SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

ICS Cybersecurity

FIELD MANUAL

Vol. 3

Author:
Dean Parsons
B.SC., GICSP, GRID, CISSP, GSLC, GCIA
Certified SANS Instructor |
CEO ICS Defense Force Inc. &
ICS Cybersecurity Leader

Contents

What to expect from these ICS security field manuals

If you are new to industrial control system (ICS) security, the SANS ICS Cybersecurity Field Manuals (volumes 1-3) will get you up to speed quickly. They provide long-lasting reference materials, free resources, and a training path in control system security for you and your teams. The three manuals consist of several sections and focus on different aspects of ICS cyber defense.

Introduction to Volume 3

ICS ATTACKS, CONSEQUENCES, AND RESPONSE

Industrial control system/operational technology (ICS/OT) facilities are seeing novel attack methods leading to incidents not commonly seen in enterprise IT networks. Traditional enterprise IT cyber attacks often focus on internal IT systems and can include compromise of digital information (including data deletion), business system configuration changes, business system downtime, information leakage, or data breaches. Compromises of ICSs are far different. ICS attacks can affect the safety of people and the environment. ICS incidents can cause physical changes which lead to catastrophic consequences. Consider, for example, the potential consequences of a compromised Safety Instrumented System (SIS) programmable logic control resulting in a failure to monitor and safely shut down an over-pressurized gas pipeline.

The ICS/OT security environment requires different technical and security management skills and technologies outside of traditional IT enterprise risk management and incident response. The mission and risk surfaces alone set ICS/OT incident response and risk management apart from traditional IT security.

This is why ICS-specific incident response processes and plans must be multi-team initiatives, created, exercised, and maintained by ICS-specific cyber skilled defenders. Patching and vulnerability management must also be adapted for ICS management.

Risk-based ICS vulnerability management

Many identified ICS vulnerabilities, if exploited, provide adversaries with capabilities similar to features inherent in control systems. ICS attacks have been observed where adversaries are "living off the land," i.e., abusing systems and industry protocols native in ICS environments to turn the control system against itself.

Living off the land was first observed in 2014 with the HAVEX[1] malware attack and more recently with the tailored CRASHOVERRIDE[2] ICS-specific framework targeting electric power grids. It is becoming a very common attack trait and will likely be well into the future.

In the 2021 Oldsmar water treatment facility cyber attack, no software or engineering equipment vulnerabilities where exploited. Rather, the attacker gained unauthorized access directly to the Human Machine Interface (HMI) from the Internet. The legitimate HMI application that runs the water treatment facility was used to manipulate water treatment operations that could have led to severe consequences. Using the HMI, the attacker increased the level of sodium hydroxide. That is the main ingredient in drain cleaner, which was changed from 100 parts per million to 11,100 parts per million. Very dangerous levels that would have been toxic for residents if it reached their homes. Human engineering operations staff noticed the incident and restored the processes to normal operations without incident.

1 https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-176-02A
2 https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

The Oldsmar event draws attention to the importance of vulnerability management and protecting ICSs, starting with their external services and Internet facing access. Common Open-Source Intelligence (OSINT) ICS exercises could be used to uncover vulnerabilities from the view of an Internet-based attack.[3]

Living off the land attacks have evolved even further in 2022 with the discovery of the PIPEDREAM malware. *"PIPEDREAM is a collection of utilities that includes tools for reconnaissance, manipulation, and disruption of PLCs [programmable logic controllers], as well as tools for intrusion operations against Windows devices. At the highest level, the PLC-related components of PIPEDREAM provide the adversary with an interface for manipulating the targeted devices. Tools in PIPEDREAM can scan for new devices, brute force passwords and sever connections, and crash the target device."*[4]

Career Development Opportunity - ICS456

SANS ICS456: Essentials for NERC Critical Infrastructure Protection course empowers students with knowledge of the what and how of the version 5/6/7 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities, provides multiple approaches for identifying and categorizing Bulk Electric Systems (BES) Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

Due to the number of legacy devices and software in ICSs, ICS patching is important, especially as the number of legacy devices and software grows. Yet, there is more to patching in ICSs than gathering and pushing packages. The best return on investment is a risk-based approach, considering the ICS risk surface compared to the IT risk surface.

3 https://www.sans.org/blog/sans-ics-site-visit-plan/
4 https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf

ICS patch prioritization: when and how

Patching prioritization in ICSs is different than in IT environments given the different risk surfaces and attack vectors unique to control system environments. Changes to an ICS's hardware, software, and configurations include but are not limited to device firmware updates, embedded hardware upgrades or replacements, setpoint changes, instrumentation calibrations, controller logic changes, and of course patching. However, patching is not solely about mitigating cybersecurity vulnerabilities. Engineering changes are also driven by system and command integrity enhancements, safety changes, and process improvement engineering feature sets.

Many ICS vendors release engineering system patches to fix bugs, thereby improving the stability of equipment and software, system safety, and operational reliability. ICS defenders should utilize scheduled engineering maintenance windows to push approved security patches once a subset have been evaluated and selected.

To prioritize ICS patching, ICS defenders should monitor and leverage the data in vendor security advisories. These advisories provide Common Vulnerability Scoring System (CVSS) measures which should be used to help assess risk and prioritize patching. However, CVSS measures are only part of the ICS patching risk assessment prioritization. If the "big picture" of ICS-specific context and ICS attack vectors are not considered, patching efforts may cause unnecessary impact and/or inadequately reduce the risk surface, and unnecessarily impede operations and/or safety.

ICS defenders should prioritize vulnerability management based on risk and patch a subset of vulnerabilities during scheduled engineering maintenance windows. Risks should be prioritized based on the following considerations:

- Having a reliable ICS asset inventory to understand the risk surface to operations.
- Knowing which assets in the environment are vulnerable.
- Leveraging sector-specific threat intelligence to understand commonly observed tactics and techniques.
- Knowing the architecture and how to place assets in control networks' enforcement zones.
- Understanding the potential for an adversary to gain access through existing and properly configured firewalls, such as logging into the HMI, engineering workstation, or data historian.
- Knowing the criticality of vulnerable assets to engineering operations.
- Placing importance of patching or mitigating vulnerabilities that provide attackers remote network access if exploited and if vulnerabilities have associated publicly available exploit kits.

ICS defenders must identify and prioritize mitigating vulnerabilities that give adversaries specific capabilities like:

- Access to the control networks where ICS commands could be injected.
- Unauthorized and/or unrestricted remote access.
- Publicly available exploit kits targeting critical engineering assets.

Career Development Opportunity - ICS410

ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. This course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

ICS CYBERSECURITY

A patch decision tree can be used to help prioritize ICS security patches. It is important to put particular emphasis on the Analyze Risk assessment step. See the following graphic for an example of the Department of Homeland Security's control system patch decision tree.

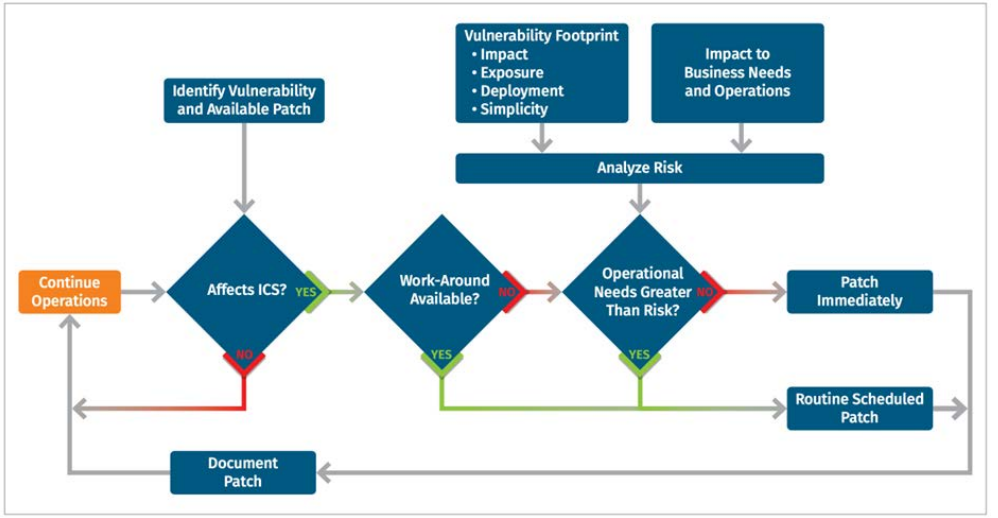


Figure 1: Department of Homeland Security ICS Patch Decision Tree

ICS incident response phases and objectives

ICS incident response adapts traditional incident response phases to suit engineering environments, prioritizes safety in every phase, and includes different multi-team stakeholders. ICS incident response stakeholders include engineering operators, external control system support vendors, government agencies, physical safety teams, physical security teams, IT security, ICS security, etc., with direction from the owner/operators of the ICS facilities.

The objectives for each phase of an ICS-specific incident response[5] include:

Phase 1: Prepare

Have well-defined, well-communicated roles and responsibilities and trained ICS-specific security defenders who understand engineering and can investigate control systems-related cyber events. A cyber-defensible position must be established as part of a well-tested and regularly updated ICS-specific incident response plan. Technical ICS security teams must ensure tools and skills are tested and ready to be deployed. This means they should understand the industrial protocols used, what normal ICS network communications look like, and possess the ability to spot abnormalities in the traffic.

Phase 2: Identify and Detect Threat

Deploy ICS-specific network visibility and threat identification techniques. These techniques are driven by consuming and applying sector-specific threat intelligence across the ICS Cyber Kill Chain.[6]

Phase 3: Acquire Evidence

Fight through the attack while maintaining safety; acquiring key network communications, endpoint, and engineering device logs; and making evidence available for meaningful and timely forensics analysis.

5 https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/
6 https://www.sans.org/white-papers/36297/

Phase 4: ICS Time Critical Analysis

Continue to fight through the attack and maintain safety while conducting time critical analysis. Traditional IT containment and eradication steps may cause more damage to safety, engineering, and production than the threats themselves. Care must be given in this phase to apply deep knowledge of how threats impact control systems and what a possible response could mean for operations and safety during containment and eradication.

Phase 5: Contain

Preserve operations through logical or physical changes in the control environment to further reduce impacts to safety and control systems. ICS Security, Engineers, and Operator teams fight through the attack, working together where evidence and intelligence can be shared, and contain the threat with as little disruption to safety and operations as possible.

Phase 6: Eradicate and Recover

In this phase, the threat or threats are eliminated from the environment(s) when it is safe to do so according to facility stakeholders and engineering. ICS security must continue to monitor and actively defend against the incident. Only then can the response team, in conjunction with applicable stakeholders, begin to restore engineering systems to their normal operational state and regain full production of engineering operations at all levels of the Purdue Network Architecture.

Career Development Opportunity - ICS515

In the ICS515: ICS Visibility, Detection, and Response course, students explore numerous hands-on technical labs and data sets from ICS ranges and equipment with emulated attacks and real-world malware deployed in the ranges for a highly simulated experience detecting and responding to control system threats. Students will also interact with and keep a PLC, a physical kit emulating electric system operations at the generation, transmission, and distribution level, and a virtual machine set up as an HMI and engineering workstation (EWS).

Phase 7: Lessons Learned

Similar to traditional IT incident response, use this phase to conduct and apply lessons learned to improve response and restoration efforts for future incidents.

Phase 8: Share Information

Share relevant tactical, strategic, and operational threat intelligence and cybersecurity lessons learned which might be of use for defense in the larger ICS and critical infrastructure community.

Figure 2: ICS Incident Response Phases

Considerations for ICS incident response

There is a common misconception where a utility may think they are too small to be a target of an ICS cyber attack or impactful cyber event. The reality is, however, that adversaries often target smaller facilities to develop and test attack methodologies in preparation to attack their ultimate target environment. Small or large, all ICS environments should have an industrial-grade incident response plan.

In particular, ICS-specific incident response phases must consider all unique aspects

Unique Systems

Nontraditional systems with industrial and proprietary setups, forensic logging capabilities, and protocols.

Reliance on External Vendor Support

External engineering teams may require special secure remote access for engineering support and may manage and be responsible for restoration copies of PLC logic, setpoints, intelligent electronic device (IED) configurations, etc.

Legacy Systems

Systems and devices that may not be eligible for patching or firmware updates or may only be available for infrequent updates to internal operating systems, such as during a scheduled engineering maintenance window.

Non-Traditional Operating Systems

Purpose-built, embedded, and/or proprietary operating systems common to control environments where many traditional security defenses are not effective or applicable.

Personnel Safety

The most important goal of control systems is not confidentiality, integrity, or availability, but safety. Only after safety has been addressed does the incident response team address confidentiality, the integrity to trust operations, and the availability of engineering devices.

Protecting Physical Assets

Control systems use physical components to change the physical world. A cyber attack could result in physical damage to engineering assets, environmental impacts, and safety implications such as injury or death.

ICS incident response specific roles and responsibilities

Many aspects of incident response need to be coordinated, planned, and regularly exercised. These incident response tasks are most effectively completed when subdivided by specific roles, which may include:

Incident Response Director/ICS Security Team Manager
Interfaces with the executive leadership team on an incident's status, resources, impacts, and options to maintain safety and operations.

Lead Responder
Guides incident response personnel and quick triage/impact timeline analysis. Advises the Incident Response Director on available actions to reduce the impact on safety and operations.

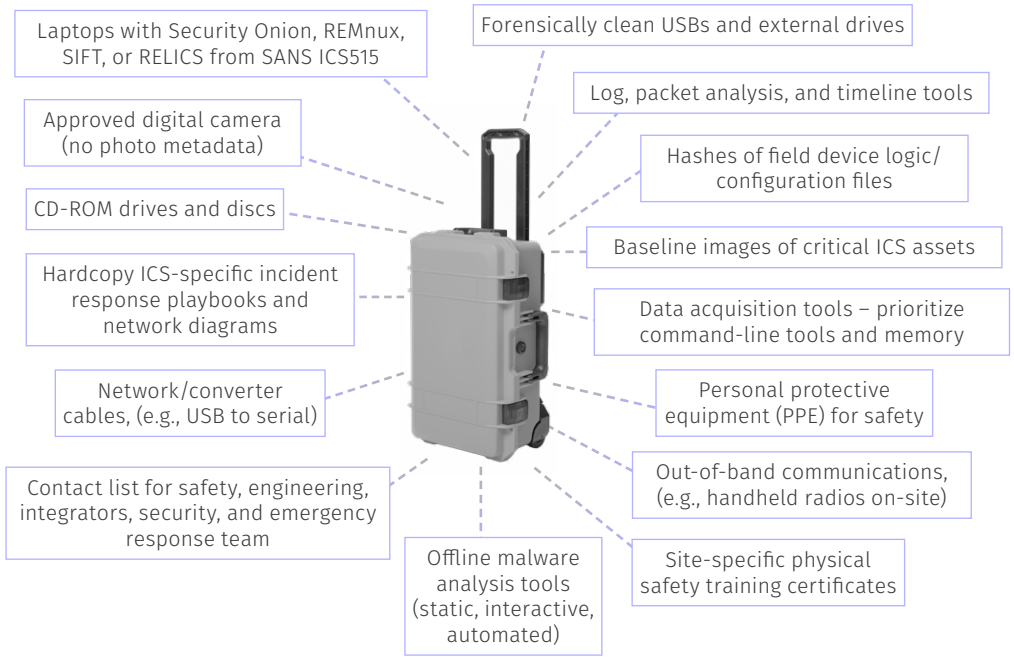
Incident Handlers
Cybersecurity and ICS field and technical personnel who may be required to make environment and asset changes. They handle evidence acquisition, scope threats and infections, and undertake analyses, among other tasks.

Fire and Security, Safety, Law Enforcement, Governments
Teams prepared for physical first aid, emergency response, evacuation strategies for physical site safety, external communications or reporting, intelligence gathering and sharing, and efforts beyond the site.

ICS incident response jump bag

The objective in industrial environments during a cyber incident is to maintain safety and operations and fight through the attack. To ensure incident response readiness, having a jump bag is essential.[7] Using the tools in the incident response jump bag in conjunction with knowledge of the affected control systems, and how they are used for engineering processes, allows an ICS cyber defender to quickly analyze, understand, and triage threats and impacts. Once the incident is analyzed and understood, the analysis, which includes response options that minimize loss of control, loss of visibility of ICS, and ensure safety, is provided to facility owners to choose and implement.

ICS jump bags should be portable (e.g., in rolling, protective cases), available at all critical sites, and/or deployed with the incident response teams as they conduct on-site response. Essential ICS incident response jump bag items include:



7 https://youtu.be/ZR4Jy9K0AhI

When to initiate ICS incident response

Rapid yet thorough analysis of data acquired from critical assets and the ICS network traffic to and from those assets, combined with knowledge of engineering operations, will help teams determine when full industrial incident response must be performed.

Use the following event conditions to help determine the potential risk to engineering, understand where the attack is in the ICS Cyber Kill Chain, and when it is appropriate to shift to full industrial incident response.

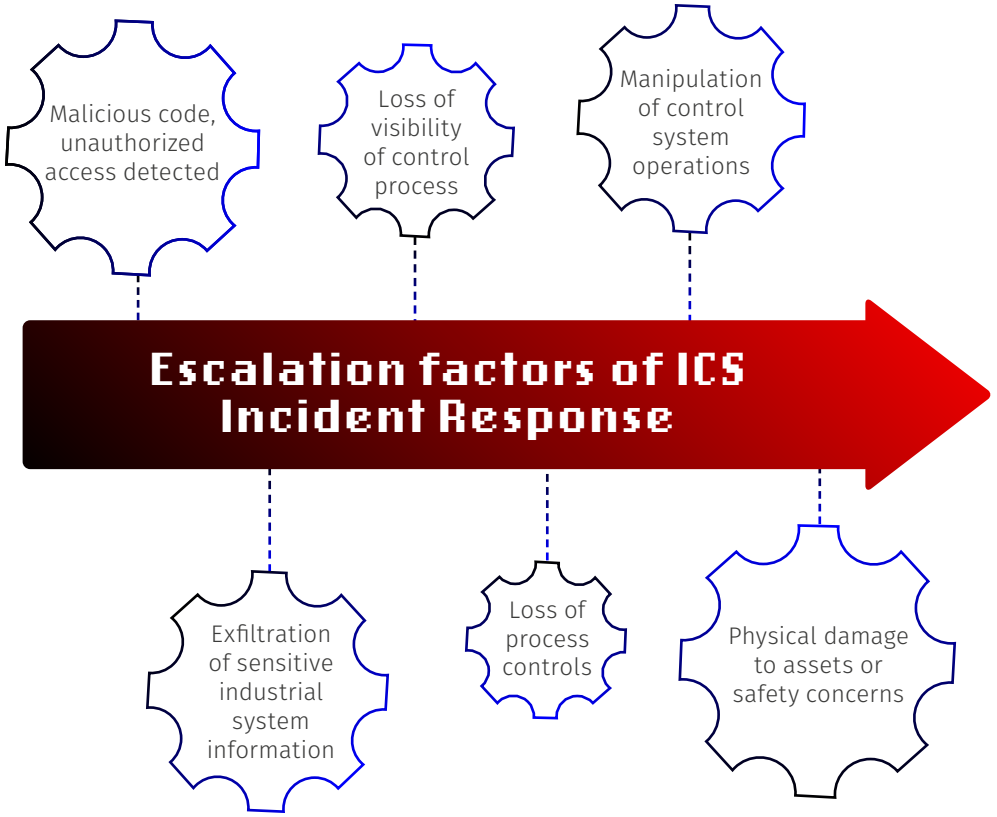


Figure 3: Event Conditions

Unique Systems Malicious Code, Unauthorized Access Detected

Installation or execution of malicious software. For example, an adversary gaining physical or logical access to a network, system, or data without authorization, or introducing a cyber-contaminant that could impact process control views or controls.

Exfiltration of Sensitive Industrial System Information

An ICS cyber incident exfiltrating sensitive control system data could be used to cause harm. For example, ICS field device ladder logic, control system configuration, or historian database entries are copied off a network. This is an indication of a follow-on (non-immediate but potentially imminent) targeted ICS cyber attack.

Loss of Control Process Visibility

An ICS cyber incident affecting the ability to view the state of the physical process. For example, a power generating facility is unable to view the current system load or the current power grid operating frequency to maintain 60Hz.

Loss of Process Controls

An ICS cyber incident affecting the ability to change the state of the physical process. For example, an oil refinery is unable to safely shut down its crude oil distillation process or maintain pipeline pressure.

Manipulation of Control System Operations

The abuse of internal native system components or protocols such as HMI commands and ICS protocols such as EthernetIP, ModbusTCP, DNP3, 61850, OPC, etc. For example, DNP3 is used to send unauthenticated “open breaker” commands to remote terminal unit (RTU) field devices to open electric circuit breakers and cut power.

Physical Damage to Assets or Safety Concerns

An ICS cyber incident affecting the physical properties or integrity of physical assets, or introducing a potential physical safety impact to plant operators, workers, and/or on-site visitors, contractors, etc.

ICS incident response must-haves

While IT/OT convergence of both technology and workforce poses unique challenges, it can drive a more realistic ICS threat detection and response process. A converged incident response plan must consider available cybersecurity defenses in both environments and work to reduce the impact of attacks through IT into ICS, which is a common vector adversaries leverage that has been observed time and again. This more realistic process can provide early warning signs of an attack that could impact or specifically target the industrial process. Incident response for ICS should consider the following:

The ICS-Specific Incident Response Plan

Conduct realistic ICS tabletop exercises driven by sector-specific control system threat intelligence or ICS gaps identified in your cybersecurity program or facility to ensure your ICS-specific incident response plan meets the needs of an ICS cyber attack.

ICS-Specific Network Security Monitoring

Ensure "plant floor" network visibility with ICS deep-packet inspection to drive incident response or proactive threat hunting. Network visibility capabilities should go beyond simply querying about indicators of compromise and also include capabilities to assist with analyzing threat tradecraft.

Trained ICS-Specific Security Defenders

Trained ICS cybersecurity personnel must understand the nuances between traditional IT and ICS security, the ICS mission, safety, the engineering process, and ICS protocols and active defense procedures.

ICS incident response in practice

Successful ICS incident response requires a clear understanding of roles, responsibilities, physical safety, engineering protocols and process, network visibility, detection, and forensics capabilities. Facilities benefit from a tested, safe, and defensible cyber position. Consider the following when adapting traditional incident response steps to suit industrial control environments:

- Acquire forensics data from key ICS assets.
- Triage quickly to understand the threat via static or automated malware analysis.
- Collaborate with engineering staff and senior management.
- Determine operational impacts.
- Analyze the impact of any reliance on external vendors and IT.
- Execute the Safe Cyber Position[8] if applicable.
- Present analysis and options (blocking C2 access, running ICS in manual mode, removing remote access, etc.) to fight through the attack (contain/eradicate).
- Contain threats while running operations.
- Eradicate when it is safe for operations.
- Conduct regularly scheduled ICS incident response tabletop exercises.
- Examine the connectivity and isolation of legacy devices.
- Develop countermeasures.
- Use indicator "hits" to scope incident and related contamination.
- Compare production and baselined configurations to detect tampering in controllers, etc.
- Identify and apply lessons learned (e.g., correct gaps in evidence acquisition, deploy additional ICS network visibility, detection capabilities, and determine whether threats are malware or human adversaries).
- Apply lessons learned to the ICS incident response plan.

8 www.youtube.com/watch?v=47rpbBonDYY

Career Development Opportunity - ICS612

ICS612: ICS Cybersecurity In-Depth is an in-classroom lab setup that moves students through a variety of advanced, technical, hands-on exercises that demonstrate how an adversary can attack a poorly architected ICS and how defenders can secure and manage the environment.

ICS connectivity: business benefits and cyber risk

Engineering systems include PLCs, RTUs, protection control relays, embedded HMIs, SISs, distributed control systems (DCSs), solenoids, meters, field bus communications, sensors, and actuators. For decades, these engineering devices and systems have operated the critical infrastructure we rely on in isolation. And, while modern connectivity into ICSs is becoming common and has led to increased data accessibility across traditional IT and OT environments with several benefits, as detailed in the below graphic, it also presents greater threats to security.

Figure 4: Benefits of Modern ICS Connectivity

Enabling connectivity to previously isolated engineering environments results in these environments now being exposed. Recent ICS attacks that take advantage of this increased ICS connectivity have been created and deployed by adversaries-for-hire and rogue nation-states which have the means and motivation to disrupt operations and impact safety. The good news is, ICS/OT cybersecurity defense is totally achievable with an effective team and an ICS security approach to risk management!

Prioritize for safety

Significant risks to safety can occur if proritizing IT or traditional business systems over industrial control systems or if the ICS/OT security reporting structure fails to fully embrace the differences between IT and ICS/OT.

Consider, for instance, a security incident on the IT business email system and a security incident on the supervisory control and data acquisition (SCADA) system of a power grid occurring simultaneously. Which incident gets priority? What pace and rigor will the organization give to the priority incident? Specifically, what drives the decision to manage these very different risks? And, what are the related impacts in these different environments?

Did the organization select their focus based on what was most important for the safety of the people, environment, and organization overall? Today's ICS incident response teams must understand the control system processes, engineering, industrial protocols, safety factors, and ICS-specific cyber threats, and tailor incident response playbooks and risk management strategies accordingly.

Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course includes an ICS attack history walkthrough for new and existing ICS/OT security managers with a major focus on lessons learned for improved ICS risk management.

ICS security management choices

ICS-specific technologies, threat detection methods, and unique incident response considerations are essential in building and maintaining an effective long-term ICS program. However, the most critical components of responding to an ICS incident are the dedicated people specifically trained in ICS incident response.

As managers we get to choose many things about our ICS/OT cybersecurity program. We get to choose our team, the best technologies, and our processes. What we do not get to choose is if we are a target. The adversary does that.

Career Development Opportunity - ICS418

ICS418: ICS Security Essentials for Managers. SANS has extended the Cyber42 Leadership Simulation game (https://www.sans.org/blog/cyber42) to ICS418 as Industrial Cyber42. Students participate in various ICS risk-based and management level decision scenarios to protect a control system using their risk management skills where the object of the game is to finish with the highest safety culture score.

ICS security leadership pathways

Common roles that lead to managing ICS/OT cyber risk include:

1. **Manager asked to "Step Over"**
   IT Security Manager is assigned the responsibility of ICS cyber risk and must build and maintain a sustainable ICS security program.

2. **Practitioner in the field asked to "Step Up"**
   ICS, IT, or engineering team member steps up to an ICS Security Manager position to build and maintain a sustainable ICS security program.

3. **ICS Manager "In Place"**
   An existing ICS manager responsible for ICS security practitioner direct reports and works to build and maintain a sustainable ICS security program.

Figure 5: Leadership Pathways

Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course empowers new and established ICS security managers from all areas to understand the differences between IT and ICS/OT, to prioritize safety, build and maintain strong relationships, build teams, effectively manage ICS/OT cyber risk, and effectively report to applicable stakeholders.

The ICS security defender skillset recipe

Technology and processes (even if automated) do not get us far in the defense area without a trained and focused workforce. Human defenders—the people, our workforce—are those who use ICS security technologies, work with engineering, safety, business, IT security, and other teams. These ICS defenders understand the ICS mission, possible impacts, and engineering recovery. They understand the industrial process, protocols, normal vs. abnormal engineering operations network traffic patterns, safety with context, the commonly targeted assets in control systems, etc. Modern trained ICS cybersecurity staff understand the nuances between traditional IT and ICS security.

As ICS risk management leaders work to build their ICS security teams, they should consider the following ICS cybersecurity skillset recipe. For the team to be effective, team members would do well to have the following skills and experience:

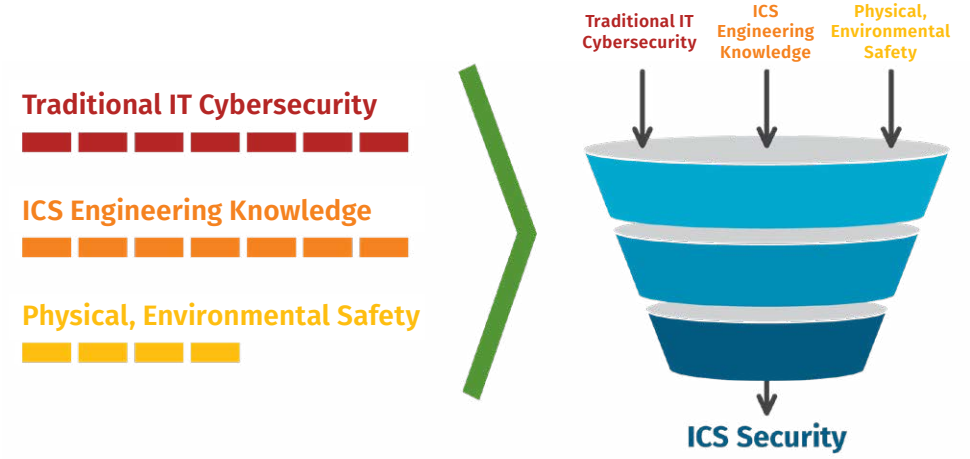


Figure 6: ICS Cybersecurity Skillsets

> **"The only defense against well-funded nation-state attacks on power systems (and the rest of the critical infrastructure that keeps us and the economy alive and free) are people with extraordinary cyber talent and skills."** - Mike Assante

ICS cybersecurity team roles

As ICS cybersecurity roles and tasks emerge and evolve, ICS managers who are building their teams should consider staffing for the following roles:

Unique Systems ICS Cybersecurity Analyst

Acquire and manage the necessary resources, including leadership support, financial, and key security personnel to support the ICS security mission, safety goals, and objectives to maintain reliability of engineering processes.

ICS Security Architect

Possess knowledge of and the ability to address all aspects of the control system architecture, best practice security from ICS reference models and network segmentation such as Purdue, and ICS410 SCADA Reference Architecture[9] reference models.

ICS Cybersecurity Incident Responder

Detect, analyze, identify, respond to, contain, eradicate, and recover from industrial cybersecurity incidents. A key part of this role in the event of an incident is working with engineering teams and a variety of external ICS/OT vendors and/or integrators and law enforcement in safeguarding the physical control systems, including SISs, to reduce cyber attack impact and return operations to a trusted restoration point.

ICS Cybersecurity Manager

Possess knowledge of and experience in IT and ICS/OT security, the tools to address industry pressures to manage cyber risk to prioritize the business as well as the safety and reliability of operations. ICS Cybersecurity Managers must build and maintain business relationships with engineering staff and executive stakeholders to communicate and reduce cybersecurity risk to engineering operations. This role requires a firm understanding of the drivers and constraints of cyber-physical environments, technologies throughout their organizations, ICS/OT security practitioners, and how to manage the processes.

9 https://www.sans.org/posters/control-systems-are-a-target/

Process Control Engineer

Design, test, troubleshoot, and oversee the implementation of new engineering processes. In plants with established control systems, engineers may design and install retrofits to existing systems and troubleshoot engineering hardware, embedded systems, control system software, and engineering/instrumentation problems in a manner that also preserves the cybersecurity integrity of the engineering system signals, sensing, commands, and control environment.

The following graphic details proposed roles and maps them to the SANS course most applicable to the role. It is important to note that roles will likely grow and require additional knowledge.

Common roles that lead to managing ICS/OT cyber risk include:

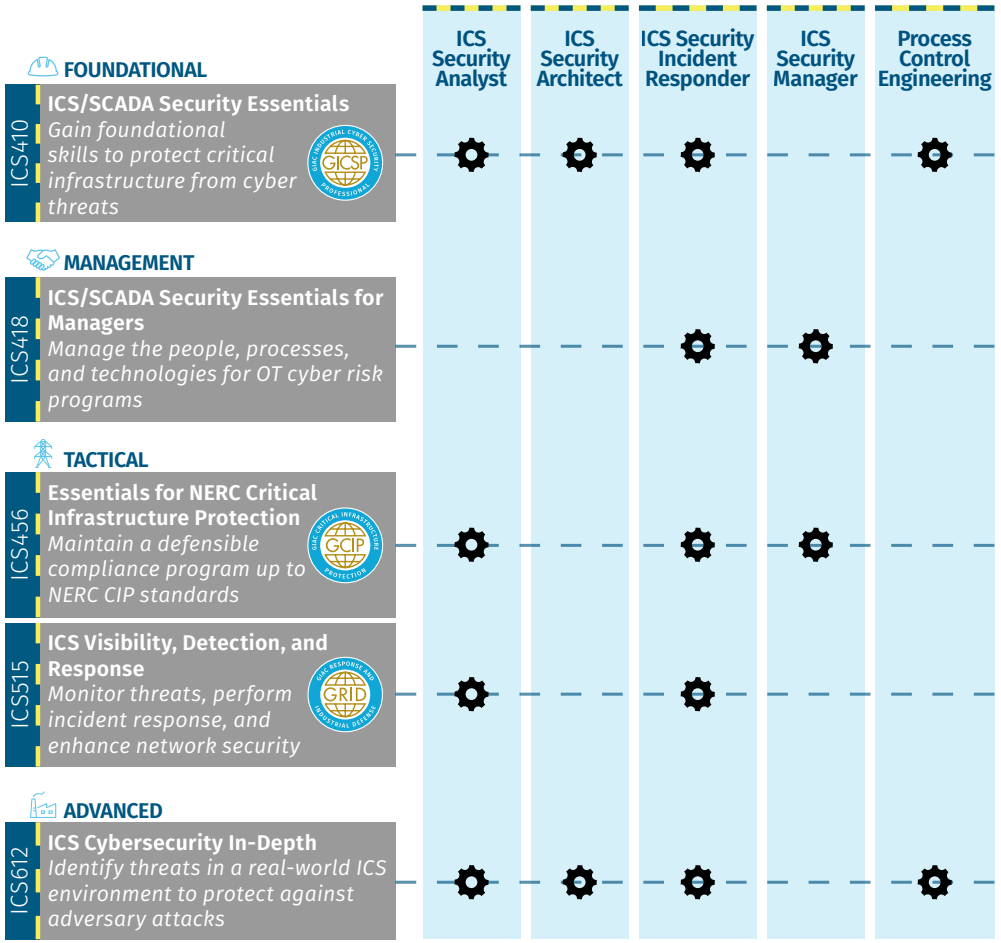


Figure 7: ICS Role to SANS Course Matrix

Key ICS management takeaways

1. **Safety Is No. 1.** In control system environments, safety is the top priority. Cybersecurity and other functions support safe and reliable operations. For example, tools like intrusion detection systems (IDSs) are preferred due to side effects of false positives in intrusion prevention systems (IPSs), which render an unsafe condition that could hurt or kill people.
2. **Embrace IT and ICS differences.** Understand and embrace the differences between IT and ICS by prioritizing the ICS business mission to secure and enable physics and engineering controls that monitor for and make physical changes in the real world that are safe for people and the environment.
3. **ICS/OT asset inventory.** A prerequisite for ICS active defense is a formal ICS/OT asset inventory. The four main methodologies of creating an ICS asset inventory (physical inspection, configuration analysis, passive traffic analysis, and active scanning) can be combined for increased accuracy while prioritizing safety.
4. **Enable active defense.** Ensure the Active Cyber Defense Cycle (ACDC)[10] has a strong foundation by implementing ICS/OT-specific architecture (align with the Purdue and SANS ICS410 SCADA Architecture models to start), then implement passive defenses to prepare for Active Defense on the Sliding Scale of Cybersecurity.[11]
5. **Deploy ACDC specific to ICS.** Empower technical ICS security staff to maintain the human-driven ICS/OT ACDC while leveraging sector-specific ICS/OT threat intelligence. Staff should be dedicated, ICS/OT-trained security resources who understand the engineering process well enough to determine if control network activity is anomalous or malicious in nature.
6. **Validate the ICS/OT incident response plan.** Validate and gain the benefits of conducting regularly scheduled, specific ICS/OT incident response plan tabletop exercises and apply related lessons learned.

10 https://www.sans.org/white-papers/36240/
11 "The Sliding Scale of Cyber Security," Sept 1, 2015, www.sans.org/white-papers/36240/

Epilogue to Volume 3

This volume details an approach for ICS incident response, the skillsets and people needed to “fight through the attack,” the need for quick analysis and triage with engineering knowledge, the right ICS tooling, an understanding of the protocols (engineering device communications), and the unique aspects of engineering and jump bag equipment.

Most importantly, this volume explains why, even though technologies and plans are crucial to ICS cyber defense, the human defenders are the most critical piece of the puzzle. We are reminded that, with the right teams and team leaders, “ICS Defense Is Doable” and required to protect the critical infrastructure we rely on daily.

The ICS community forum

An excellent way to get involved is by participating in SANS’s ICS Community Forum. ICS professionals discuss current security events, share tips, ask questions, and connect with others who are passionate about securing our critical infrastructure. Never again miss a community event, job opportunity, or the latest free resources authored by SANS ICS practitioner faculty.

https://ics-community.sans.org/

SANS ICS curriculum

SANS has joined forces with industry leaders to strengthen ICS cybersecurity. This initiative equips security professionals and control system engineers with security awareness, work-specific knowledge, and the hands-on technical skills needed to secure automation and control system technology.

Ensure that managers retain and train cybersecurity defenders knowledgeable in both IT and ICS/OT-specific cybersecurity incident response and who possess a high level of technical engineering knowledge.

ICS410: ICS/SCADA Security Essentials
Provides an understanding of industrial control system components, purposes, deployments, significant drivers, and constraints. Also included are hands-on lab learning experiences to control system attack surfaces, methods, and tools.

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

ICS515: ICS Visibility, Detection, and Response
Help deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/

ICS456: Essentials for NERC Critical Infrastructure Protection
Empowers students with knowledge of the "what" and the "how" of the NERC CIP standards. It provides multiple approaches for identifying and categorizing BES cyber systems, and helps determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

https://www.sans.org/cyber-security-courses/essentials-for-nerc-critical-infrastructure-protection/

ICS612: ICS Cybersecurity In-Depth
Provides advance coverage of security concepts primarily driven by applied learning with hands-on labs. The in-classroom environment simulates a real-world factory, and the labs move students through a variety of exercises that demonstrate how an attacker can compromise an ICS environment and how defenders can better secure and manage the environment.

https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth/

ICS418: ICS Security Essentials for Managers
The ICS418 course fills the identified gap amongst leaders working across critical infrastructure and operational technology environments. It equips ICS managers with the experience and tools to address the business and industry pressures to manage cyber threats and defenses to prioritize the business, safety, and reliability of ICS operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints that exist in cyber-physical environments and obtain a nuanced understanding of how to manage the people, processes, and technologies throughout their organizations. ICS418 empowers new and established ICS Security Managers.

https://www.sans.org/cyber-security-courses/ics-security-essentials-managers/

SANS SECURITY AWARENESS

Create a More Secure ICS Environment with SANS Security Awareness
SANS Security Awareness ICS Training keeps the unique needs of ICS industries in mind, equipping anyone who works within ICS environments with the information and tools necessary to protect and defend all types of control systems, including Supervisory Control and Data Acquisition (SCADA), DCS and other small systems, such as PLCs. Our 12 computer-based ICS learning modules are fully Sharable Content Object Reference Model (SCORM) compliant and can be deployed on any learning management system.

https://www.sans.org/security-awareness-training/products/specialized-training/ics-engineer/