White Paper

By

Anthony Ciccozzi
Lead Cybersecurity
Engineer, P.E., GICSP

Securing critical infrastructure networks

Protecting critical infrastructure networks from cybersecurity threats requires a comprehensive consideration of all connected assets. While the traditional focus has been on Information Technology (IT) networks—those networks prioritized secure data collection, storage, communication and use—more focus needs to be placed on non-IT critical infrastructure and services. This requires an understanding of the basic threats and principles related to Operational Technology (OT), Industrial Control System (ICS) and Industrial Internet of Things (IIoT) networks.

Traditional IT networks are responsible for a number of services, have a number of users and connectivity internally within an organization and externally (e.g., to the internet). This presents challenges when trying to secure them, as potential attackers have many points where they can enter and exploit a system (referred to as an attack surface). Servers running critical applications and web portals for vendors and customers all need to be designed securely, monitored and maintained.

New threats target critical infrastructure such as power management devices, in a manner that could leave businesses vulnerable. While IT breaches and incidents (e.g., ransomware) often get the media headlines, there are other non-IT critical systems that need to be considered when securing an entire infrastructure: the networks |and devices in the OT, ICS and IIoT deployed within an infrastructure.

While IT networks focus on data, ICS/OT networks:

- Control or monitor critical infrastructure and assets (e.g., temperature, voltage, current, pressure, etc.)
- Have specific availability, reliability and safety requirements
- Often use combinations of vendor proprietary and commercial off-the-shelf (COTS) components
- Are separate from but integrated with IT systems
- Have legacy systems running critical processes

In this paper, we focus on concepts and methods related to securing the ICS/OT systems. High-level suggestions on how to effectively protect and monitor those systems from threats are presented. We've also included some of the most common questions regarding OT/ICS cybersecurity to help guide discussions about it at facilities.

Powering Business Worldwide

Assessing ICS/OT systems

To determine the best ways to protect ICS/OT systems, it is important to analyze them to understand their architecture, devices and critical functions they need to perform. Threat and vulnerability analysis should be performed to determine vulnerabilities, i.e., weaknesses and gaps in devices, architecture and system maintenance. Companies need a full view of their networks to protect and maintain them by having the ability to detect threats.

An assessment will enable cybersecurity managers to measure and comprehend risk and see how they map to a system's attack surface—identifying all the possible ingress points that leave systems vulnerable (Figure 1: Attack surfaces and threats).

This includes all areas where attackers can:

- Affect inputs and outputs
- Manipulate controls
- Change control privileges
- Lateral movement to others

Understanding the attack surface makes it easier to address risk and prioritize resources to maximize risk reduction.

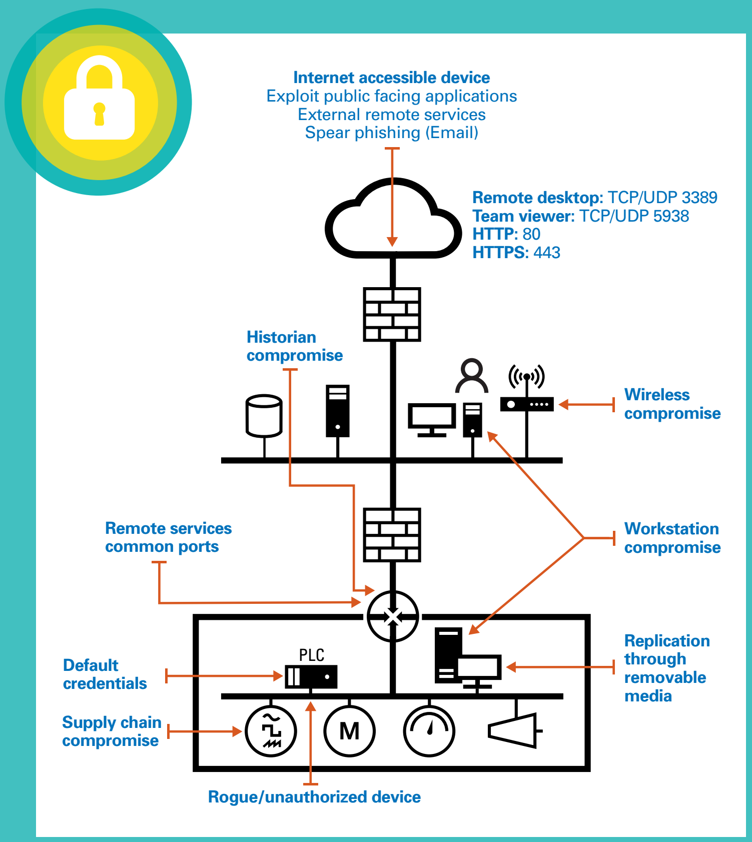

Internet accessible device
Exploit public facing applications
External remote services
Spear phishing (Email)
Remote desktop: TCP/UDP 3389
Team viewer: TCP/UDP 5938
HTTP: 80
HTTPS: 443
Historian compromise
Wireless compromise
Remote services common ports
Workstation compromise
Default credentials
PLC
Replication through removable media
Supply chain compromise
M
Rogue/unauthorized device

Figure 1. Attack surfaces and threats

Assessing ICS/OT systems

The assessment will also provide visibility to attackers' ability to move around the network once they have penetrated the system (known as lateral movement). Without proper segmentation, traffic restrictions and network controls in place, it may be easy for an attacker to penetrate ICS or OT systems through a weak link and move throughout, potentially doing even more damage.

Another key element is the ability to detect intrusions when they occur. The amount of time between the initial attack and the time it is detected is known as dwell time. The global median dwell time for intrusions identified by external third parties and disclosed to the victims dropped to 28 days from 73 days in 2020 according to Mandiant[1]. The ability to detect threats as soon as they occur is vital to limiting the amount of damage attackers can do once they reach the systems. This requires properly deployed ICS/OT monitoring solutions and properly configured logging and alerting on individual devices along with assurance that warnings are not ignored.

Backup and recovery

A robust backup and recovery strategy is also important to protecting critical infrastructures. Due to the availability requirements of most OT facilities, the ability to restore systems to a point in time that they were functional is critical and should be considered as part of an overall defense-in-depth strategy. Facilities that maintain a good backup of all their systems, devices and components are more likely to restore full operation after an incident in a shorter amount of time than facilities without one. This could range from backing up individual programs, settings, databases or configurations to taking a full image of a server. It is never recommended to store backups locally on the systems that are being backed up; they should be stored in a secure remote location. Recovery plans should include where backups are stored and the method and procedures for restoration.

Secure architecture guidelines

An end-to-end understanding of system assets, functions and dataflows is required to ensure the highest level of infrastructure protection. To begin, different zones must be defined at all levels of the network. This goes beyond understanding what machines are on the network. It is necessary to identify the machines by their IP addresses, how the data flows between them and who is responsible for the security of each different zone within the network.

Higher criticality zones should be functionally isolated to protect them from unnecessary and less critical traffic; minimum standard IT functions like email should be kept out of these zones. Logical segmentation to achieve isolation (e.g., VLANs) and ICS-specific boundary protections (e.g., firewalls) can also be used to protect critical zones.

Some other concepts that should be applied include:

- Applying traffic filtering
- Using default deny (allow traffic by exception)
- Implementing whitelisting (explicitly allow known hosts)
- Performing deep-packet inspection on firewalls (e.g., ICS protocol aware inspection)
- Applying data diodes (one-way communication devices)

To harden the endpoints of the system, disable unused ports and services, change default credentials, remove/rename unused accounts and use secure protocols wherever possible (e.g., https vs. http). For an added layer of security, create a neutral zone to separate assets that need access across different zones. Require users to authenticate more than once so only authorized users gain access to the most sensitive information.

Remote access to a system may be critical to operate, maintain or troubleshoot. Remote access to critical zones should be limited to ports that have been approved and are monitored. No direct access from a less trusted zone should be allowed without traversing layers of defenses and security controls (e.g., authenticating and authorizing the user or asset trying to make the connection). There are two different types of remote access: interactive (user-initiated and controlled) and automatic (machine-to-machine). Remote access is often implemented to make it easier for vendors to service machines from outside the facility and conveniently onboard new employees. But when such access is granted, it can leave the system open to outside attacks—so it pays to take the time to do it right. While there are many methods and concepts that can be applied (including zero-trust solutions), a common method that balances effectiveness with cost and complexity is the use of a jump host. A jump host prevents remote-access users from having direct access to the control networks by requiring them to reauthenticate before getting access to the control network. Consider adding a virtual jump host dedicated to each entity that needs remote access. Further, restrict the permissions of each account to only have access to the systems that they support. Users of a jump host should not be able to bring files and or tools into the system.

Finally, provide visibility to the system with real-time monitoring for threats and vulnerabilities. This will reduce the potential dwell time should the systems be compromised and will enable cybersecurity managers to react quickly to any potential threats that come to their attention. But don't depend simply on having the technology in place; make sure people are trained to monitor the systems appropriately.

Supply chain and device selection criteria

When choosing components to secure ICS/OT infrastructures, look for products that are secure by design and offer full lifecycle vulnerability management. Ensure the firmware from chosen vendors is authentic, hasn't been compromised and has upgradable security that offers protection from new threats as they come up.

Any components added to the system should have the ability to use multifactor authentication to support role-based access controls. The use of a separate OT-specific active directory server can make managing these accounts easier. Set specific accounts for the people who need access and be sure to disable accounts once they are no longer needed. The fewer open accounts, the fewer opportunities attackers have to enter the system.

Check to see which industry standards the vendor adheres to in its product development and determine if they are stringent enough to support the necessary applications. Vendors should also be able to show they maintain a secure development lifecycle (SDLC) for their products and have that SDLC validated by an independent organization.

Evolving threats

It's important to note that protecting ICS/OT systems is not a static operation. Once done, security procedures and protocols must be monitored and updated regularly to stay current on potential emerging threats. Consistently evaluate people, processes and technology to make sure they are familiar with/reflect the most recent security training possible. Cybersecurity for ICS/OT systems should be centralized and automated as much as possible to eliminate the possibility of human error from the equation. Lastly, a team should be consistently monitoring, analyzing, assessing and adapting new environments as they become available.

Eaton recommends creating a specific schedule for monitoring cybersecurity details as seen in **Figure 1. Cybersecurity lifecycle maintenance.**

Yearly (every 15 months)

- Asset inventory and baseline generation
- Network topology and drawing review
- Vulnerability assessment

Monthly (every 35 days)

- Pre-update configuration baseline
- Backup system assets
- Vulnerability review (vendor and public)
- Deploy patches and firmware updates
- Deploy "security" updates (e.g. AV definitions)
- Review access control lists
- Review user accounts and controls
- Post-update configuration baseline

Bi-weekly

- Logging review and analysis
- Time synchronization verification

Other considerations

- Redundancy, resilience and failure modes
- Overall system health check

Cybersecurity at Eaton

The assessment will also provide visibility to attackers' ability to Cybersecurity design principles at Eaton form the foundation for secure development of all our intelligent products, and our SDLC process integrates security at every phase of the product, from its inception to deployment and maintenance phases.

Eaton is a one-stop shop for OT cybersecurity needs. From assessment services to personnel training, we can make OT systems as secure as possible from beginning to end.

Frequently asked questions

If our IT department handles the security of the network and the workstations, is this something we need to address as a facilities team?

It is important to ensure all risks are addressed. Do not make assumptions about the protections for ICS/OT equipment and environments. It is important to have the IT department aligned with operational and cybersecurity objectives and understand the nature and criticality of the system and its assets.

Running standard IT tools in an OT environment can cause operational and availability issues and may not account for the risks on the OT assets (as most of these tools are not designed for the embedded proprietary devices on these networks).

Can we use the same vendor our IT team uses for assessments and penetration testing to secure our OT networks?

It's important that an OT cybersecurity vendor fully understands the systems they are working with and what the potential effects of creating downtime are. In general, it is better practice to hire vendors with OT cybersecurity specialization. If a current IT vendor is OT and ICS aware and has protocols in place to do such an assessment, it is possible to use the same vendor. Ensure they understand the system and have a plan to execute safely.

If we have a limited staff to dedicate to cybersecurity, what should we prioritize when we maintain our OT systems?

Prioritize developing an accurate asset inventory of the system. After all, companies can only protect what they know they have. Second, prioritize a vulnerability assessment to discover what potential vulnerabilities are available to malicious outsiders so they can be closed, especially those in the most critical systems. It's also important to have a disaster recovery plan in place should the system need to be restored for any reason, whether cyberattack, natural disaster, fire, etc. No matter what happens, it's important to have a clear path ahead to recovery with defined stakeholders, triggering events, actions and reporting. Within your organization, look to collaborate with different teams to pool and augment resources and skillsets (e.g., IT and ICS/OT teams). Finally, consider 24/7 monitoring to assist with asset inventory, vulnerability management, configuration changes and malicious traffic.

For the ICS assets that are being newly installed or upgraded, are there well-defined, mandatory cybersecurity specifications for connectivity?

There are some general ICS cybersecurity standards and best practices that can be referenced. There are a number of defined standards that may or may not be "mandatory" based on the global area and market segment. In general, the IEC 62443 series of standards and NIST Cybersecurity Framework (CSF) are good reference standards for ICS/OT systems. Whether a new or upgraded system, it is critical to understand the core system functions and critical requirements (e.g., real-time availability, safety, etc.), dataflows, trust zones and overall distribution of assets. From there, network- and asset-level controls can be applied.

How can I improve OT security with vulnerability management?

Threat and vulnerability management for any network is critical. Start with a comprehensive asset inventory and understanding of the architecture, dataflows, assets, system functions, network threats, weaknesses and vulnerabilities that can be analyzed and prioritized to minimize overall risks to data and system availability. For any system (IT, ICS, OT, IIoT), vulnerabilities should be reviewed and addressed monthly (at a minimum). Addressing them could mean patching/updating firmware, implementing compensating controls (e.g., disabling a service, adding a firewall, tightening access controls, etc.) or increasing monitoring for cases where it is not possible or practical to patch or update immediately.

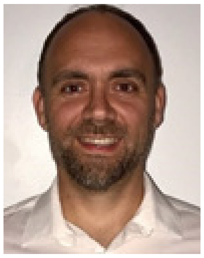
Organizations often have several ICS/OT systems with different architectures, vendor products and even teams responsible for maintaining them. How can you drive consistent application of security across these sites?

This is very common, especially in large organizations. The best approach is to offer standard ICS/OT-focused awareness and technical training to all teams, where basic cybersecurity concepts and objectives can begin to be normalized. Then start collaborating internally to come up with standardized reference architectures and policies and processes to maintain these systems. At a high level, some basic tenets can be applied to almost all systems (e.g., a maintenance schedule that includes a monthly vulnerability review).

References

1 Mandiant M-Trends Special Report, Mandiant, 2022 15671

Meet the author



Anthony Ciccozzi,
P.E., GICSP

Anthony provides internal consulting for cybersecurity as it relates to embedded systems, distributed energy systems, communication and control applications and various standards/frameworks, including NERC CIP, IEEC 62443, IEEE 1686 and the NIST Risk Management Framework (RMF). He has over 20 years of experience developing solutions and delivering services for the utility, oil and gas, rail/transit and mining industries. Anthony is a Global Industrial Cybersecurity Professional (GICSP) from the SANS institute, holds a Project Management Professional (PMP) certification from PMI and is a licensed Professional Engineer (PE) in New York.

For more information visit
Eaton.com/Cybersecurity

Learn more about our services at
Eaton.com/CybersecurityServices

EATON
Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP083046EN / GG
June 2022

Disclaimer This article is for educational purposes only. Eaton disclaims any liability for the content of this guide.

Follow us on social media to get the latest product and support information.