ICS410: **ICS/SCADA Security Essentials**

GICSP
Industrial Cyber Security Professional
giac.org/gicsp

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

Course Preview
available at: **sans.org/demo**

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as ICS penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of ICS, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: ICS Overview

Students will develop and reinforce a common language and understanding of industrial control system (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

TOPICS: Global Industrial Cybersecurity Professional (GICSP) Overview; Purdue Levels 0 and 1; Purdue Levels 2 and 3; DCS and SCADA; IT & ICS Differences; Physical and Cybersecurity; Secure ICS Network Architectures

SECTION 2: Field Devices and Controllers

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During section 2, students will develop a better understanding of where these specific attack vectors exist and how to block them, starting at the lowest levels of the control network. Students will look at different technologies and communications used in Purdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from the PLCs they programmed in section 1 and look at what other fieldbus protocols are used in the industry. Later in the section, students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol.

TOPICS: ICS Attack Surface; Purdue Levels 0 and 1; Ethernet and TCP/IP

SECTION 3: Supervisory Systems

Section 3 will take students through the middle layers of control networks. Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each. After a hands-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Purdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks.

TOPICS: Enforcement Zone Devices; Understanding Basic Cryptography; Wireless Technologies; Wireless Attacks and Defenses; Exercise: Network Forensics of an Attack; Purdue Level 2 and 3 Attacks

SECTION 4: Workstations and Servers

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Finally, students will explore attacks and defenses on remote access for control systems.

TOPICS: Patching ICS Systems; Defending Microsoft Windows; Defending Unix and Linux; Endpoint Security Software; Event Logging and Analysis; Remote Access Attacks

SECTION 5: ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course section, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

TOPICS: Building an ICS Cybersecurity Program; Creating ICS Cybersecurity Policy; Disaster Recovery; Measuring Cybersecurity Risk; Incident Response; Exercise: Incident Response Tabletop Exercise; Final Thoughts and Next Steps

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

> **"A mix of hands-on and theoretical class, being driven by a highly skilled instructor, makes this the best training in ICS security."**
>
> — Rafael Issa, **Technip**