Thought leadership
White paper

Integrating Cybersecurity into Industrial Control System Lifecycle Maintenance

Anthony Ciccozzi
Lead Cybersecurity Engineer, PE, GICSP, PMP.

Overview

Cybersecurity risks to connected systems have never been greater, as malicious threat actors look to exploit system vulnerabilities (weaknesses and gaps in protection). These vulnerabilities often exist on assets with the least security oversight —electrical breakers, backup generators, industrial gateways, elevators, automatic transfer switches, fire protection systems, pumps, etc. Ensuring the security of these "soft targets" is critical to maintaining the safety and uptime of your business operations and employees. A vulnerability in these infrastructure devices not only puts the availability and safety of that piece of equipment at risk, but provides the potential of unauthorized access to the IT network (email, customer and personnel info, financial records, etc.).

Technology is driving increased connectivity, distribution and overall capability into Industrial Control System (ICS) and Operational Technology (OT) networks. These networks often have specific real-time functions with stringent availability, performance and safety requirements. Domain expertise to properly engineer and maintain these systems requires a multi-discipline comprehensive understanding of these requirements and additional items, including cybersecurity, failure modes and asset reliability.

A full lifecycle maintenance program that integrates consideration for availability, reliability, performance and cybersecurity has become a necessity. Couple this with resource and budget limitations, and the need for lifecycle maintenance programs becomes more apparent. It is often necessary to partner with internal teams and external vendors to provide the required collective expertise.

Cybersecurity considerations for Industrial Control Systems

Addressing cybersecurity on ICS/OT networks requires comprehensive cross-functional consideration and typically is not the responsibility of any single discipline or entity within an organization, something that results in distributed or ambiguous ownership. Specific real-time consideration of the availability, performance, safety and other needs of the system need to be considered. Often, given the embedded nature of components in these networks, typical IT methods, tools and policies are either not effective or cause damage to a system. Scanning a system of laptops and workstations with a tool designed for these assets is different than scanning a network of controllers and other embedded devices that are less complex and lack processing capabilities. The impact to these systems can range from a device failure or process disruption to random data dumped onto a network.

Case studies — Cybersecurity cannot be decoupled from overall maintenance

There are many types of ICS networks serving different functions across several markets. In the most general sense, ICS networks are a collection of vendors proprietary and Commercial Off the Shelf (COTS) devices interconnected and distributed to meet common availability, performance, safety and security objectives. It is difficult to decouple some system functions from each other and cybersecurity.

Powering Business Worldwide

Consider a few case studies published by the North American Electric Reliability Corporation (NERC). NERC issued a lesson learned report[1] describing several cases where Automatic Transfer Switch (ATS), Universal Power Supply (UPS) and other power system component failures caused several issues. In one case, network traffic to a primary control center was impacted due to an overcurrent event that took firewalls offline. While the result was a loss of communication, the root cause was attributed to a series of cascading issues in a power distribution units (PDUs), ATSs and UPSs leading to firewall de-energization.

While the root cause was not attributable to a cybersecurity incident, could an attacker exploit this scenario? Should this failure be considered more of a cybersecurity vulnerability or a general system weakness?

In another NERC lessons learned report[2], issues related to firewall vulnerabilities were analyzed. Vulnerabilities, weak access controls and inadequate firewall rules were attributed to a Denial of Service (DoS) attack. Mitigating these risks, the report concludes, could have been achieved with effective basic cybersecurity hygiene and maintenance practices, including secure architecture (segmentation and boundary defenses), secure maintenance (vulnerability management), and testing. Often, the existence of a technology—in this case a firewall, but it could be antivirus (AV), strong password and account controls, etc.—gives a false sense of the cybersecurity by masking real underlying risks. The NERC[2] and Ukrainian[3] examples demonstrate the existence of a technology alone is not adequate. Proper design, implementation and maintenance are required. In the case of the firewall in the NERC report, vulnerability management to identify and address vulnerabilities, secure configuration audits to ensure proper firewall rules were in place and periodic assessments to verify these activities would have likely prevented the attack

Security maintenance considerations

There are several industry standards[6 7 8], best practices[9 10] and vendor recommendations[11 12] that provide guidance for secure ICS design, deployment and maintenance. These all focus on the concept of defense in-depth, which layers defenses to progressively reduce cybersecurity risk. By improving the ability of a system to identify, detect, protect, respond and recover, risks are reduced. What can be lost in all the ICS standards, guidelines and defense in- depth is the need for cybersecurity and system-aware people, process and technology. As was shown in the NERC firewall vulnerability case study[2], more diligence was required than just the existence of the technology (e.g., firewall).

The following common ICS vulnerabilities could all be addressed with a comprehensive lifecycle maintenance program:

- Inaccurate inventories
- Poor vulnerability and threat management
- Poor configuration management
- Missing backups
- Weak and out-of-date access controls
- Inadequate security configurations

An effective cybersecurity maintenance program includes periodic activities on a biweekly, monthly and yearly schedule as in **Figure 1**.

These activities align with several industry-standard best practice frameworks. Notice, in addition to the cybersecurity benefits, the benefits of overall system maintenance include:

- Updated drawings
- Asset management
- Configuration management
- Backup and recovery
- Time synchronization
- Logging and log review

With proper planning and execution, cybersecurity maintenance activities can be performed on a running system (e.g., asset inventory, network monitoring, configuration audits and backup generation). However, the additional activities listed in **Figure 1** could—and should—be performed during a system maintenance outage. Verifying redundancy in controllers and networking and verifying the power schemes will reduce not only cybersecurity-related risks, but risks to availability and performance. Think of the value to the NERC firewall outage[1].

Full lifecycle cybersecurity services from ICS experts

Augmenting a lifecycle maintenance program with partners with ICS-specific domain expertise that includes cybersecurity is often a cost-effective way to reduce overall risk and maximize availability and reliability. Cybersecurity consideration should be developed based on industry standards and best practices, including NIST Cybersecurity Framework (CSF), ICS CERT, IEC 624433-3, Center for Internet Security (CIS) Critical Security Controls (CSCs) and device-specific certifications including IEC 62443-4-2 and UL-2900.

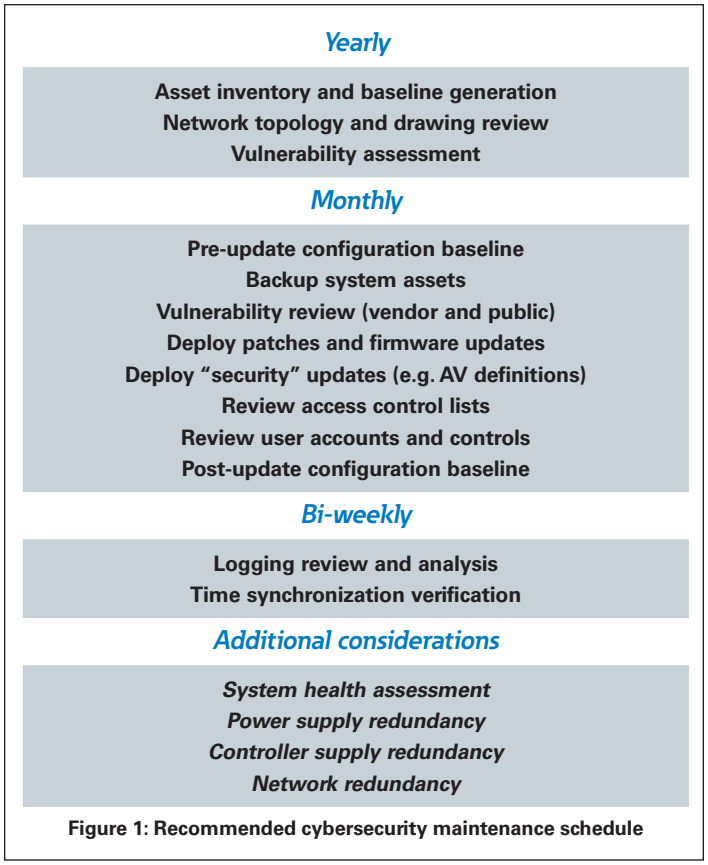

Figure 1: Recommended cybersecurity maintenance schedule

Startup and commissioning

A cybersecurity-focused commissioning should be performed when new devices and networks are modified to ensure safe, secure and reliable operation while not creating a vulnerability to the broader network. It is critical to ensure any default controls or accounts used to facilitate commissioning are properly applied and the system is adequately hardened. A commissioning service also provides baseline traffic captures and artifacts that can serve as the foundation of a complete cybersecurity maintenance program.

For new construction, the ideal time to perform cybersecurity commissioning services is during the equipment commissioning process. This will provide an accurate asset inventory and the network map necessary for building a robust ICS cybersecurity program and establishing the integrity of the OT operations.

Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) should not only consider overall system function, redundancy and specific failure mode testing, but also specific consideration for cybersecurity and overall maintenance. The following should be addressed and collected during FAT, SAT and commissioning:

- Asset inventory
- Secure configurations
- Baseline traffic captures
- Fully patched and updated assets (vulnerability management)
- Change default access controls
- Disable unused physical and logical ports

Generating and performing these activities provides a starting point and a reference baseline for future maintenance.

Cybersecurity assessment

Done properly, and with full consideration of risks to system availability and safety, a broad-based assessment of a system's overall security profile can be performed. A full assessment of a system's attack surface, vulnerabilities and maintenance practices should be performed yearly at a minimum. This type of assessment not only evaluates the security posture of a system, but provides an evaluation of its maintenance practices.

Hardening

Hardening systems includes addressing identified gaps, weaknesses and vulnerabilities. Cybersecurity experts will present options to remediate or mitigate identified cybersecurity risks related to people, process and technology, which include:

- Delivering personnel training
- Developing and revising processes
- Applying patches and system hardening
- Applying firewall rules
- Changing system access controls (update passwords, disable/remove unused accounts, etc.)

Industrial Network Defense

A service focusing on network boundaries offers several benefits. Network boundary defenses provide asset visibility, enforce functional isolation, traffic restrictions, secure remote access and general protection to prohibit unauthorized access to critical assets. Boundary defenses can be readily deployed with minimal disruption to existing operations and network architecture.

This service focuses on protecting vulnerable equipment and systems that lack modern cybersecurity features. It's ideal for old, out-of-date equipment that is no longer supported and non-air gapped and shared networks, as it adds compliance for NIST CSF, IEC-62443 and NERC CIP.

Personnel training

TCybersecurity awareness and training for your technical and non-technical employees on industry standards, best practices, and your specific policies and procedures is important. Post-incident analysis of cybersecurity events typically reveals the initial attack vector opening was accidentally created by an insider who was not properly trained. This service helps avoid this situation by covering a wide range of topics, from temporarily opening network ports to requiring vendors to follow specific technology hygiene practices.

Secure maintenance and monitoring

The continuous maintenance and real-time monitoring of an ICS/OT network is critical. This involves real-time asset identification and vulnerability, anomalous activity and rogue device detection. Configurable alerting, logging and alarming can be configured for centralized collection, correlation and alerting from all asset types for a comprehensive view of system operation and potential intrusions, risks and threats.

Consulting

Access to a vendor's domain expertise is invaluable when integrating cybersecurity and system operations. Again, considering the NERC firewall example [1], IT staff or even the ICS staff responsible for the asset may not have the expertise or the organizational structure to fully consider the deployment, power requirements and potential fault scenarios. A power management expert has the expertise to help identify and advise on a fully integrated solution. Consulting engagements can almost entirely be defined by the customer and can range from consultation on overall network architecture design and refinement and policy creation or curation to technical assessment or maintenance.

References

1 Loss of monitoring or control capability due to power supply failure

2 Risks posed by firewall firmware vulnerabilities

3 E-ISAC Analysis of the Cyber Attack on the Ukrainian Power Grid

4 Dragos 2019 Year in Review: Lessons Learned from the Front Lines of ICS Cybersecurity

5 Analysis of the Cyber Attack on the Ukrainian Power Grid

6 NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security

7 ICS-CERT References and Resources

8 Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016

9 Center for Internet Security (CIS) Controls (V7.0)

10 Center for Internet Security (CIS) Industrial Control System (ICS) Companion Guide

11 Cybersecurity considerations for electrical distributions systems

12 Security best practices checklist reminder

Author

Anthony is an ICS cybersecurity specialist responsible for leading cybersecurity product assessments in the Eaton Secure Development Lifecycle (SDLC). He provides internal consulting for cybersecurity as it relates to embedded systems, distributed energy systems, communication and control applications, and UL, NERC CIP, and NIST Risk Management Framework (RMF) compliance programs. Anthony has experience integrating cybersecurity technologies, controls, and best practices into hardware, software, and network development. This experience includes over 13 years developing solutions for the utility industry including smart grid, generation, transmission, and distribution solutions.

Learn more at:
Eaton.com/cybersecurityservices

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

Printed in USA
Publication No. WP027017EN / GG
June 2020

Powering Business Worldwide

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