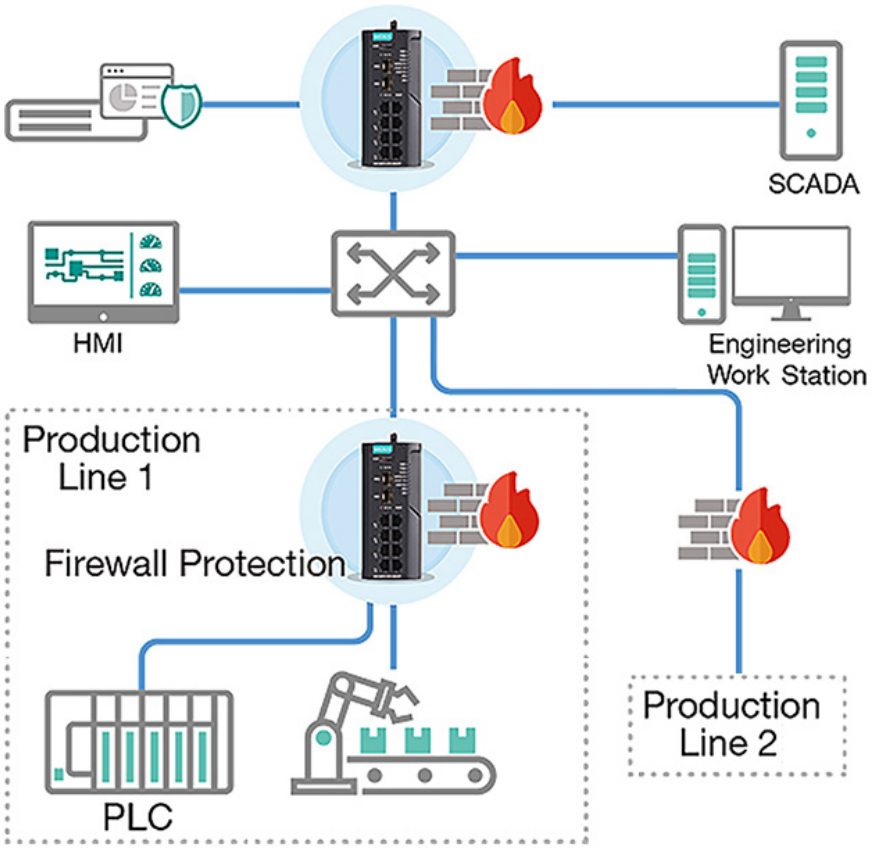


Figure 3. Network segmentation builds boundaries to protect production lines without impacting each other when cybersecurity incidents occur.

Stage 3 vulnerabilities: Services and data disruption

Stealing or destroying critical business data from networks is costly and harmful to any organization. However, these malicious actions are far from the worst-case scenario of a successful cyberattack. During the last stage of a cyberattack, the hacker is no longer studying networks but actively causing damage.

During stage 3 of a cyberattack, the hacker could make a machine or network resources unavailable to authorized users by temporarily or indefinitely disrupting services on a host. This is typically called a Denial of Service (DoS) attack, which involves flooding a targeted machine in an attempt to overload it with pings. Furthermore, a hacker could unleash malware, including ransomware to deny you access to your network resources until a ransom is paid.

> **"To limit the attacker's ability** to move throughout your network and commandeer your devices, we recommend network segmentation (figure 3) and traffic control."

How to mitigate

Although damage has already been done by the time the cyberattack reaches stage 3, you can still mitigate the overall harm to your network by ensuring sufficient DoS or DDoS (distributed DoS attacks that involve multiple systems) protection and deploying an industrial intrusion prevention system (IPS) for ransomware and other malware. You also should maintain reliable system backups and blacklist unauthorized protocols to minimize data loss.

Stay vigilant

With cyberattacks targeting increasingly more industrial networks, it is crucial to identify and mitigate system vulnerabilities before these

weaknesses are exploited by those who intend to do harm. There are two directions you can take to enhance network security. One is to ensure that your industrial networks have a foundation—secure network infrastructure, which allows authorized traffic to flow to the correct places. Alternatively, you can identify critical assets and give them layered protection, such as industrial IPS or whitelisting control.

ABOUT THE AUTHOR

Felipe Sabino Costa is a LATAM industrial cybersecurity (IACS) expert with Moxa.

Today's automated systems need better protection from cyberthreats.

Even the most highly automated systems are still vulnerable to cyberthreat vectors. 1898 & Co. provides industry-leading assessments, cyber program development, road maps, training, detection and incident responses to help you meet these challenges head-on. Learn more about how we can help protect your systems at **1898andco.com/CyberSolutions22**.

1898 & CO℠
PART OF BURNS McDONNELL

ICS Penetration Test

Working with the Blue Team, this active assessment or simulation of a real-world cyberattack tests an organization's cybersecurity capabilities and exposes vulnerabilities within technology, people and processes.

ICS Red Team

This simulated, adversarial assessment attempts to identify and exploit weaknesses within an organization's cyber defenses. Detection capability efficacy may also be validated.

ICS Purple Team

Working with the Purple Team is a more collaborative approach between the Red Team and the Blue Team. The Blue Team may extend beyond the core ICS cyber team to include site ops, engineering and IT.

Examining the Good, the Bad, and the Ugly of OT Security

By Jim Richberg, Fortinet

Organizations recognize the importance of OT security but are struggling to build an appropriate cybersecurity strategy.

Operational technology (OT) and critical infrastructure security are top of mind these days. Although companies acknowledge OT security's importance, they are still struggling to build a strategy that can counter today's mounting threats. Fortinet recently conducted research on this topic, culminating in the 2022 State of Operational Technology and Cybersecurity Report. The findings give insight into what's working, what's not working, and what's next.

The good: High threat awareness

What's improving, albeit slowly, is that 97 percent of global organizations now consider OT a moderate or significant factor in their overall security risk posture. As OT systems become more attractive to malicious actors, C-level executives understand the significance of safeguarding these environments to reduce risk to their companies.

It's also worth noting that 52 percent of organizations have the ability to track all OT activities from the security operations center (SOC)—that's progress, but it's still not enough since it means nearly half of organizations with OT remain blind to important information affecting OT security. A lack of centralized visibility contributes to risk and weakens an organization's security posture. While OT security is increasingly important to most survey respondents, there's still progress to be made.

"A lack of centralized visibility contributes to risk and weakens an organization's security posture."

The bad: Who owns OT security?

Organizations are still wrestling with full protection of their OT assets. In the relatively new world of IT connected and internet-accessible OT, the report reveals that collective OT security efforts by enterprises across the globe represent progress but remain insufficient to provide full protection of ICS and SCADA systems.

The problem may be compounded because, unlike IT security, OT security ownership is not yet a C-level responsibility, but rather is still being owned by relatively low-ranking professionals. However, more executives are aware of and concerned about the security of OT systems. While the CTO and CISO/CSO remain among the leaders who most influence cybersecurity decisions, the survey suggests that others in the C-suite are weighing in on cybersecurity.

This year, 35 percent of respondents ranked the CTO among the top three security influencers—down from 50 percent last year. And 33 percent named the CISO/CSO to the top three, down from 45 percent in 2021. One-third of respondents picked the vice president or director of network engineering or operations as the person with ultimate responsibility for OT security. This is a significant rise above the previous year's percentage. Roughly twice as many organizations now vest OT security responsibility with an operationally focused leader as they do with the CIO or CISO/CSO.

The slow and incremental progress organizations reported in their security maturity in the past year has done little to improve actual security results. Consequently, the great majority of OT organizations continue to sustain breaches—often many times each year.

The ugly: A confluence of risks

What's worse, this lack of impact on the number of OT security breaches is occurring even as OT security moves higher in many organizations' risk portfolios. Security is seen as increasingly critical considering current realities. Geopolitical events are increasing the likelihood of assaults, more OT systems are being connected to the internet, and threats are becoming more sophisticated and causing greater damage.

> **"Organizations can reduce their risk** and improve their security and operational efficiency by using integrated security solutions."

In the previous 12 months, a staggering 93 percent of companies reported suffering an incursion, with 78 percent having more than three. Downtime, monetary or data loss, brand reputational damage, and even impact on safety were all consequences. Most organizations, without a doubt, have more work to do.

Three action steps for stronger security

Organizations need to adopt a new three-pronged approach to OT security to meet the demands of today's shifting threat landscape and changes in the interconnected OT-IT environment. First, put in place solutions that give OT a centralized view. Organizations should have centralized, end-to-end visibility of all OT activities to increase security. According to the survey, top-tier firms—the 6 percent of respondents who reported no intrusions in the previous year—were more than three times as likely to have such centralized visibility as their peers who had been hacked.

Second, consolidate security solutions and providers to facilitate cross-environment integration. Organizations should strive to combine their OT and IT solutions and to consolidate around a smaller number of providers to reduce complexity and obtain a centralized view of all devices—both IT and OT. Organizations can reduce their risk and improve their security and operational efficiency by using integrated security solutions.

Third, use network access control (NAC) technology. Organizations that avoided incursions in the previous year were significantly more likely to have implemented role-based NAC, which ensures that only authorized individuals have access to essential systems and digital assets.

Set the stage for OT security success

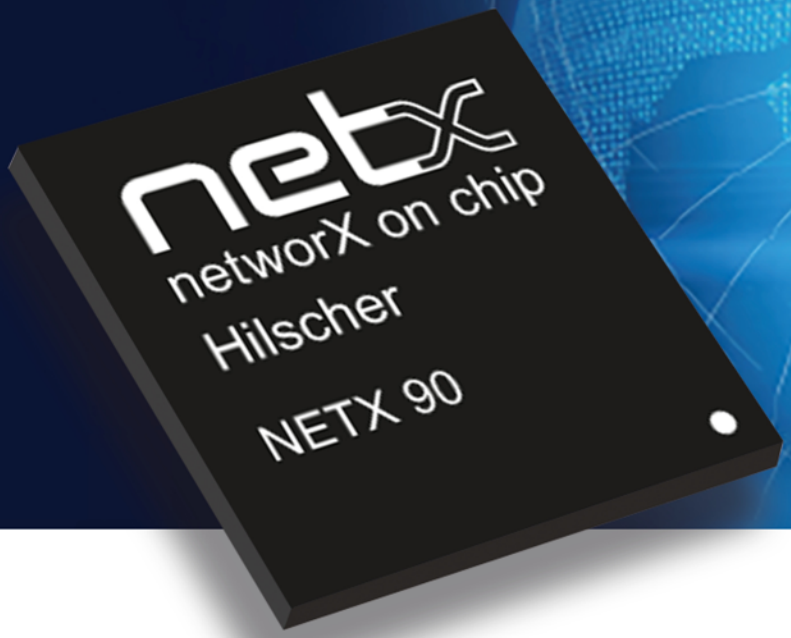
Given current geopolitical events, governments are warning that they expect cyber-attacks on essential infrastructure and key economic assets to escalate. Centralized, end-to-end visibility, along with tool and vendor consolidation, and NAC use, will set the stage for success. Additional best practices include using artificial intelligence (AI)-based tools that enable predictive behavior analytics, and security orchestration and automation technologies to support zero-trust access operations. Collectively, these capabilities will help organizations protect themselves against threats from malicious insiders,

cybercriminals, and state-sponsored attackers. These capabilities will also help organizations across a broad range of industrial sectors to mature their OT security more quickly.

ABOUT THE AUTHOR

Jim Richberg is a Fortinet field CISO focused on the U.S. working to bring cybersecurity solutions to industry and the public sector following a more than 30-year career driving innovation in cyber intelligence, policy, and strategy for the U.S. government and international partners. He served as national intelligence manager for Cyber and the senior federal executive focused on cyber intelligence within the more than $80 billion U.S. intelligence community (IC) annual operating budget. He was the senior advisor to the director of national intelligence (DNI) on cyber issues and set collection and analytic priorities for the IC's 17 departments and agencies on cyber threats.

Secure Your Industrial Ethernet With netX 90



Built-in Security:

- **Secure boot and cryptography**
  Encryption via SSL/TLS for HTTPS, OPC UA, MQTT, VPN
- **IEC 62443 compatible**
  Enables layered security for Defense-in-Depth design
- **Built-in diagnostics**
  Monitor operating conditions for predictive analysis
- **Multiple processors**
  Logical separation of communication and application tasks
- **Partitioned design**
  Restricts software access to on-chip peripherals on either side
- **Minimum ten-year availability**

Single Pair Ethernet Ready:

- **IEEE 802.3cg standard**
  10 Mbit speeds and intrinsically safe with Ex equipment
- **Internal xMAC processors**
  Enable protocol specific switching between two channels
- **Supports SPE**
  Connect external PHY devices via MII interface
- **IO-Link sensor networks**
  Connect two 10 Mbit channels with SPE port up to 1,000 meters
- **Real-time Ethernet connections**
  Pair existing 100 Mbit RTE with 10 Mbit SPE
- **Switch Capabilities**
  Use netX 90 as a switched device between 100 Mbit RTE and 10 Mbit SPE

hilscher
COMPETENCE IN COMMUNICATION

Learn more from Hilscher:
call 1.630.505.5301
email: info@hilscher.us or
visit www.hilscher.com,
www.netIOT.com

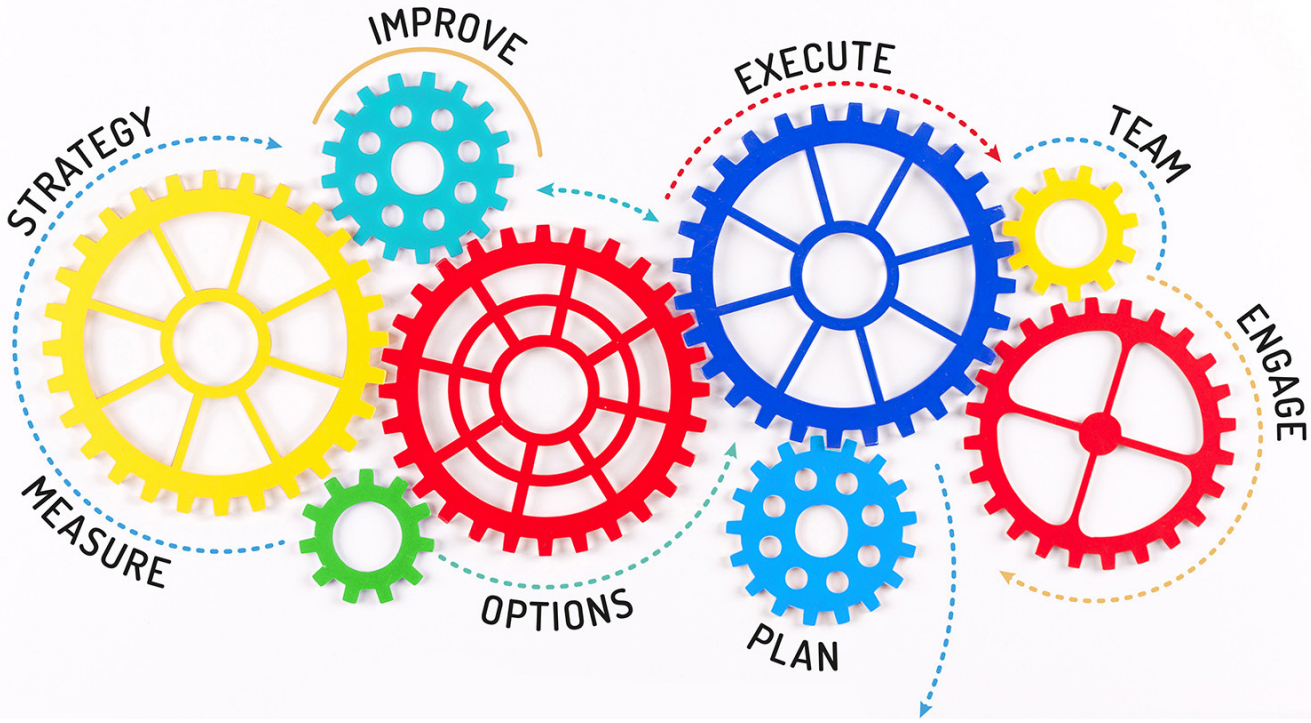
DeviceNet EtherNet/IP PROFIBUS PROFINET EtherCAT Modbus CC-Link CANopen sercos POWERLINK IO-Link OPC UA MQTT

Recovery Starts with Better Change Management

Before and after a cyber-attack, robust change management techniques can ensure production uptime and resilience

By Jack Smith, Automation.com

Cyber risks are on the rise. Manufacturing and industrial operations long ago shed their belief that they were invulnerable because their systems were too isolated or too obscure to be targeted. Organizations now seek to understand the impact and likelihood of their cybersecurity risks and then seek to reduce those risks. But mitigating risk is only the first part of comprehensive cybersecurity planning.



To enable continuous operations and limit business impact when a cyber-attack does occur, organizations need additional tactics. These can include strategically hiring cybersecurity talent, or using new methods to identify, combat, and recover from attacks. Given increasingly interconnected and frequently updated systems, robust software-system management is a particularly useful tool.

Rise of OT cyber risks

Improvements to a plant's operational technology (OT) cyber risk management and mitigation plans should be made in tandem with the rise of attacks, which are up 144% from 2020, according to Industrial Safety & Security Source (ISSSource). Data from the company's OT Security Incidents in 2021: Trends & Analyses report, which analyzes data from its ICSSTRIVE.com database, says "the year 2021 saw the number of cyber-attacks with physical consequences in process and discrete manufacturing industries more than double over those reported in 2020.... Almost all these incidents were the result of targeted ransomware. Almost all these attacks impacted multiple physical sites."

In a recent webinar, ISSSource reported that OT ransomware incidents with physical consequences have increased 133% year-over-year since 2020, and that published estimates cite up to $140 million in damage per event. The types of facilities subject to these attacks cover the industry spectrums (figure 1).

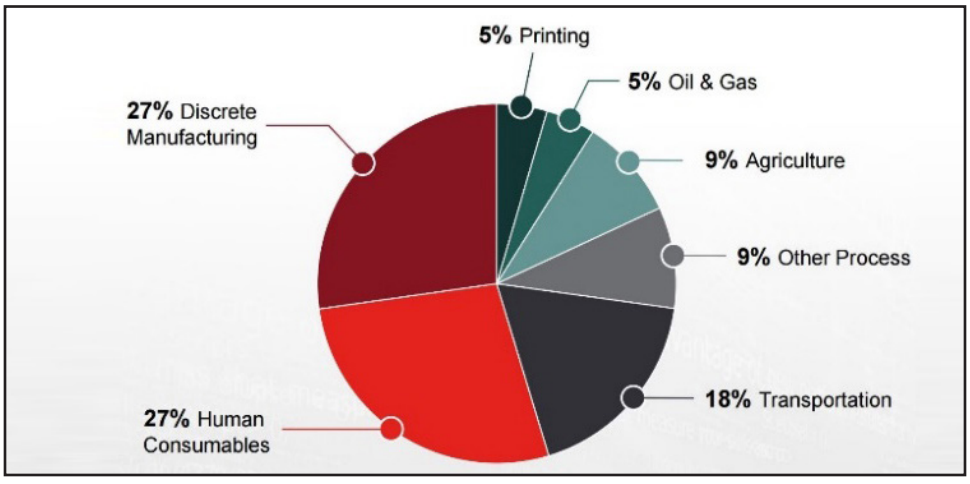


Figure 1. Cyber-attack distribution by industry. Courtesy: Industrial Safety & Security Source

McKinsey & Co. expects that, over the next three to five years, three major cybersecurity trends will have the biggest implications for organizations of all types:

1. **Growing on-demand access to ubiquitous data and information platforms.** Organizations are collecting vast amounts of customer and machine data and are increasingly using the cloud for storing, managing, and protecting these data.

2. **A growing regulatory landscape and continued gaps in resources, knowledge, and talent.** "Many organizations lack sufficient cybersecurity talent, knowledge, and expertise—and the shortfall is growing. Broadly, cyber risk management has not kept pace with the proliferation of digital and analytics transformations, and many companies are not sure how to identify and manage digital risks," McKinsey says.

3. **Hackers are using AI, ML, and other technologies to launch increasingly sophisticated attacks.** "The stereotypical hacker working alone is no longer the main threat. Today, cyber hacking is a multibillion-dollar enterprise, complete with institutional hierarchies and R&D budgets. Attackers use advanced tools, such as artificial intelligence, machine learning, and automation," McKinsey says. "Other technologies and capabilities are making already known forms of attacks, such as ransomware and phishing, more prevalent."

Preparing for the inevitable

Automation can be used to counter more of the sophisticated attacks coming at organizations, says McKinsey. "Automation should focus on defensive capabilities like security operations center (SOC) countermeasures and labor-intensive activities, such as identity and access management (IAM) and reporting. AI and machine learning should be used to stay abreast of changing attack patterns. Finally, the development of both automated technical and automatic organizational responses to ransomware threats helps mitigate risk in the event of an attack."

As the level of digitization accelerates, organizations can use automation to handle lower-risk and rote processes, freeing up resources

for higher-value activities, McKinsey advises. Automation decisions should be based on risk assessments and segmentation to ensure that additional vulnerabilities are not created. For example, organizations can apply automated patching, configuration, and software upgrades to low-risk assets but use more direct oversight for higher-risk ones.

> **"Ensuring that the correct,** authorized versions of software are always running is paramount to keeping production running."

As ransomware attacks increase, organizations must respond with technical and operational changes, adds McKinsey. "The technical changes include using resilient data repositories and infrastructure, automated responses to malicious encryption, and advanced multifactor authentication to limit the potential impact of an attack, as well as continually addressing cyber hygiene. The organizational changes include conducting tabletop exercises, developing detailed and multidimensional playbooks, and preparing for all options and contingencies—including executive response decisions—to make the business response automatic," the report states.

Software system change management

Regardless of their sector, size, or task set, industrial production environments require complex information technology (IT) setups designed to handle integrated systems and high volumes of data. While both OT and IT departments use digitalization to improve productivity and other business outcomes, sometimes the two worlds require translation and teamwork so their different methods and best practices can be achieved. For example, although it has become standard practice for IT departments to schedule routine backups and manage data storage, OT personnel have been slow to adopt such data hygiene and software-system management solutions.

Ensuring that the correct, authorized versions of software are always running is paramount to keeping production running—

whether OT or IT personnel are tasked with managing the system. With version control and change management tools, operators can have access to the most current software and know when changes require further action. Advanced software solutions can summarize the entirety of an automated production environment and analyze devices on the shop floor. Because they can detect differences in programming configuration and firmware versions, even for identical sensors, such systems make it easier to isolate errors.

Change management is a structured process for planning and implementing new ways of operating. According to an article in the April 2022 issue of InTech, the official publication of ISA—International Society of Automation, "An automated, standards-based documentation process saves time and cost while increasing quality. With standards-driven processes and workflows comes the assurance of following the best industry practices during the definition, design, development, integration, documentation, and support of automation projects. This ensures the execution of projects with precision and standardization."

Successful change management relies on four core principles:

- Understanding change or changes to be made
- Planning the best way for the necessary changes to occur
- Implementing changes in the most effective manner
- Communicating the implemented changes to the appropriate stakeholders

That's just the beginning. If changes are made by multiple people to OT-centric code, the potential exists for one group to not know what another group is doing. If changes that affect the operation—and/or cybersecurity—of a manufacturing facility are made, they must be made for a valid reason. There must be documented justification for the change. If a robust change-management system is in place, that system should track and catch any deviation from what is expected in the procedures or code. The system's activity history will reveal who changed what, where, when, and why.

Good change management is not a one and done proposition, nor is it best executed by spot checking. Good change management must be in place continually—in real time. Whether unauthorized changes come from lack of employee communication, unauthorized OT system users, or actual cyber malfeasance, change management that's done correctly is a company's best insurance against downtime and resource for recovery.

From detection to backup to recovery

Version control and software change-management tools can help organizations at all stages of cybersecurity activity—from detection of vulnerabilities to recovery from attack. They can be used to ensure data is current and corresponds to the latest iteration. They can reveal data anomalies and, hence, vulnerabilities and exposures.

A state-of-the-art change management system can manage software programs and configuration settings data in a standardized way, so change history can reveal who changed what, where, when, and why. Such tools can aid the user in managing insecure protocols, misconfigurations, and other vulnerable security points, as well as provide automatic assessment of vulnerabilities, affected assets, and the entire industrial control system. Through threat detection functionality, the tool can automatically discover, protect, and manage an industrial control system's critical assets and provide users with risk and vulnerability reporting.

When a production system malfunctions for whatever reason, maintenance staff can take an average of three or four hours to track down changes using a manual approach to managing software versions. Automatic backups reduce the downtime and facilitate rapid recovery. The backups enable users to restore the last authorized version or an earlier one if that was the one running before the malfunction occurred.

When version control and software change-management systems are installed on premises, on the OT network side of the factory floor, tasks from detection to backup to recovery can be automated. The system should provide for the IP addresses of assets and devices to be scanned and added to the system even if they are located below the

programmable logic controller (PLC) level. The information gathered should include the device brand, manufacturer, firmware version, and where the device is physically located in the rack.

When users run an automated backup, it should also be possible to send this information to a threat analysis component, which can check the web to see if there are vulnerabilities in software components or firmware versions. It is also helpful if the threat analysis can identify unusual traffic patterns, malware, or external, unapproved access to the network.

Multi-faceted change management: octoplant

An example of a state-of-the-art change-management system is octoplant from AUVESY-MDT. octoplant is a new data management platform that provides a vendor-independent and comprehensive view of all automation backup processes involving OT and IT. This change-management platform consists of eight solution sets tailored to specific industrial needs (figure 2).

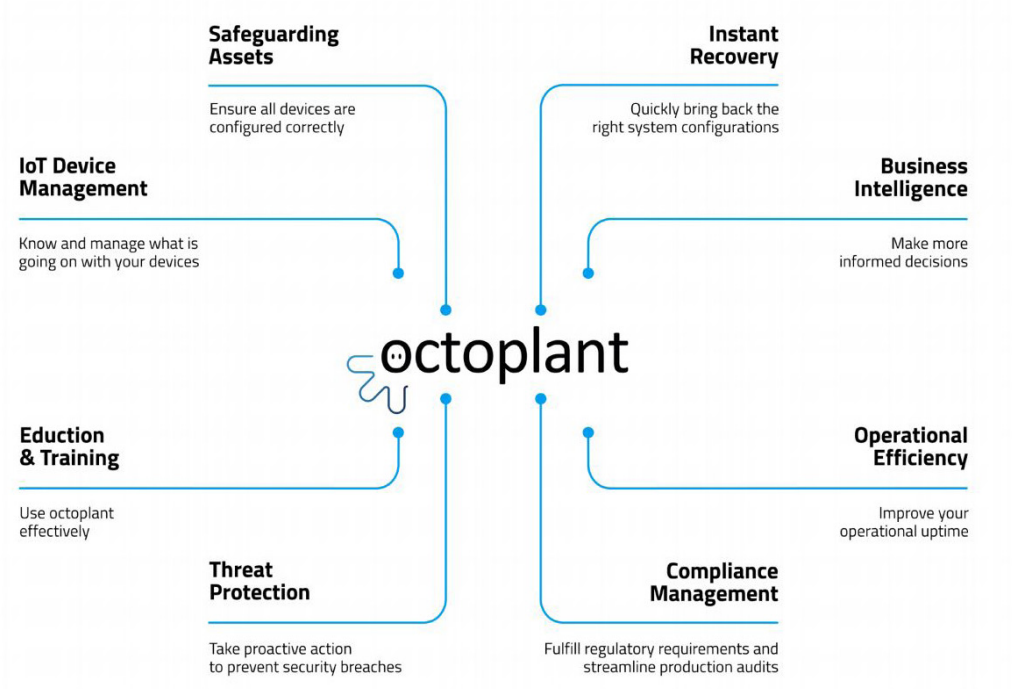


Figure 2. The octoplant platform comprises eight solution sets that offer features tailored to specific industrial needs. *Courtesy: AUVESY-MDT*

octoplant solution sets encompass threat protection, safeguarding assets, IoT device management, instant recovery, operational efficiency, business intelligence, compliance management, and education and training for all industrial software. According to Stefan Jesse, Group COO at AUVESY-MDT, while comparable software may only cover individual machines or partial aspects of a plant such as PLC, SCADA, and HMI, or the programming of robotics, octoplant provides visibility into the function and safety status of all plant elements.

octoplant uses dashboards (figure 3) to display the various statuses of the plant. Production managers can see where programs and configurations are stored and how up to date they are, as well as the current and correct status of all machine programming, the version history of all changes, and tabular and graphical reports detailing program differences.

Figure 3. octoplant uses dashboards to display the various statuses of the plant. *Courtesy: AUVESY-MDT*

Automated backups can be scheduled to ensure the correct authorized version of each piece of software is always running. These backups can be applied to a single device or the entire plant, even if the facility consists of several hundred or even several thousand devices, sensors, pieces of hardware or software components, says Jesse.

Final thoughts

Cyber-attacks are on the rise so improvements to cyber risk management and mitigation plans should be made now. With increasingly interconnected systems and exponentially growing quantities of data, industrial operations must put systems in place that allow them to detect vulnerabilities and respond when a breach occurs. Robust data and software-system change-management tools can help ensure companies remain running during normal operations and respond quickly when the worst occurs and prevent production downtime during normal operations and ensure resilient recovery when the worst occurs.

ABOUT THE AUTHOR

Jack Smith (jsmith@automation.com) is a contributing editor for Automation.com and ISA's InTech magazine. He spent more than 20 years working in industry—from electrical power generation to instrumentation and control, to automation, and from electronic communications to computers—and has been a trade journalist for 22 years.

GLOBAL CYBERSECURITY ALLIANCE

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

Get Engaged!

- Follow our blog: www.isa.org/isagcablog
- Download our white papers and guides: www.isa.org/isagcashare
- Join the End User Council: www.isa.org/endusercouncil

MEMBERS:

cervello, SecurityRisk Advisors, OMICRON, Honeywell, Johnson Controls, Rockwell Automation, HEXAGON, NOZOMI NETWORKS, Life Is On Schneider Electric, FORTRESS, CLAROTY, WALLIX, xage SECURITY, FORTINET, exida, radiflow Secure your Assets, PURDUE UNIVERSITY Polytechnic Institute, BUREAU VERITAS, tdi technologies, INL Idaho National Laboratory, munio SECURITY, DRAGOS, Carrier, BASEROCK IT SOLUTIONS, DIGITAL IMMUNITY STAY PRODUCTIVE, STAY SECURE, tenable, MSI, 1898 & CO., TiSafe, ACET SOLUTIONS, WisePlant Smart, Safe & Secure, HERONTECH, CYBEROWL, EATON Powering Business Worldwide, LOGIIC, PETRONAS, InstMC Companion Company, KPMG, Deloitte., ConsoleWorks Cybersecurity Operations Platform, ISASecure, SURGE ENGINEERING, Johns Manville A Berkshire Hathaway Company, senhasegura by MT4, txOne networks, xylem Let's Solve Water, CYPHY DEFENSE, Idaho State University, COONTEC, RED TRIDENT INC, UL Solutions

Top 25 ICS Vulnerabilities

By Henry Martel, Antaira Technologies

Weaponized cybersecurity attacks can destroy critical infrastructure systems that support daily life

Industrial control systems (ICS) have been of incredible value to industrial companies. The ability to control the production and manufacturing process of goods and services has been a major milestone in our modernized world. However, everything comes with risks. Malicious actors, attackers, and hackers are terms used to describe the individuals who try to intentionally cause harm through virtual and physical means to systems responsible for our modern lifestyles. These attacks can result in bad press and government fines. Moreover, they can cause serious harm or death to individuals or even whole communities by destroying water purification systems, disabling power plants, and prolonging critical system outages.

Crossing cybersecurity boundaries

Cybersecurity attacks, vulnerability exploits, and digital espionage have crossed the boundaries into what was once considered off-limit targets. Hacking and cyber-attacks have always been considered a “dark art” primarily focused on taking small systems offline, stealing data, and

holding information for ransom. But times have changed. Cybersecurity attacks have evolved and become weaponized with the capabilities of destroying critical infrastructure systems that support everyday life. An example of such a cyber weapon was the STUXNET worm that infected Siemens Industrial Systems.

Understanding common networking vulnerabilities

Time and experience are required to understand how attackers gain access into networks and exploit vulnerabilities in the sources that generate them. There is no straightforward method that will provide 100 percent protection against cyber-attacks. Instead, the following list should be a small element of a broader toolkit used as part of the cybersecurity lifecycle.

1. **Lack of employee training.** ICS engineers often find themselves dealing with Industrial Internet of Things (IIoT) devices that need advanced configurations and third-party support. In many cases, engineers have limited access to the necessary resources for stable configurations. Instead, engineers with only a basic understanding of information technology (IT) systems take it upon themselves to manually configure devices and place them in their networks. Due to no formal training on networking, IT security policies, protocols, and cybersecurity, devices are often misconfigured and riddled with security holes and vulnerabilities.

2. **Misconfigurations.** Systems that have been misconfigured present major security vulnerabilities. For example, poorly configured security settings can limit different types of traffic on an interface but leave commonly used ports open for intruders to exploit.

"Granting unqualified users permission to access device commands and other programming features is a common vulnerability."

3 **Insider threats.** Insiders are often responsible for cybersecurity breaches, both inadvertently and deliberately. A disgruntled employee may "shoulder surf" lax employees and steal passwords as they are entered. This provides unwarranted access to systems and knowledge of plant workings that can lead to havoc.

4 **Unnecessary user access.** Granting unqualified users permission to access device commands and other programming features is a common vulnerability. Users who don't fully understand company security policies, the complexity of how devices interact with each other, or the ramifications of how a misconfiguration can impact a network should not be allowed to configure or make changes to important systems or critical devices.

5 **Asset disposal.** Disposing of old equipment that used to be a part of a company network must be done carefully by sanitizing any traces of the network. Any data captured from expired assets can be used to provide reconnaissance of the network.

6 **Third-party outsourcing.** Contractors, vendors, and outside consultants provide guidance and subject matter expertise to manufacturers as well as other companies who require their assistance. Having outside personnel accessing critical systems from remote locations is a typical daily occurrence that often gets overlooked by busy admins and engineers. While the initial person they hired might be properly vetted, the contractor might then turn around and hand menial tasks to someone who is careless, hasn't had the proper security clearance, or is not qualified to have accessibility to the network.

7 **Legacy hardware/software.** Legacy hardware and technologies operating inside of industrial systems is a common practice we still see today. Many companies who are operating legacy systems do not have the finical resources to make the necessary upgrades and instead choose to patch and replace components as needed. However, this type of operational model opens the door to security vulnerabilities that can easily be exploited by a seasoned hacker

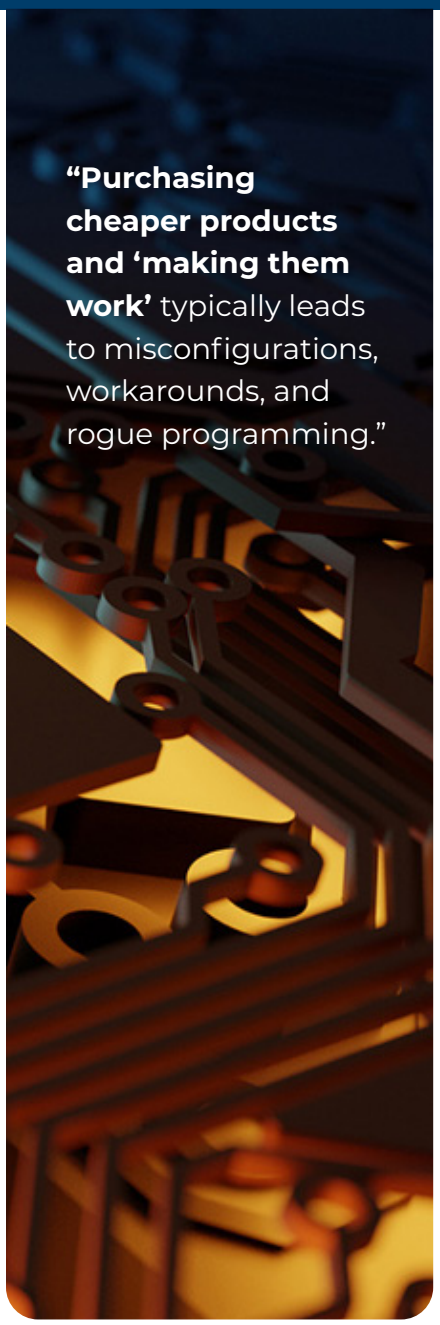
due to outdated systems having little to no manufacturing support in terms of cybersecurity, while patches and system updates are nonexistent.

8 **Inadequate hardware.** Companies often try to save money by purchasing inadequate hardware that's not designed for a specific application. Purchasing cheaper products and "making them work" typically leads to misconfigurations, workarounds, and rogue programming, which opens the door to security gaps and vulnerability exploitation.

9 **Hardware design flaws.** Industrial control systems interact with a wide variety of devices that are designed with limited cybersecurity features. For example, power analyzers or liquid flow control sensors might be considered smart because they communicate with a centralized management system but can be susceptible to simple programming errors and software code that can easily be overwritten, making them ideal targets for malicious code execution.

10 **No backups.** Not having secure copies of local backup configurations for critical systems can lead to a wide range of vulnerabilities. Often is the case where a critical system or piece of equipment has failed and urgently needs to be replaced. When no working backups exist, complex configurations that must adhere to company security policies are misconfigured and present security gaps for intruders to exploit.

11 **Software updates.** Not having the latest version of software for a device can lead to security and vulnerability issues. When manufacturers release software updates, it's typically to resolve known security and functionality issues and add functionality that can prevent future issues from occurring.



12 **Memory overload.** Memory overload takes place when an attacker gains unauthorized access to a device. At this point, the attacker can execute simple code to input more data than the device can hold, overloading stored memory and causing the device to crash, reboot, or provide entry to low-level commands that can be reprogramed to point toward malicious code that can be executed later.

13 **No download validation.** Downloading software for applications and security patches can sometimes lead unsuspecting users to a look-alike website that offers what looks like legitimate software. Not having any mechanisms to validate software can lead to a wide range of security holes and vulnerabilities that can cripple a network.

14 **Poor network design.** Operational networks have become just as complicated and robust as their IT counterparts and often require segmented isolation for various functions and processes through virtual local area networks (LANs) or firewalls. Poor network designs don't provide isolation needed for security, and instead are configured as one large network that provides an attacker access to everything inside the network.

15 **Network assessments.** Fully functional networks often are left alone and with minimal monitoring and system reporting tools operating in the background. It's rare that admins take the extra step of assessing the network for security flaws, vulnerabilities, and operational readiness. These types of extra measures are needed to ensure that operational technology (OT) networks are fully protected and updated with the latest vulnerability patches, security updates, and optimal configurations.

16 **Limited network visibility.** Admins and engineers responsible of managing OT networks typically have monitoring tools that can track the availability of hardware devices and applications running on the network. However, in today's complicated networks with multiple network segmentation and remote access capabilities, admins need to be more vigilant with the way they monitor traffic.

Secondary firewalls monitor traffic at a packet level and ensure that no unknown data packets traverse the network or map out destinations and hardware signatures for later use as a planned attack on the network.

17 **Lack of documentation.** Not having updated documentation on your network, connected devices, security policies, and operational procedures can lead to a wide range of security vulnerabilities, such as incorrectly configured security features, unpatched software holes, incorrectly segmented networks, open access, and availability that should be secured.

18 **Telecommuting.** Over the past two years, there has been a significant increase in remote workers and telecommunication positions. In many cases, these employees need access to internal company resources for work purposes. Companies that do provide remote access capabilities to remote workers typically use a virtual private network (VPN) or other connection software to provide an additional layer of security. However, companies are finding out that these employees have basic to little security on their home networks and have security holes that can be easily compromised. Once a company computer or laptop connects to the local home network, it's attacked and, through malicious code, can be taken over later. Once the machine is connected to the company network through a VPN, the attacker can gain access to the business's resources.

"Not having updated documentation on your network, connected devices, security policies, and operational procedures can lead to vulnerabilities."

19 **Remote applications.** Having remote applications for company resource access, tech support, and real-time monitoring and alerting can be extremely beneficial. However, these types of applications present a major security risk and vulnerabilities to their adherent nature. An attacker who can steal credentials for these types of applications can wreak havoc on an OT network. Be sure to enforce strict password policies and two-factor authentication to ensure that only granted users can access these types of applications on the network.

20 **Phishing.** Phishing and email scams have always been major sources of vulnerability exploits and malicious code execution. The process is simple and highly effective. Unsuspecting users download a file from what looks like a trusted source or click on a weblink. The process downloads a small malicious piece of code that can be used later to download a secondary piece of code or software and allows attackers access into systems.

> **"Two-factor authentication** can be defeated if a hacker takes control of the computer after authentication has taken place."

21 **Two-factor authentication workarounds.** Two-factor authentication is an excellent way to reduce the likelihood that the wrong person gains access to information, but it can be defeated if a hacker takes control of the computer after the two-factor authentication has taken place. A remote industrial automation control system technician may log in from a home network, thinking that the information in transit is safe thanks to the VPN. But a virus or remote access trojan (RAT) that was accidentally installed earlier can be activated by the presence of the VPN, and access may be unknowingly granted by offering an innocuous message saying that the first login failed and to try again.

22 **Unsecured data sockets.** Using default or commonly known data sockets or communication ports for applications within an OT network presents huge vulnerabilities. Attackers are aware of the common port settings and write malicious code directly targeting these ports.

23 **Unnecessary services.** Running all default services on applications that are not needed can leave security gaps in the OT network. Find out what services are necessary to run the hardware and applications and shut off everything else.

24 **Weak firewall rules.** Firewalls are an intricate part of enterprise networks. However, in the case of OT networks, many firewalls are not configured as thoroughly and instead are configured with only basic parameters for functionality. In these types of scenarios, firewalls can be easily bypassed and the lightly secured network can be accessed.

25 **Authentication bypass.** Users often tire of logging into systems to make small changes, especially if long, complicated passwords are required for authentication. In many cases, users will disable authentication, unknowingly exposing their system to attackers.

Final thoughts

Addressing most of these vulnerabilities requires a holistic approach that addresses every link in the chain. This includes people involved with those systems on every level, and not just the tools they utilize.

ABOUT THE AUTHOR

Henry Martel (henry.martel@antaira.com) is a field applications engineer at Antaira Technologies, a company that provides industrial networking solutions with advanced security feature sets to protect critical systems against would-be actors or malicious activity.

Join ISA in Galveston, TX this November for the automation event of the year!

- Network with ISA leaders and automation professionals from around the world
- Attend technical presentations on trending topics including Digital Transformation, Process Industry, IIoT and Smart Manufacturing, and Cybersecurity
- Attend the ISA Honors and Awards Gala
- Can't attend in person? This conference will also be available LIVE, virtually!

For details and to register visit isa.org/alc.

International Society of Automation
Setting the Standard for Automation™

#ISAALC