Best Practices in ICS Security for System Operators

Introduction

Industrial automation and control systems have become increasingly connected to internal and external networks. This exposure has resulted in a number of new threat vectors, and we have seen the frequency of cyber attacks grow significantly over the last few years. Given the complexity of industrial control systems (ICS), and the serious impact of downtime in these environments, there are often very limited opportunities to patch vulnerable systems. The challenge of securing these systems calls for a structured and comprehensive approach. In this paper we provide a starting point with a detailed set of security best practices for ICS.

Assess risks and consequences

The first crucial step for automation operators is to fully comprehend vulnerabilities and how each one affects operations.

- Understand the risks the organization faces and how likely the occurrence of each one is in each critical system
- Consider the deterrents in place to protect against each risk, and assess the consequences of those safeguards being by-passed
- Consider a variety of possible outcomes and differentiate between a vulnerability that will result in a minor inconvenience and a flaw that will cause downtime, revenue loss, or worse consequences

This will help system operators prioritize their security plan and budget.

The U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) defines cyber threats as anyone attempting to access control systems or networks who lack proper authorization to do so. Sources behind these threats can include disgruntled individuals, hostile governments, terrorist organizations, or any other intruder with malicious intent. ICS-CERT urges organizations to implement rigorous protection around industrial control systems.

Regulations

Regulatory compliance mandates are an important consideration when developing a security plan. There are regulations across several industries running critical infrastructure, with one example being NERC CIP for the power industry. NERC CIP standards are extensive, and organizations failing to comply can be subject to significant penalties. During security assessments, it is essential to consider industry-specific security regulations and standards in order to ensure compliance and reduce the risk of increased expenditures associated with achieving compliance in the future. Start with the ISA/IEC-62443, a series of standards, technical reports, and related information that define procedures for implementing electronically secure, industrial automation and control systems. The guidance applies to end-users (i.e., asset owners), system integrators, security practitioners, and control systems manufacturers.

The same ICS security solution will not work for every organization, but there is a process for establishing, designing, and implementing an industry best-practices solution that makes sense for a system operator's organization and current facilities. Find the right expertise to help determine the roadmap to compliance and avoid errors caused when security is viewed as an after-thought addition.

The guidance applies to end-users, system integrators, security practitioners, and control systems manufacturers.

Expertise

Utilizing either an internal security group or contracting a knowledgable third-party to perform a thorough security assessment and gap analysis will provide system operators with a current view of their security landscape. This allows organizations to use essential information to establish security objectives, goals, and implementation strategies. Specialists should work through the processes, networks, and equipment to identify, quantify, and prioritize potential vulnerabilities. The team appointed should develop a prioritized mitigation plan and a practical approach to address the risk. They will test the network, facility, and devices to identify vulnerabilities. Whether running an oil refinery, a smart grid network, or a municipal water system, system operators must find individuals with the right expertise and experience to advise and protect the operation from the threat of cyber attack.

Develop objectives and goals

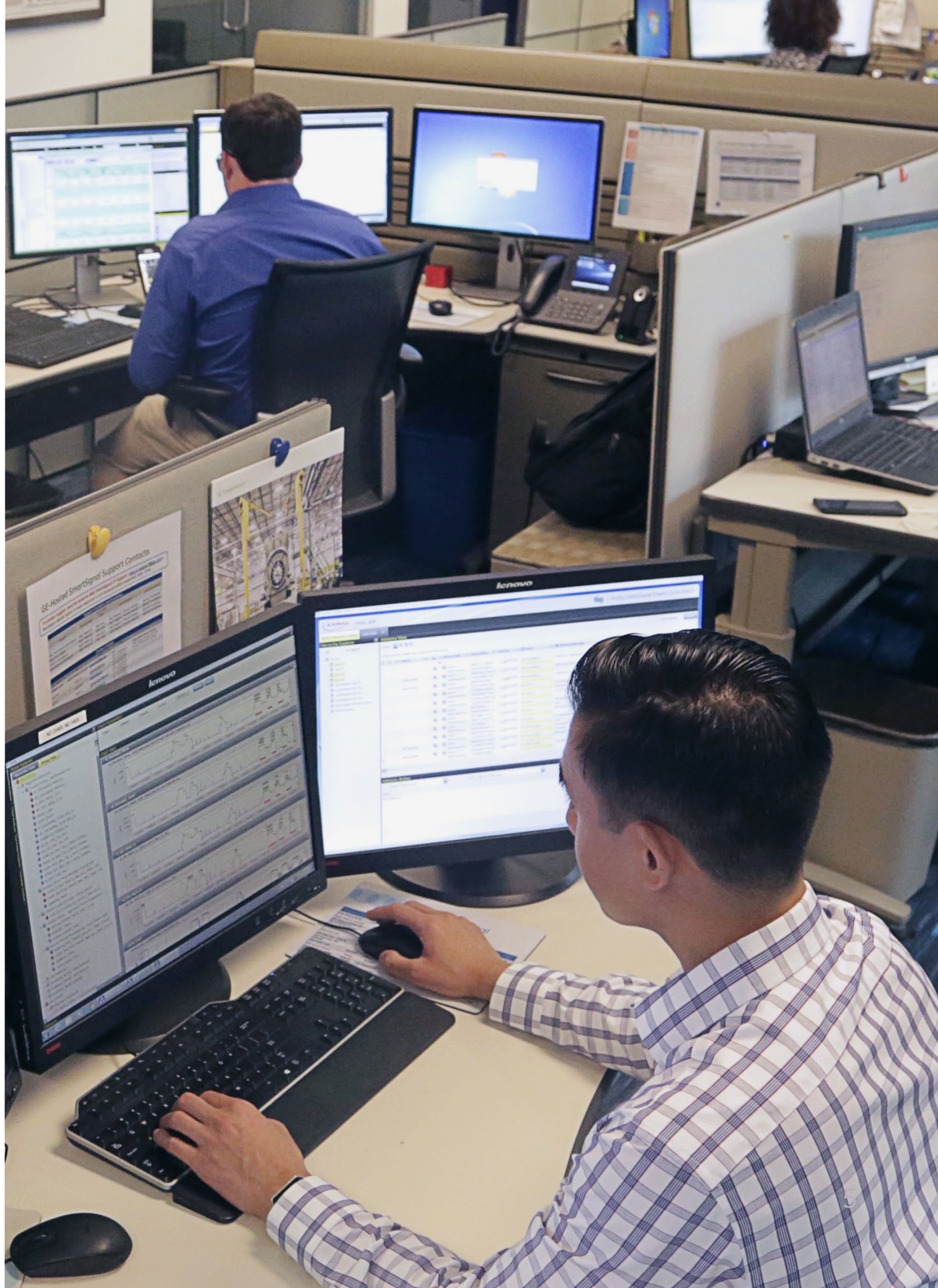
After completing the security assessment and gathering the information necessary to understand the threat landscape, set a security foundation with best practices, policies, and strategies. System operators will have identified the security gaps, prioritized their highest risk areas based on consequences, and set objectives and goals to address the most important systems with the biggest, most impactful, and immediate risks.

ICS security policy

Include the right individuals within the team to help with planning, deploying, testing, and refining the implementation. This group will consist of representatives with both technical and business knowledge of the industry. If choosing to include a third-party organization, it must have a deep understanding of the industry's regulatory compliance mandates, the system operator's organizational and internal objectives, and its facilities.

Be sure to develop policies and procedures specific to ICS, which is separate and distinct from the system operator's IT security policies and procedures. While they can refer back to the corporate IT security documents, ICS policies and procedures should include information to help the entire security staff clearly understand the expectations and responsibilities of each team and member, and how their responsibilities diverge.

In addition to responsibilities and roles, the ICS security policy document should cover consequences for team members who do not comply, as well as specific organizational policies, such as how system operators choose to handle antivirus software, portable media, remote access, etc. Provide a comprehensive policy to address people, process, and technology risks while creating a plan for long-term enforcement.



Policy and procedure vulnerabilities

In June 2011, the National Institute of Standards and Technology, or NIST, published a guide for organizations that utilize industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), as well as programmable logic controllers (PLC). The guide provided several recommendations to help improve the security posture of these control system configurations.

For one, NIST notes that vulnerabilities in ICS are often exploited due to inadequate policies or the lack of specific policies for control system security.

Another area is training. Many organizations lack formal training to educate employees on security polices and procedures. Research from several sources continues to show that the majority of security breaches are due to human error. NIST recommends a formal security training and awareness program to educate employees on policies, procedures, and expectations.

Additionally, NIST points out that control engineers have traditionally received very little security training. They also note that, until recent years, device manufacturers have not built security features into products.

Both of which introduce significant risk to organizations. As part of the training, the guide advocates specific security procedures to be implemented to train staff for the industrial control systems. Staff responsible for enforcing security should also be held accountable for administering documented security policies.

Another key to improving the security posture of organizations is to implement independent review and audit of ICS. The audit should examine systems' records and activities to ensure compliance with ICS security and procedures. It should also detect ICS breaches and offer recommended changes to improve system robustness.

Finally, NIST urges organizations to implement a disaster recovery plan, or DRP. Too many organizations lack a documented business continuity plan, which could lead to an extended period of downtime as well as production loss. Similarly, organizations need a documented process for controlling modifications to hardware, software, firmware, and documentation to protect ICS from "improper modifications before, during, and after system implementation." Failure to do so could lead to security missteps and create unnecessary risks.

Enforce security through the supply chain

To ensure all defined security goals have been met, the devices in the system operator's environment must adhere to the company's ICS policy, which aligns with the organization's overall security objectives and goals. A system operator's infrastructure is only as strong as its weakest device, in this case. Incorporating robustness and security certifications in your procurement process is a proven technique to drive change in the supply chain.

System security

Devices attacked in the field can cause a host of problems, including lost revenue during downtime, increased downtime in the case of patching for bug fixes, and damage to a system operator's reputation. While device vulnerabilities that are exploited are not necessarily the operator's fault, it is still the operator that will bear the real and potentially enormous cost of a successful cyber attack. Manufacturer devices must be made secure and robust before deployment in order to reduce the risk of an attack being introduced through them. Using the security policy ensure system devices support the desired security frameworks the organization has put into place.

Third-parties

System operators need to make sure all of their staff, contractors, and consulting organizations with access to the infrastructure are fully aware of the ICS security policy. In addition, have senior management present the information to employees, consultants, and partners with access to the ICS to ensure full buy-in, and continue regular communications updates to ensure security stays top-of-mind.

Next, train staff on information relevant to their specific roles, explaining how to apply security and where to go if they suspect the infrastructure has been compromised, or if a specific device has been affected. Tailor training to fit different roles (engineering, executives, visitors, contractors, etc.), focusing on how to securely place a supply order when presenting to office administrators, for example, and tailoring topics and sessions for managers when working with executives.

Manufacturers

Finally, in addition to the current security of devices, manufacturer security policies are also important. The manufacturer should provide alternative mitigation suggestions for use until patches are available and can be applied. Some operators cannot apply patches right away, but may be able to apply signatures or restrict access to a system they know to be vulnerable. Patch performance must be at the discretion and within the control of the system operator. While the system operator can determine when to patch systems, it must still rely on the mitigation patch from the manufacturer to ensure immediate protection. Poor patching procedures from the device manufacturer will leave the system operator vulnerable to potentially extensive, costly exposure.

Certification

To ensure manufacturers are providing system operators with secure devices with strict procurement and purchasing processes, work with manufacturers that offer certified, globally-recognized industrial process automation, control, and safety systems. Finally, opt for third-party certifications whenever possible to ensure vendors conform to the organization's desired level of stringent security objectives. This will reduce operator costs associated with comparing solution claims and risk. It will also ensure systems meet current and emerging international cyber security and government regulations.

Risk mitigation designed specifically for ICS

Many automation operators invest a significant amount in IT infrastructure mitigation tools, but they overlook the same level of specificity when it comes to ICS protection. Traditional IT solutions will not reduce the risk of ICS attack; however, utilizing devices explicitly designed to protect the critical infrastructure can greatly reduce the risk of these vulnerabilities.

Segmentation

Remember to segment the network by user roles—users with similar authority and requirements should be segmented together because electronic connections between network segments populated by users and devices with dissimilar roles or authority can form a path for attack. Defining user roles and enforcing the principle of least privilege is an essential tool for limiting the insider threat and restricting (or at least slowing down) attack propagation.

Authentication

Like physical access, such as an access control device through which each employee is given a certain code to reach certain areas of a locked building, the same concept applies to logical access to critical ICS resources. Identify who should have access to what resources, what privileges they should have, and how it should be enforced. Users need to be identified and authenticated. Once authenticated, users can then be allowed to perform certain functions based on their role (the same way the executive's code allows him or her through every door of the building but keeps employees out of sensitive areas like engineering source code libraries).

Patch management

In addition, operators may not have the configurability or capability to patch a publically released vulnerability quickly, which leaves the system exposed to a widely known issue—an invitation to trouble.
In order to reduce exposure, ICS-specific mitigation devices provide protection once enabled with the vulnerabilities solution, allowing for security coverage between when the vulnerability is identified and when the manufacturer releases the patch for operator implementation.

Look for ICS-specific mitigation devices that protect against newly found vulnerabilities within days of discovery, without the need to shut down operations to implement a patch. Reduce exposure to risk and protect brand equity with a comprehensive database of non-public (zero-day) industrial control vulnerabilities and profiles, and rule sets that address the complete vulnerability, not just the single exploit.

Establish strong corporate buy-in and governance

As an ICS operator, remain vigilant and monitor security and activity continuously. Look closely at anything that looks unusual. Implement solutions specific to operational protocols or environments for relevant visibility. Update signatures, install patches, and vigilantly enforce ICS security policy. Use commercially available traffic capturing tools that enable an accurate behavior baseline specific to your organization.

Review your system regularly to consider new security additions. For instance, intrusion detection systems on their own are not considered a strong enough defense, but with a firewall, could be part of a broader protection solution for the system operator's facilities.

Once an ICS security policy and plan has been established, get corporate buy-in. The number one issue facing operators when it comes to security is not a lack of technical knowledge, but corporate support and appropriate governance for implementation. Be part of the solution to establish a culture that emphasizes security from the top down. Without corporate dedication to ICS security starting at the C-level, it is difficult to create and maintain long-term goals, obtain required funding, and execute best practices.

Next, rally the troops. Gather the internal champions, technical experts, and decision makers the organization needs to have constantly involved in its security direction, and have them help with this effort. While it is not always possible to have a dedicated security team, it is important to have individuals with clearly defined roles and responsibilities who are aware of the security policy and direction.

Finally, consider outsourcing parts of ICS security to knowledgeable third parties to capitalize on their extensive expertise and objectivity. ICS security and its associated risks and vulner abilities are constantly and rapidly evolving, so ongoing monitoring is crucial. It's not something organizations can have employees working on for only a few hours a week; the consequences could potentially be dire if something is overlooked. Stay ahead of potential attacks by having a team constantly monitor for new vulnerabilities and exposures, compare the organization's current solution to what's newly available in the market, and keep the organization compliant and secure.

In conclusion

System operators face a dynamic challenge in keeping their systems secure. Implementing a set of best practices around assessing risks and consequences, developing objectives, enforcing security through the supply chain, utilizing mitigation devices designed for ICS, and establishing corporate buy-in will dramatically reduce the risks and costs of cyber attack.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital