ARTICLE

Four steps to harden your ICS cybersecurity and improve OT systems resiliency with little or no cost.

usa.siemens.com/network-security

Recommended Steps

1. Understand the similarities and differences between OT and IT cybersecurity
2. Conduct a detailed site survey to create an accurate inventory of networks and networked devices
3. Optimize currently deployed network components
4. Implement comprehensive and automated data protection

Cybersecurity isn't a foreign concept to industrial enterprises. Management, engineers and technicians can't help but see its headlines in their trade and business press, regardless of their sector. In fact, a 2019 global survey[1] of 282 industrial companies operating in critical infrastructure and process industries revealed that 80 percent consider Operational Technology (OT) cybersecurity to be a high priority.

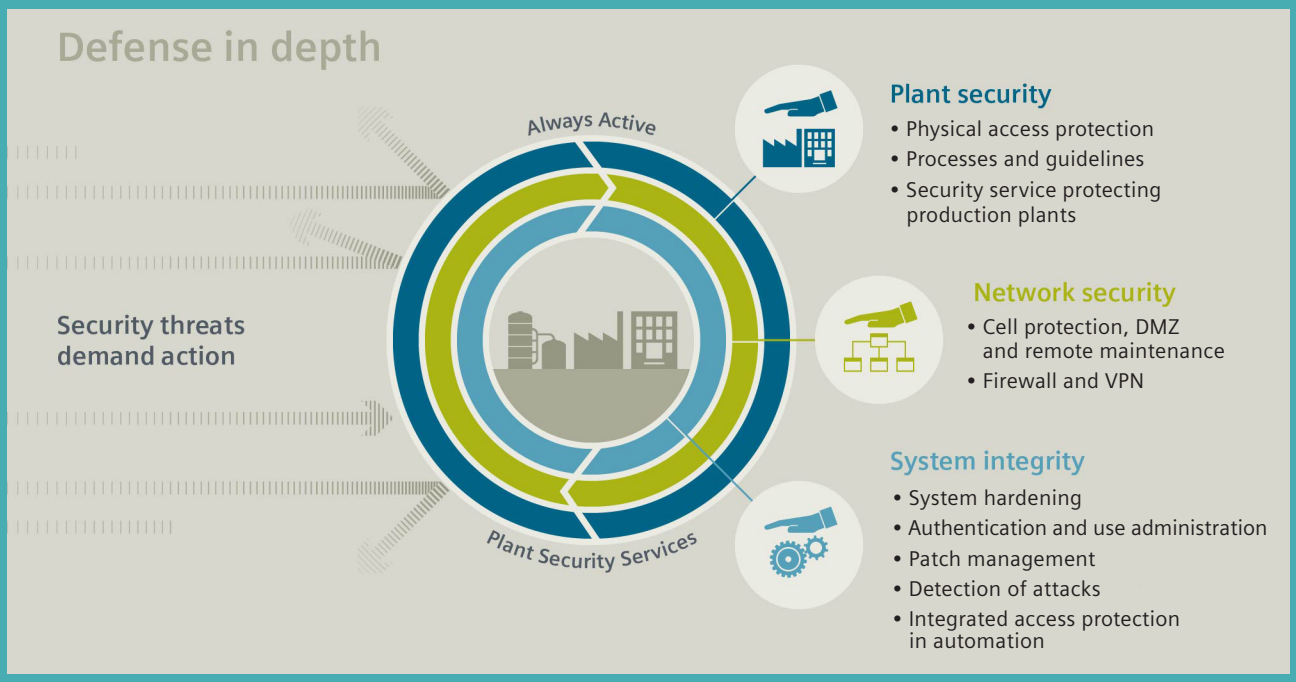
However, that same survey found that only 31 percent had implemented an incident response program and only 57 percent had committed any budget to cybersecurity. This suggests a wide gulf exists between intention and practice, a gap not lost on the various sources of cyber threats of all kinds – increasingly criminal enterprises, state actors, and so-called hacktivists with political agendas. That's in addition to solitary hackers using powerful tools readily available on the Dark Web, such as ransomware-as-a-service.

Implementing a comprehensive, defense-in-depth OT cybersecurity program, including an effective incident response and data/business recovery plan, doesn't necessarily require a lot of cost. It does demand some specialized knowledge, plus time and effort. Much of the time can be potentially recovered on future projects when accurate documentation and better familiarity with existing systems may reduce pre-engineering and startup time.

Following are four steps Siemens recommends that industrial enterprises consider taking to deploy and harden OT cybersecurity in addition to improving their resiliency and data/business recovery times should an intrusion occur.

Author
Chuck Tommey, IT/OT Networking Consultant,
Siemens Industry, Inc.

SIEMENS



What is a "defense-in-depth" cybersecurity model?

Taking its cue from Middle Ages castle defenses, defense-in-depth cyber security uses layers to protect critical systems and assets. It starts with ensuring the security of the physical perimeter with gates and locks to keep unauthorized personnel out. Then, to keep out cyber intruders, it layers multiple levels of additional safeguards, including firewalls, anti-virus/whitelisting software, plus PC system hardening and Intrusion Detection Systems (IDS) with special signatures for the industrial environment and anomaly-based detection for previously unseen malware

1 Understand the similarities and differences between OT and IT cybersecurity

OT and Information Technology (IT) cybersecurity have the same goal: To keep the business safe from external cyber-attacks and insider threats, whether they are malicious or, in the case of the latter, more likely unintentional. However, OT and IT cybersecurity typically have different approaches with different priorities, management structures, types of protected assets, and even different standards.

First, consider their respective goals. IT focuses on data confidentiality, integrity and availability, while OT focuses on personnel and environmental safety – a huge concern not typically part of IT's responsibilities – as well as asset availability and utilization, plus the integrity of operating data and relevant intellectual property. OT networks must operate in near real-time with minimal latencies, while IT networks can operate with best-effort packet timings, with latencies in seconds not being disruptive.

Second, each group has different backgrounds, management and responsibilities. With computer science backgrounds, IT usually reports to the CSO (Chief Security Officer) or CIO (Chief Informational Officer), who reports either to the CFO (Chief Financial Officer) or CEO (Chief Executive Officer).

With industrial engineering backgrounds, OT typically reports up through plant management and, at the executive level, the COO (Chief Operating Officer).

Third, IT and OT use different standards for their frameworks. Both may employ layered, defense-in-depth approaches, but IT follows the ISO/IEC 27000 family of information security standards. In OT, the ISA/IEC 62443 series and NIST SP 800-82 standards are most prevalent as they provide flexible frameworks to address and mitigate security vulnerabilities in industrial automation and control systems.

Finally, IT and OT are responsible for different types of hardware and software. While IT strives for tightly controlled and short lists of supported hardware, operating systems, and software applications with refresh cycles in the 3-5 years range, OT is stuck with managing and securing many legacy machines, systems, and applications which can span 30-plus years.

The reason IT and OT must better understand each other is they must collaborate to sufficiently protect OT as part of the much larger and increasingly digitalized business enterprise. That's especially true as OT starts incorporating such technologies as edge and cloud computing, the Industrial Internet of Things (IIoT) connectivity, remote asset performance monitoring and diagnostics, and much more.

OT and IT Cybersecurity Standards

It can be hard to keep cybersecurity standards straight, especially as industrial digitalization drives the convergence of OT and IT network operations. Here's a list of the key relevant standards and frameworks, grouped according to their respective orientation:

OT cybersecurity standards

- **ISA/IEC 62443:** From the International Society of Automation (ISA), a process automation trade group, and adopted internationally. Most often used in manufacturing and process industries.
- **NIST SP 800-82 Rev 2:** Specifically required by most utility-regulating authorities via the DHS Critical Infrastructure Program (CIP)
- **Federal Energy Regulatory Commission (FERC)** and the **North American Electric Reliability Corporation (NERC),** the former regulates the interstate transmission of electricity, natural gas and oil, and oversees NERC, which focuses on compliance with CIP to protect North America's bulk electric system.

IT cybersecurity standards

- **ISO 27001,** best practices for implementing an Information Security Management System (ISMS), designed around risk-based management
- **NIST CSF** (The National Institute of Standards and Technology Cybersecurity Framework): Based on NIST SP 800-53 and ISO 27001
- **Critical Security Controls** (CIS): Top 20 cyber mitigation controls

2 Conduct a detailed site survey to create an accurate inventory of networks and networked devices

A basic cybersecurity dictum is *you can't protect what you don't know exists*. That's why it's important to document every OT network and device attached to each one. Most industrial operations today have deployed a mix of wired and wireless networks, with best practices involving the segmentation of those networks. Segmentation makes it easier to contain initial cyber intrusions, minimizing their spread and threat to an entire plant.

Start with documentation from existing project files, preferably as-built, if it exists, not as-designed. The latter often will differ over the former because the physical or logical environments were different when a network or various connected assets were deployed – or, they've been changed since their deployment.

With this documentation in hand, assign an engineering intern or technician to walk down the network and redline the diagrams, documenting every port and their attached cables while also labeling them. Of course, if no diagrams exist, as could be the case for years- or decades-old plants, then the intern or technician will have to draw the diagrams and should do so using a capable 2D CAD tool (versus hand-drawing), so the resulting files will be digital, which will make them much more useful and versatile.

As a critical part of this project, a network verification scan should be done to ensure all device ports are identified and categorized. One of the most popular free, open-sourced scanner tools is Network Mapper (Nmap). These tools need to be employed with caution in SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) networks, because they could cause inadvertent interruptions of field devices.

This is another reason that IT and OT groups need to collaborate and educate each other. Tools like Nmap might be safe to use for scanning purely IT network environments, but could cause problems if misconfigured for OT ones. ICS forums can provide a wealth of guidance on the proper use of network scanners in OT environments. Also, Siemens offers a 21-day free trial of its newly updated SINEC Network Management System, designed specifically for OT, which can provide large-scale, policy-based device and security management.

Going forward, be sure any future project RFPs (Request for Proposal) require network diagrams with physical or scanner verification before project start and after site acceptance.

Siemens SINEC Network Management System (NMS) for Industrial OT Networks

Siemens SINEC NMS provides centralized control and visibility as well as policy-based configuration of different components over large-scale OT networks. It goes beyond the FCAPS (fault, configuration, accounting, performance, security) management categories of the ISO Telecommunications Management Network model. This includes a northbound interface to enable network and diagnostic data to be shared with different systems and applications, such as HMIs and SCADA Systems. It also includes several distributed operational levels for greater scalability yet continued visibility and centralized management as a network grows and becomes more complex. The SINEC NMS also can help users fulfill the security requirements of IEC 62443. Click here for more information.

3 Optimize currently deployed network components

Documenting all OT networks and connected devices and equipment will include firewalls, routers, and other such gear. Documented data should include details like manufacturer, model/order number, firmware revision, instrument label, and used ports with cable identifiers and destinations. This level of detail enables proactive management and allows research of current support options. Now, update firmware and software to current versions and service packs.

Next, disable all unused services, features, and ports, and change default logins and passwords to complex, hard-to-crack, alpha-numeric ones that include symbols.

Set up user-specific, policy- and role-based logins and passwords, providing user privileges based on Identity and Access Management (IAM) best-practice principles. Many software packages provide integration with Microsoft Active Directory, the world's most widely used directory services platform for Microsoft Windows domain networks. Finally, industrial enterprises should enable all security-related logging, sending login histories to a Syslog server, so user activities and alarms can be traceable, if forensics are needed.

4 Implement comprehensive and automated data protection

Having proactive safeguards in place is important, but it's also critical to have effective reactive procedures ready to respond to intrusions, especially to quickly restore the integrity of operations, applications, data or any combination of the three. Key ICS and SCADA functions should be backed up with hot standbys featuring immediate failover capabilities should their primary counterparts be disrupted.

For data protection, automated and contemporaneous backups are preferable; or at least they should be done on a weekly interval. Ideally, the backup storage will be off-network and, even better, offsite, too.

The former protects backup data in case malware, such as ransomware, succeeds in circumventing defense-in-depth and network segmentation measures and locks it up. In the NotPetya ransomware attacks of 2017, the global shipping giant Maersk almost had to start completely from scratch until they found an Active Directory server in Africa that was offline due to an unrelated network equipment failure.[2]

The latter protects data backups from the physical damage to storage servers that can be caused by natural or man-made disasters, such as hurricanes, tornadoes, explosions, and fires.

Keep in mind that backups are useless if the OT/IT staff doesn't know how to restore them, lacks the right tools to do so, or if the backup system is misconfigured and can't restore the needed system data. Three facets of restoration must be part of an effective, response-ready recovery strategy:

- OT/IT staff must know how each unit of software and hardware is licensed and the procedure to recover and reinstall those licenses. For example, reinstalling a virtual machine or hard drive image may not work, if the license is tied to old hardware, especially if the hard drive serial number is part of the system fingerprint.
- As authentication by certificates becomes more prevalent, it's important to understand which devices require certificates and how to renew, reinstall and, if needed, reimport those certificates.
- Backups must be tested regularly to ensure they can be restored. To do this, pick a system to restore during every scheduled outage or downtime period. This assures backups are operational and gives the OT/IT team practice with restoration procedures. It also allows detailed written procedures to be developed, updated, and improved.

Think about cybersecurity like safety and get started today

Like plant health, safety, and environment (HSE) programs, cybersecurity should be considered alongside them as a required mainstay risk-reduction program with support from executive management, owners, and the board of directors.

The steps outlined above should become regular routines and added to Preventive Maintenance (PM) schedules. This ensures that they join other OT PM routines conducted regularly, with assigned resources and responsibilities, if they're not already being done continuously as with backups.

Cybersecurity consultants and managed services from Siemens can certainly help provide both the specialized knowledge, tools, and monitoring required. However, industrial enterprises must also be prepared to respond to and recover from cybersecurity incidents, which more and more are not a matter of "if" but "when."

That's why they need to treat cybersecurity as a matter of business continuity – just as they would a natural disaster or fire – with plans, training, regular drills, all at regular intervals at least twice yearly. It's also why companies with doubts about the maturity of their industrial cybersecurity should get started on evaluating their safeguards today and strengthening them if necessary.

For essential guidance on how Siemens can advise on industrial cybersecurity or provide managed services both for asset protection and incident response, please visit the Siemens website or contact us at **siemensci.us@siemens.com**.

1 Thomas Menze, The State of Industrial Cybersecurity. (ARC Advisory Group, July 2019), 5-6

2 Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History. (WIRED.com, Aug. 22, 2018)

Legal Manufacturer
Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005
Telephone: 1-800-241-4453
Order No:o.: NTAR-CY4STP-0124

info.us@siemens.com
usa.siemens.com/network-security