ESTABLISHING THE ICS CYBERSECURITY PROGRAM

ICS Cybersecurity Leadership

POSTER

sans.org/ics

Poster created by Dean Parsons—co-author of SANS ICS418 course.

ICSPS_ICS418_0525

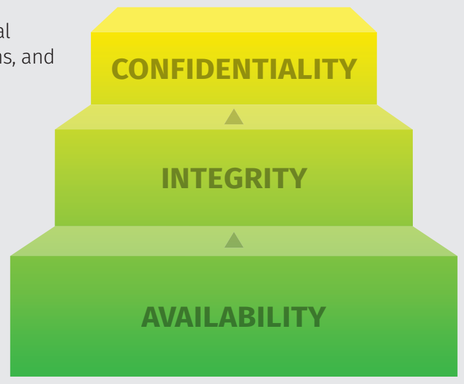
SANS

Safety Prioritization and Security in ICS

The priority in IT security tends to be data confidentiality, integrity, and availability. The priority in ICS is safety and is accomplished by operating a control system with a process that maintains safety, integrity, availability, and confidentiality. This involves:

- Safe engineering operations,
- Integrity of the engineering process and commands,
- Availability of the operational processes and safety systems, and
- Confidentiality of sensitive ICS engineering information that may exist in the ICS network(s).

IT PRIORITIES



ICS PRIORITIES

Leading an ICS Security Program

Safety could be at risk if information technology (IT) or traditional business systems are prioritized over industrial engineering control systems. Likewise, safety is at risk if the responsible reporting structure for industrial control systems (ICSs) or operational technology (OT) security fails to fully embrace the differences between IT and ICS/OT.

Consider this example: two security incidents occur simultaneously; one on the IT business email system and another on the supervisory control and data acquisition (SCADA) system of a power grid. Which incident should be prioritized to receive the needed resources to investigate, respond, and defend? What pace and rigor will the organization give to the priority incident? Specifically, what drives the decision to manage these very different risks and very different impacts?

This example makes it clear: organizations should prioritize the incidents to ensure the safety of people, the environment, and the organization overall.

To effectively lead ICS/OT cyber risk and defense strategies accordingly:

- **ICS incident response teams** must understand the control system processes, industrial protocols, safety factors, ICS-specific cyber threats, and be able to tailor incident response.
- **ICS leaders** must manage a new type of ICS-specific security team to work with engineering staff to find and report meaningful control system-specific key performance indicators to effectively manage ICS/OT cyber risk and defense strategies accordingly.

IT Security is NOT ICS Security

Industrial engineering control system assets are often inaccurately compared to traditional IT assets. IT and ICS systems have different missions, objectives, and impacts during an incident. They also have different devices, including but not limited to embedded operating systems and engineering devices speaking nontraditional industrial protocols. Adversaries targeting ICSs must use different attack tactics and techniques for access, execution, collection, and persistence to degrade safety, manipulate control, and damage physical engineering assets or property.

IT SECURITY – MOVING AND SECURING DATA

Traditional IT security focuses on digital data at rest or data in transit and the pillars of confidentiality, integrity, and availability.

ICS/OT SECURITY – ENABLING AND SECURING PHYSICAL INPUT AND ACTIONS

ICS/OT systems manage, monitor, and control real-time engineering systems for physical input values and control output for physical actions in the real world. Generally, the order of priorities in ICS environments is:

1. Safety of operations
2. Integrity of operations
3. Availability of engineering systems
4. Confidentiality of control system data

The graphic to the right details six areas where the differences between IT and OT/ICS systems results in different requirements.

ICS CYBERSECURITY SKILLSETS AND ROLES

ICS Knowledge Levels

As an ICS team's skillsets and roles are considered, the ICS Knowledge Levels can be used to guide the development plans for team members, tasks, roles, and responsibilities. Each knowledge level can be used to build a strong ICS security team and establish and mature an ICS security program.

Base Knowledge – LEVEL 0

Base knowledge training should focus on security behaviors for individuals who interact with, operate, or support industrial control systems. A training program may introduce ICSs, the risks or types of ICS attacks, basic system and network defenses and controls, as well as typical ICS governance and policy best practices. The training program's goal should be to change human behavior in an ICS environment and reduce risk at a fundamental level.

Foundational Knowledge – LEVEL 1

Foundational knowledge training should ensure the workforce involved in supporting and defending industrial control systems are trained to keep the operational environment safe, secure, and resilient against current and emerging ICS cyber threats. Across a diverse audience, this training level should build, develop, and ensure a common language in control systems and an understanding of the underlying engineering processes while providing an overview of the basic tools specific to ICS security across a wide range of industry sectors and applications.

Mastery Knowledge – LEVEL 2

Mastery knowledge training should be role-specific and focus on individuals and organizational needs to advance ICS cybersecurity defense knowledge, skills, and ability in a specific field, architect proper ICS network architecture, and conduct incident response and recovery practices with engineering teams.

Expert Knowledge – LEVEL 3

Expert knowledge training should focus on coordinated industrial advanced incident response and improving team capabilities and toolsets. Expert training typically consists of joint exercises and projects with engineering and other facility teams.

Leader – LEVEL 4

ICS cybersecurity leadership training should focus on technical team development and leadership, risk management, approaches for building relationships with other teams, tracking meaningful metrics, maturing the overall ICS cybersecurity program, and communicating technical concepts to non-technical audiences, including reporting to the board.

JOB DESCRIPTIONS

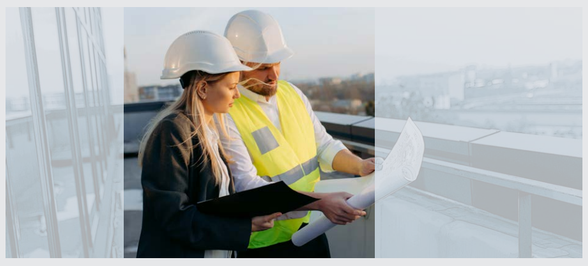
The differences between traditional IT and ICS are many: mission, safety, system design, support, cybersecurity controls, incident response. So, it isn't surprising that roles and tasks are also different. The following job descriptions are specific to ICS and OT security and increasingly recognized across multiple ICS sectors.

ICS Security Analyst

Daily engineering systems practitioner. Cybersecurity responsibility over some piece of the control system environment (could be server, access, applications, cyber threat intel, network monitoring, remote access, etc.) while prioritizing safety and reliability of engineering processes.

EXAMPLE TASKS:

- Establishes and maintains ICS network and engineering field device asset inventory.
- Establishes and maintains ICS network visibility and monitoring.
- Performs tactical ICS incident response.
- Executes threat Intelligence consumption and proactive threat hunting.

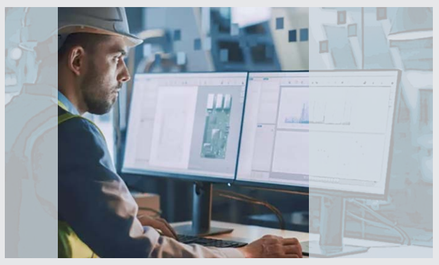


ICS Security Architect

Ensures ICS network security is established, maintained, and meets compliance and other requirements necessary to protect the engineering systems in the operational environments at both local and remote sites. Designs and supports a defensible control system network architecture for secure internal, external, and remote connectivity, aligned with ICS specific network security best practice with industrial incident response in mind. Prioritizes the mission of the safety of people and reliability of operations and adequately addresses all aspects of the control system network architecture and integrity.

EXAMPLE TASKS:

- Appropriately segments engineering systems, field devices, and related network traffic flows based on the Purdue model aligned to the SANS ICS410 SCADA Reference Architecture (e.g., Levels 0–4) or similar.
- Involved in all phases of network technology deployments and changes such as all Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) phases to ensure industrial network equipment feature-sets are available and can be enabled, including but not limited to ICS traffic capture and threat monitoring across Levels 0–4 to drive the Active Cyber Defense Cycle (ACDC) for industrial-specific incident response.
- Performs security reviews to identify gaps in control system network architecture, internal and external connectivity, including wired, wireless, and remote access, to ensure integrity of control system protocols and commands.



ICS Security Incident Responder

Monitors, detects, analyzes, and responds to industrial cybersecurity incidents caused by traditional malware, specific control system malware, or human adversaries who threaten engineering operations. Works closely with engineering teams and management to ensure safety and the resilience of engineering system hardware, industrial protocols, safety protocols, external ICS support, and engineering applications are maintained for recovery to a trusted restoration point for all engineering processes.

EXAMPLE TASKS:

- Leverages ICS cyber threat intelligence to drive proactive threat detection and scope possible impacts to control system assets and networks and overall engineering processes and safety.
- Characterizes and analyzes network traffic to identify anomalous engineering activity and potential threats to control devices, network resources, or control system command integrity that may include the abuse of legitimate industrial control protocols and critical engineering assets.

ICS Cybersecurity Leader

Leadership role. Secures engineering and control system environment, tracks industrial security events, manages tactical teams, reports metrics, and matures the ICS security program. Builds and maintains inter-departmental, organizational, and vendor relationships across operations, risk, safety, and security at senior levels. Possesses IT and ICS/OT security experience to address industry pressures to manage cyber risk to prioritize the business—with the safety and reliability of operations top of mind. Builds and maintains business relationships with all stakeholders to communicate and reduce cybersecurity risk to engineering operations. Requires a firm understanding of drivers and constraints that exist in these cyber-physical environments and ability to manage the processes, technologies, and ICS/OT security practitioners.

EXAMPLE TASKS:

- Understands and continuously communicates the value of ICS/OT-specific security to maintain safety and manage engineering risk.
- Manages the people, processes, and technologies necessary to create and sustain a long-term ICS cyber risk program that considers business and safety culture.
- Aligns with compliance standards and best practices to empower ICS/OT security practitioners and engineering staff to appropriately conduct industrial incident response and recovery.

Process Control Engineer

Designs, tests, troubleshoots, and oversees implementation of new engineering processes. In facilities with established control systems, the 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.

EXAMPLE TASKS:

- Applies engineering system knowledge within all new technology initiatives that require or rely on the control system or any subsystem at the design phase through to implementation.
- Programs and manages the programmable logic controller modules and logic code including managing trusted known good logic files, code compare tools, and device recovery procedures.
- Supports technical engineering system configurations, including security settings and troubleshooting.
- Works with incident response teams before, during, and after cyber incidents.

ICS CYBERSECURITY TEAM DEVELOPMENT

The ICS Security Skillset Recipe

Human defenders use ICS security technologies and work with the 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, and 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 can 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. (See figure to the right).

ICS Team Development Pathway

Use this chart to map each job role within the ICS security area to a training path for control system and cyber-specific knowledge and practical hands-on skills.

		ICS Security Analyst	ICS Security Architect	ICS Security Incident Responder	ICS Security Leader	Process Control Engineering	ICS/OT Security Pen Tester
		Acquires and manages resources, supports, and performs key industrial security protection while adhering to safety and engineering goals	Ensures control system network security compliance and best practices for control networks	Executes specific industrial incident response for incidents that threaten or impact control system networks and assets, while maintaining the safety and reliability of operations	Builds and maintains business relationships with engineering staff and C-suite stakeholders by communicating and managing cyber-to-physical risks while reducing security risk to engineering operations and simultaneously prioritizing safety	Tests, programs, troubleshoots, and oversees changes of existing processes or implements new engineering processes through the deployment and operations of engineering systems and automation devices	Discovers system vulnerabilities and works with asset owners and operators to mitigate discoveries and prevent exploitation from adversaries
FOUNDATIONAL	ICS 310 — **ICS Cybersecurity Foundations™** *Learn the cyber fundamentals to protecting ICS/OT environments*	●	●	●	●	●	●
ESSENTIAL	ICS 410 — **ICS/SCADA Security Essentials™** (GICSP) *Gain the essential skills to keep critical infrastructure safe from cyber threats*	●	●	●		●	●
MANAGEMENT	ICS 418 — **ICS Security Essentials for Leaders™** *Manage the people, processes, and technologies for OT cyber risk programs*			●	●		
TACTICAL	ICS 456 — **Essentials for NERC Critical Infrastructure Protection™** (GCIP) *Maintain a defensible compliance program up to NERC CIP standards*	●		●	●		
TACTICAL	ICS 515 — **ICS Visibility, Detection, and Response™** (GRID) *Monitor threats, perform incident response and enhance network security*	●		●			
ADVANCED	ICS 612 — **ICS Cybersecurity In-Depth™** *Identify threats in a real-world ICS environment to protect against adversary attacks*	●	●	●		●	
ADVANCED	ICS 613 — **ICS/OT Penetration Testing & Assessments™** *Perform safe, hands-on ICS/OT penetration testing and assessments to identify vulnerabilities and improve operational resilience*	●	●				●

MATURING THE ICS CYBERSECURITY PROGRAM

The ICS Cybersecurity Leadership Cycle

"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 Pioneer

ICS Cybersecurity Leadership Defense Move

Move forward with an established team while considering each concept below:

SAFETY IS NUMBER 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.

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.

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 (1) physical inspection, 2) configuration analysis, 3) passive traffic analysis, and 4) active scanning) can be combined for increased accuracy while prioritizing safety.

DEPLOY ICS-SPECIFIC ACDC
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.

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 the lessons learned.

ICS Cybersecurity Tactical Defense Move

Work with an established ICS cybersecurity team to implement or verify your ICS security program against the SANS Five ICS Cybersecurity Critical Controls.

These five controls are the most important technical ICS cybersecurity controls and were designed to be an ICS/OT-specific cybersecurity strategy flexible enough to align with most organizations' risk models. These controls can be mapped to existing standards and frameworks such as IEC62443 and NIST CSF. Each of the five ICS Cybersecurity Critical Controls are described below.

ICS-SPECIFIC INCIDENT RESPONSE
Operations-informed ICS incident response plan with focused control system integrity and engineering recovery capabilities during an attack on an aspect of the engineering systems. ICS-specific incident response exercises must be designed to reinforce risk scenarios specific to the ICS engineering operations and control systems.

DEFENSIBLE CONTROL SYSTEM NETWORK ARCHITECTURE
Network architectures that support effective segmentation, visibility of control system traffic for analysts, log collection, asset identification, industrial DMZs, and enforcement for process communication integrity and reliability.

ICS NETWORK VISIBILITY AND MONITORING
Continuous network security monitoring of the ICS environment with protocol aware toolsets and system-to-system interaction analysis capabilities used to inform engineering of potential risks to the control, view, and safety of operations.

SECURE REMOTE ACCESS
Identification and inventory of all remote access points and allowed destination environments, on-demand access, and MFA authentication where possible, and jump host platforms to provide control and monitoring points within segments.

RISK-BASED VULNERABILITY MANAGEMENT
Understanding of cyber digital controls deployed and device operating conditions that aid in risk-based vulnerability management decisions to patch vulnerabilities, enable appropriate safety-informed mitigations to impacts, or monitor for possible attack exploitation internal to the control network.

LEVELING-UP ICS/OT CYBERSECURITY AND LEADERSHIP SKILLS

The role of the ICS/OT Cybersecurity Manager requires knowledge of risk management, engineering operations, IT cybersecurity, and ICS cybersecurity. This role bridges the gap between the disciplines to manage unique challenges and puts forth required resources, technologies, and practices to protect critical infrastructure.

SANS ICS418 students may come to class with different backgrounds, all coming together to address and progress workforce development, governance, ICS risk management, program maturity measurement, and culture. Common pathways into ICS Leadership are as follows:

Manager Responsibility Shift: Step Over—IT Security Manager who must create an ICS security program.

Practitioner to Manager: Step Up—ICS, IT, Engineering practitioner stepping up to an ICS security leadership position.

Existing Manager: In Place—An existing leader who has ICS security practitioners reporting to them.

SANS 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. **www.sans.org/ICS418**

0923