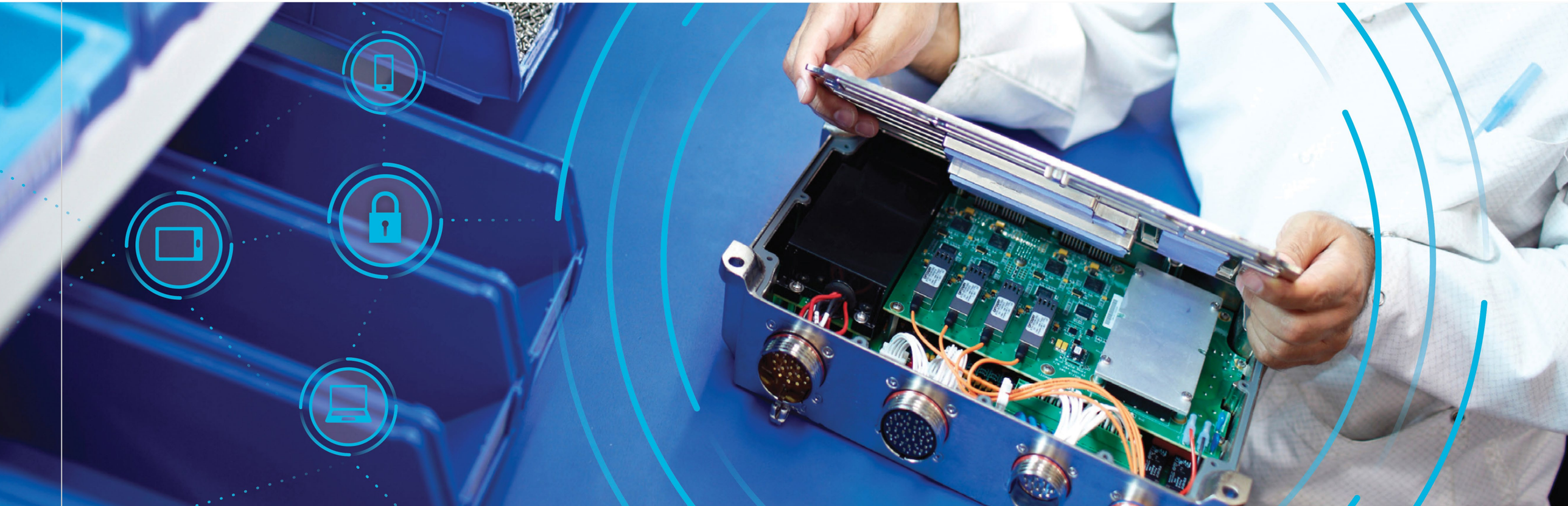
Best Practices in ICS Security for Device Manufacturers

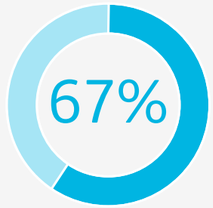


Introduction

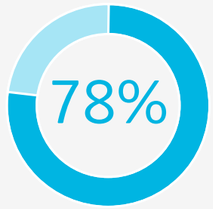
Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are used in industrial automation processes for critical infrastructure industries such as oil and gas, electric, power, medical, nuclear, chemical, and water. Historically, ICS and SCADA systems have been isolated from the traditional IT network and subsequently protected from most threats. However, as the rapid growth of interconnectivity among systems continues (i.e. Internet of Things, Industrial Internet), ICS and SCADA systems are now accessible and becoming high priority targets for hackers. As a result, virus and hacker attack frequency is also increasing. While the industry has made positive strides to improve disclosure of these vulnerabilities, there is much more work to be done. Because industrial control systems are incredibly complex and operational downtime has significant impact, powering off to patch a vulnerability is simply not an option, and securing these systems can sometimes be a monumental task. It is increasingly important that device manufacturers find ways to reduce the number of vulnerabilities that reach the field.

Critical infrastructure operators have invested significant resources into implementing secure IT policies and procedures. However, the rapidly changing ICS threat landscape has created a vital need for ICS-focused security. More than ever, device manufacturers of critical infrastructure must take action to improve the robustness and security of their devices. These improvements will reduce liability from cyber attacks, improve customer retention, and protect brand equity for device manufacturers and their customers. This whitepaper aims to identify best practices for ICS device manufacturers to ensure the development of secure, robust devices.

The thread of cyber attacks are real



of companies with critical infrastructure suffered at least one attack in the past 12 months[1]



expect a successful exploit of their ICS/SCADA systems within the next two years[1]

79,790 security incidents per company across **61** countries in 2014[2]

66% of organizations are not ready to address security issues for OT[3]

91% of power generation organizations have experienced a cyber attack[4]

159 vulnerabilities reported, with most of them impacting systems used in the energy sector[4]

79 energy incidents were reported[4]

38% of reported attacks are against power and water[4]

14 water incidents were reported[4]

Assess your own risks and consequences

In order to properly design, develop, and implement strategic best practices for security, it is essential that manufacturers of critical infrastructure understand the organization's current security capabilities and the effect the threat landscape may have on its products. Device manufacturers should not only aim to understand the risks the organization faces, but also aim to determine the potential consequences of an attack. They must perform corporate-wide assessments of training and development policies in addition to the specific assessment of devices and development teams. These assessments will allow for prioritization of the most vulnerable targets with the greatest potential harmful consequences and, in turn, enable device manufacturers to address their most vital areas first. The ultimate goal is to design a robust and secure device or system by implementing security throughout the entire development process, rather than approaching security as a separate test requirement at the end of design.

In addition to assessing the specific threat landscape, it is also important to ensure that device manufacturers consider compliance to applicable mandates established by regulatory bodies. Understanding the gaps between the current security posture of the device manufacturer's organization, applicable regulatory mandates, and the future direction of regulations enables compliance and allows for sufficient planning and prioritization to ensure future compliance.

Expertise

Even seemingly innocent tasks in an IT environment could spell disaster in an ICS. For example, pinging devices to see which ones are running, a common occurrence on an IT network, could cause an ICS system controller to shut down entirely.

ICS security specialists are required for establishing, designing, and implementing an industry best-practices solution that makes sense for your organization and development processes. Find the right expertise to help determine the roadmap that will improve your product development process to help you achieve compliance and avoid critical errors caused when security is viewed as an afterthought.

Performing a thorough security assessment and gap analysis, whether internally or with a knowledgeable third party, will provide a solid baseline that allows you to establish security objectives, goals, and implementation strategies. Specialists should work through your processes, networks, and equipment to identify, quantify, and prioritize potential vulnerabilities.

The team you appoint should develop a prioritized mitigation plan and a practical approach to address risks. They will test your process, facility, and devices to identify vulnerabilities. Whether manufacturing embedded devices, host devices, control applications, or network components, your organization needs expert solutions to help ensure the development of highly secure, quality products with low risk of vulnerability exposure.

Understand your customers' security needs

Device manufacturers need to stay on top of the security policy and compliance needs of their customers in addition to their own security issues.

The North American Electric Reliability Corporation (NERC) is a not-for-profit organization tasked with ensuring bulk power system reliability in North America. Overseen by the Federal Energy Regulatory Commission (FERC), NERC develops and enforces reliability standards, annually assesses seasonal and long-term reliability, and monitors the bulk power system. NERC CIP regulations are designed to govern customers of the device manufacturers. If it is not demonstrated that the organization's devices can meet those regulatory requirements, customers will go elsewhere. For instance, if an operator's security policy states that its system requires a periodic password change, and within its system is a device with a design that does not support such a policy, the operator needs to spend significant effort to create a workaround or perhaps review additional device vendors to achieve compliance.

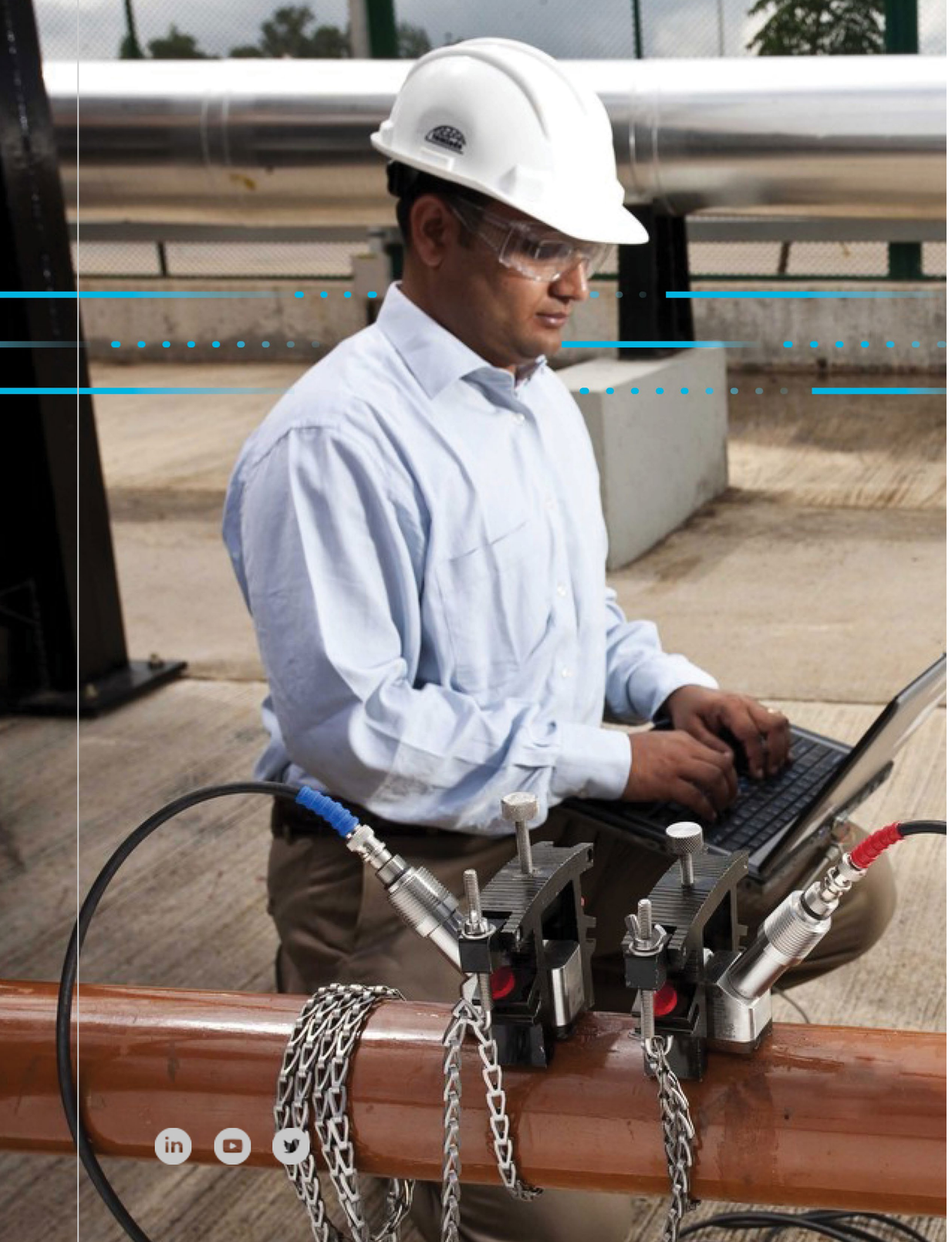
As a manufacturer, staying on top of the policies and regulations that apply to your customers will ensure they remain compliant and remain a customer. Otherwise, they will understandably need to look elsewhere.

In addition to device and manufacturing assessments, personnel must also be educated, tested, and certified in order to achieve compliance so that the manufacturer's customers (automation operators) will be successful in achieving compliance. Without device compliance, organizational compliance is not possible.

One way to ensure that you stay ahead of the curve in terms of meeting all of your customers' regulatory needs is to improve security awareness and expertise at all levels of your organization. Dedicating resources to improve staffing, training, and planning around cyber security can actually improve R&D efficiencies by minimizing redesigns and bug fixes early in a product's life cycle, and by facilitating industry compliance and certification efforts. While cyber security is often seen as overhead, it can actually help you better address security concerns for current and prospective customers, help you bring products to market faster, protect your customers' brands, and ensure that you run your business proactively rather than responding to external events.

NERC CIP Reliability Standards

- **CIP-002-1** Critical Cyber Asset Identification
- **CIP-003-1** Security Management Controls
- **CIP-004-1** Personnel & Training
- **CIP-005-1** Electronic Security Perimeters
- **CIP-006-1** Physical Security of Critical Cyber Assets
- **CIP-007-1** Systems Security Management
- **CIP-008-1** Incident Reporting & Response Planning
- **CIP-009-1** Recovery Plans for Critical Cyber Assets
- **CIP-010-1** Cyber Security—Configuration Change Management & Vulnerability Assessments



Certification

Certification will establish a benchmark for the secure development of the applications, devices, and systems found in critical infrastructure. The certification process presents device manufacturers with an independently verified result to communicate their product robustness and security to customers while providing control systems operators with complete, accurate, and trustworthy information about the network security and resilience of their deployed products. This process of certification eliminates gaps between customer requirements and manufacturer development. Some operators require independent verifications or certifications of devices and practices to ensure security compliance. Undergoing these procedures can align your organization with these requirements and set you apart from the competition by demonstrating your commitment to ensuring the consistent development of secure products. By understanding operators' needs and meeting compliance regulations to ensure you are developing products that fit their requirements and expectations, manufacturers can reduce design costs and build long-term customer relationships.

According to DarkReading.com, the U.S. Department of Homeland Security's ICS-CERT has been regularly issuing vulnerability advisories for SCADA products. Vendors have increasingly been issuing patches, but the easily exploitable design flaws inherent in many products remain.

Some renowned SCADA security experts contend that the current process of reporting bugs, patching bugs, and issuing alerts via ICS-CERT falls short. The bigger ICS/SCADA systems that control power plants or chemical plants are not typically the subject of ICS vulnerability alerts, and most vendors still aren't fixing features in their products that were created prior to the networked environment, or that just don't factor in security.

But ICS-CERT has been lauded for helping raise awareness of security problems in the systems and software that run power plants, and for the other services it provides to the ICS industry, including incident response and free tools.

Rigorously test

Once you have conducted an internal assessment and gained a thorough understanding of your customers' security and compliance requirements, focus on your organization's design and engineering processes. Continually implement practices to ensure that you fulfill the required compliance set forth by customers throughout product development. Make certain your source code is free of bugs and your source code repositories are secure. Continuously conduct internal testing at various stages of development—especially during the quality assurance cycles—to verify that security is solid throughout all steps.

You may use internal or external testing tools, but they must be foolproof and calibrated regularly. Use automated testing equipment armed with the most up to date tests, including newly emerging threats, to ensure robustness and security throughout the product development lifecycle, reduce development time, and minimize vulnerabilities released to the field.

Creating a platform for your internal testing, one that will find known and unknown vulnerabilities, will allow faults to be reproduced, isolated, and identified. These platforms —whether built in-house or obtained from a qualified third party—will monitor your entire system while your device is being tested and provide an analysis of an attack's impact on the whole system, not just the device under test. An important aspect of any test is the inclusion of the most recent types of threats to ensure your platform is being tested against real world risks.

Team security training

Employee training is vital to maintaining security. Secure systems can be made instantly vulnerable by the unwitting action of an unaware employee. Enforce the commitment to security and secure development practices designed to mitigate potential vulnerabilities by implementing a thorough training regiment for your team.

Design your security training program to meet individual needs and ensure that everyone thoroughly understands your organization's security requirements and plans. They must learn about common attacks and mitigation, how to use automated tools, and when to incorporate best security practices.

Developers must be properly trained on equipment—even if they insist they understand its use—in order to ensure maximum effectiveness. Individuals from every department must receive training from experts outlining security practices and policies relevant to their jobs.

Continue to provide employees with the in-depth knowledge and expertise required to stay up to speed on their role in developing secure products. Cyber security is constantly evolving. Discovering ways to efficiently and effectively apply good security practices and meet regulatory obligations at the same time is not easy. Outside organizations can often deliver the most effective and up-to-date information and training to minimize vulnerabilities in the workplace and ensure standards are continually met.

Establish corporate governance

Executives within the manufacturer's organization must drive commitment to security and lead the charge in calling for its implementation. With commitment from the top, a corporate security culture will breed effective results. Without a culture that emphasizes security from the C-level down, it is difficult to establish long-term goals and objectives, attain required funding, and implement solid security practices.

Device manufacturers need to recruit key internal champions, technical experts, and decision makers who are consistently involved in security decisions and direction setting. These people may not always have an active role day to day, but they must be active overall and have clearly defined roles and responsibilities.

Once the implementation has been completed and individuals have established their roles and responsibilities, it is important to constantly monitor for new vulnerabilities and exposures to stay well ahead of potential attacks. This makes it possible to implement any necessary changes before it's too late.

Because of the ever-changing threat landscape, it is important to maintain training and continuously assess internal security policies, as well as the required standards and compliance mandates of customers. These include security policies, procedures, configuration management, certification and accreditation, remediation plans, and security awareness training. This will identify any gaps in your program and provide detailed recommendations for improvements.

Conclusion

Device manufacturers for ICS face a dynamic challenge in keeping their devices and their customers' systems secure. Implementing a set of best practices around assessing risks and consequences, rigorous testing, team security training, certification, and establishing corporate buy-in will dramatically reduce the risks and costs of cyber attack.

Device manufacturers for ICS face a dynamic challenge in keeping their devices and their customers' systems secure.

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