SANS | GIAC
CERTIFICATIONS

ics.sans.org

ICS

INDUSTRIAL CONTROL SYSTEMS SECURITY

Courses and Free Resources

SANS CURRICULUM FOCUS AREA
INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY

The current landscape presents a diverse and chaotic picture of the threats facing industrial control system owners and operators.

Attacks that cause physical damage or impact physical processes are no longer limited to theory or speculation. We are now seeing incidents where malicious actors successfully intrude, cause system damage, and impact operations using ICS-tailored malware. We need to be prepared to defend our control systems against increasingly sophisticated adversaries.

SANS Industrial Control Systems Security courses will teach you to:

- Recognize ICS components, purposes, deployments, significant drivers, and constraints

- Identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats

- Understand approaches to system and network defense architectures and techniques

- Perform ICS incident response focusing on security operations and prioritising the safety and reliability of operations

- Implement effective cyber and physical access controls

- Develop ICS-specific cybersecurity programs and measure its impact across the organization

"The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find."

—Bassem Hemida, **Deloitte**

🌐 ics.sans.org   👤⁺ ics-community.sans.org/signup   🐦 @SANSICS

ICS CURRICULUM ROADMAP

Defending What Makes, Moves, and Powers the World

Every ICS Security Professional Should Know

ICS 410 — ICS/SCADA Security Essentials™

GICSP

Gain foundational skills to protect critical infrastructure safe from cyber threats

NERC Protection

ICS 456 — Essentials for NERC Critical Infrastructure Protection™

GCIP

Maintain a defensible compliance program up to NERC CIP standards

ICS 515 — ICS Visibility, Detection, and Response™

GRID

Monitor threats, perform incident response and enhance network security

ICS 612 — ICS Cyberecurity In-Depth™

Identify threats in a real-world ICS environment to protect against adversary attacks

Every ICS Security Manager Should Know

ICS 418 — ICS Security Essentials for Leaders™

Manage the people, processes, and technologies for OT cyber risk programs

TRAINING & CERTIFICATION

COURSE		GIAC CERTIFICATION	PAGE
ICS410	ICS/SCADA Security Essentials™	GICSP	6
ICS418	ICS Security Essentials for Leaders™		7
ICS456	Essentials for NERC Critical Infrastructure Protection™	GCIP	8
ICS515	ICS Visibility, Detection, and Response™	GRID	9
ICS612	ICS Cybersecurity In-Depthv		10

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

In a world that is seeing increasingly sophisticated and impactful industrial cyber threats, these courses prepare OT security professionals to lead, defend, and protect industrial control systems at the foundational, management, tactical and advanced skill sets. With SANS ICS Security, train to defend what makes, moves, and powers the world.

FOUNDATIONAL

ICS 410

ICS/SCADA Security Essentials™
Gain foundational skills to protect critical infrastructure safe from cyber threats

GICSP — GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL

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™
Maintain a defensible compliance program up to NERC CIP standards

GCIP — GIAC CRITICAL INFRASTRUCTURE PROTECTION

ICS 515

ICS Visibility, Detection, and Response™
Monitor threats, perform incident response and enhance network security
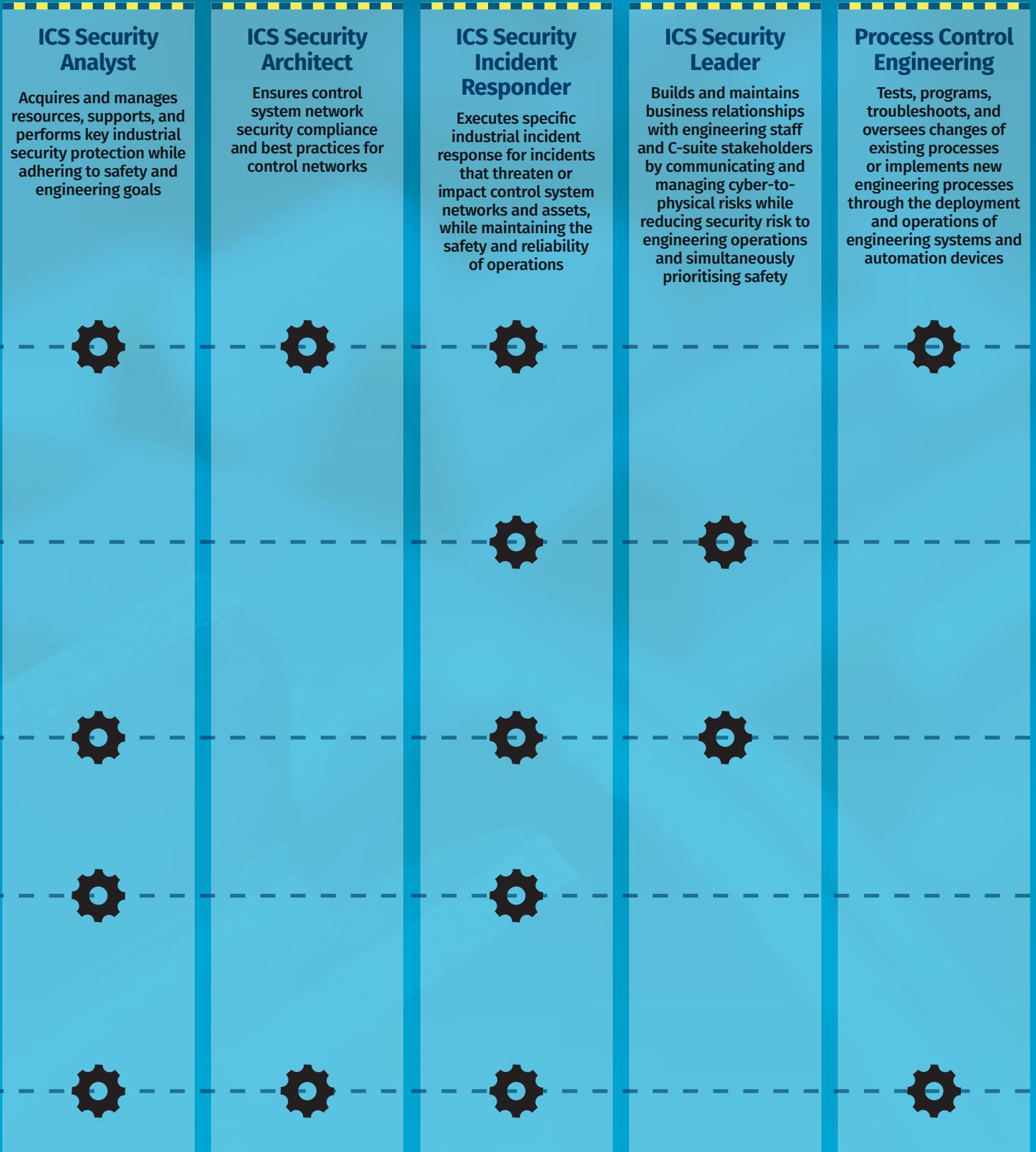
GRID — GIAC RESPONSE AND INDUSTRIAL DEFENSE

ADVANCED

ICS 612

ICS Cyberecurity In-Depth™
Identify threats in a real-world ICS environment to protect against adversary attacks

ics.sans.org   ics-community.sans.org/signup   @SANSICS

ICS CAREER PROGRESSION

ICS Security Analyst

Acquires and manages resources, supports, and performs key industrial security protection while adhering to safety and engineering goals

ICS Security Architect

Ensures control system network security compliance and best practices for control networks

ICS Security Incident Responder

Executes specific industrial incident response for incidents that threaten or impact control system networks and assets, while maintaining the safety and reliability of operations

ICS Security Leader

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 prioritising safety

Process Control Engineering

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

Where multiple courses are shown for a given role, determination of the best course to take would be based on the number of years of experience and sector of work.

ICS410: **ICS/SCADA Security Essentials™**

GICSP
Industrial Cyber Security
Professional
giac.org/gicsp

6	36	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

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

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 industrial control system 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 industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, 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 industrial control system 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.

GICSP
Industrial Cyber
Security Professional
giac.org/gicsp

Global Industrial Cyber Security Professional

The GICSP bridges together IT, engineering and cyber security to achieve security for industrial control systems from design through retirement. This unique vendor-neutral, practitioner focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

- Industrial control system components, purposes, deployments, significant drivers, and constraints
- 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

sans.org/ics410

ICS418: **ICS Security Essentials for Leaders™**

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

▌ Articulate the value of ICS security and tie cyber risk to business risk decisions

▌ Trend current and future technology changes to address business needs

▌ Measure successes in industrial cyber risk management, complete with metrics for executives and boards

▌ Use best practices to enable ICS security incident detection and response for their teams

▌ Leverage external information, including threat intelligence, to guide their ICS security program

▌ Provide governance, oversight, execution, and support across industrial facilities for ICS security initiatives and projects

▌ Apply the differences between IT and ICS security for an effective control system cybersecurity program

▌ Develop their security workforce to address gaps in hiring, training, and retention

▌ Apply advanced techniques to help shape and shift their organization's culture of security

Who Should Attend

ICS418 is aimed at leaders of staff who are responsible for securing the day-to-day running of operational technology and industrial control system environments across an organization—this includes distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Leaders of these teams often come from a diverse background with either a focus on management skills and minimal understanding of ICS environments, or technical individuals who rise in the ranks to a leader with minimal management skill development.

The course was designed to bridge the gap between those two skill sets, "raising the water level for all ships" when it comes to ICS security leaders, including:

▌ Leaders asked to "Step-Over"
 - Traditional information technology (IT) security manager that must create, lead, or refine an ICS Security program

▌ Practitioner to Leader: "Step-Up"
 - Industrial engineer, operator, or ICS security practitioner promoted to a manager position to create, lead, or refine an ICS security program

▌ Leader Development: "In-Place"
 - An existing ICS security manager that is looking to further develop their leadership skills, specific to industrial security

ICS security is an ever-changing field requiring practitioners to continually adapt defense strategies to meet new challenges and threats. To compound the issue, any security changes need to be thoroughly tested to maintain the safety and reliability of industrial operations.

Globally, "critical infrastructure" and "operators of essential services" represent hundreds of thousands—if not millions—of industrial organizations. Some of them are the lifelines to our modern society, like water, power, oil and gas, food processing, and critical manufacturing—but every industrial facility owner or operater must know their engineering processes are safe and secure. With increased threats, new technology trends, and evolving workforce demands, it is vital for security leaders in operational technology (OT) to be trained in techniques to defend their facilities and their teams.

The two-day ICS418 fills the identified gap amongst leaders working across critical infrastructure and OT environments. It equips new or existing leaders responsible for OT/ICS, or converged IT/OT cybersecurity. The course provides the experience and tools to address industry pressures to manage industrial cyber risk to prioritize the business, safety and the reliability of operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints that exist in these cyber-physical environments and will obtain a nuanced understanding of how to manage the people, processes, and technologies throughout their organizations.

This Course Will Prepare You To

▌ Develop ICS-specific cybersecurity programs and measure its impact across the organization

▌ Use management and leadership skills to communicate your ICS security vision to executives and other leaders

▌ Build (and keep) your ICS security team, using forecasting, capability modeling, and workforce planning

▌ Assess the overall effectiveness of your organization's industrial cyber risk management program

▌ Manage the various constraints across IT, OT, engineering, and physical security to improve your organization's culture

Authors Statement

Now, more than ever, it is important to train and equip ICS security leaders with the skills and knowledge they need to protect critical infrastructure—the critical engineering systems that make, more and power our world. This course is the culmination of decades of experience in building and managing OT/ICS security teams—and it is the course we wish was available to us when we started on our ICS security journey. We've drawn across our roles in different industrial sectors and teams—as former company executives, team leads, incident responders, and managers—to create a course empowering leaders facing the greatest challenge of our time: industrial control system cybersecurity.

—Jason D. Christopher & Dean C. Parsons

"This course is a must for managers in the ICS space, and I am sure many people out there are probably trying to build an OT security program based on IT standards and guidelines. This course did a great job of pointing out those differences and will benefit anyone that attends in the future."

—Jason R., **MP Materials**

ICS456: **Essentials for NERC Critical Infrastructure Protection™**

GCIP
Critical Infrastructure
Protection
giac.org/gcip

5	31	Laptop
Day Program	CPEs	Required

You Will Be Able To

▋ Understand the cybersecurity objectives of the NERC Critical Infrastructure Protection (CIP) standards

▋ Understand the NERC regulatory framework, its source of authority, and the process for developing CIP standards, as well as their relationship to the other Bulk Electric System (BES) reliability standards

▋ Speak fluent NERC CIP and understand how seemingly similar terms can have significantly different meanings and impacts on your compliance program

▋ Break down the complexity to more easily identify and categorize BES cyber assets and systems

▋ Develop better security management controls by understanding what makes for effective cybersecurity policies and procedures

▋ Understand physical and logical controls and monitoring requirements

▋ Make sense of the CIP-007 system management requirements and their relationship to CIP-010 configuration management requirements, and understand the multiple timelines for assessment and remediation of vulnerabilities

▋ Determine what makes for a sustainable personnel training and risk assessment program

▋ Develop strategies to protect and recover BES cyber system information

▋ Know the keys to developing and maintaining evidence that demonstrates compliance and be prepared to be an active member of the audit support team.

▋ Sharpen your CIP Ninja!

Who Should Attend

▋ IT and OT (ICS) cybersecurity

▋ Field support personnel

▋ Security operations personnel

▋ Incident response personnel

▋ Compliance staff

▋ Team leaders

▋ Persons involved in governance

▋ Vendors/Integrators

▋ Auditors

The five-day ICS456: Essentials for NERC Critical Infrastructure Protection empowers students with knowledge of the what and the 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 BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6/7 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

This course goes far beyond other NERC Critical Infrastructure Protection (CIP) courses that only teach what the standards are by providing information that will help you develop and maintain a defensible compliance program and achieve a better understanding of the technical aspects of the standards. Our 25 hands-on labs utilize three provided virtual machines that enable students to learn skills ranging from securing workstations to performing digital forensics and lock picking. Our students consistently tell us that these labs reinforce the learning and prepare them to do their jobs better.

You Will Learn:

▋ BES cyber system identification and strategies for lowering their impact rating

▋ Nuances of NERC-defined terms and the applicability of CIP standards and how subtle changes in definitions can have a big impact on your program

▋ The significance of properly determining cyber system impact ratings and strategies for minimising compliance exposure

▋ Strategic implementation approaches for supporting technologies

▋ How to manage recurring tasks and strategies for CIP program maintenance

▋ Effective implementations for cyber and physical access controls

▋ How to break down the complexity of NERC CIP in order to communicate with your leadership

▋ What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls

▋ How to understand the most recent Standards Development Team's efforts and how that may impact your current CIP program

"This is a great course that examines NERC CIP standards and compliance from a variety of perspectives. I recommend it to anyone working with CIP."

—Tom Duffey, **Accenture Security**

GCIP
Critical Infrastructure
Protection
giac.org/gcip

GIAC Critical Infrastructure Protection

"The bulk electric system or "the grid" is arguably the most critical of the critical infrastructures demanding that personnel charged with supporting it, understand the impact of their actions and inactions with regard to system reliability, safety and security. The GIAC Critical Infrastructure Protection will help validate that the professionals who access, support and maintain the critical systems that keep the grid running have an understanding of the regulatory requirements of NERC CIP as well as practical implementation strategies to achieve both regulatory compliance and its cybersecurity objectives." –Ted Gutierrez, co-author of SANS ICS456: Essentials for NERC Critical Infrastructure Protection

• BES cyber system identification and strategies for lowering their impact rating

• Nuances of NERC defined terms and CIP standards applicability

• Strategic implementation approaches for supporting technologies

• Recurring tasks and strategies for CIP program maintenance

ICS515: **ICS Visibility, Detection, and Response™**

GRID
Response and
Industrial Defense
giac.org/grid

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

▮ Analyze ICS-specific threats and take proper courses of action to defend the industrial control systems

▮ Establish collection, detection, and response strategies for your ICS networks

▮ Use proper procedures during ICS incident response

▮ Examine ICS networks and identify the assets and their data flows in order to understand the network information needed to identify advanced threats

▮ Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS

▮ Build your own Programmable Logic Controller using the SANS ICS515 Student Kit, which you retain after the class ends

▮ Gain in-depth knowledge on ICS targeted threats and malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and EKANS

▮ Leverage technical tools such as Shodan, Wireshark, Zeek, Suricata, Volatility, FTK Imager, PDF analyzers, PLC programming software, and more

▮ Create indicators of compromise (IOCs) in YARA

▮ Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, the Collection Management Framework, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

Who Should Attend

▮ ICS incident response team leads and members

▮ ICS and operations technology security personnel

▮ IT security professionals

▮ Security Operations Center team leads and analysts

▮ ICS red team and penetration testers

▮ Active defenders

> "ICS515 integrated the OT/ICS side of security into the course well, not like other courses I've taken that taught general IT security with OT added as an afterthought."
>
> —Josh Tanski, **Morton Salt**

ICS515: ICS Visibility, Detection, and Response will help you gain visibility and asset identification in your Industrial Control System (ICS)/Operational Technology (OT) networks, monitor for and detect cyber threats, deconstruct ICS cyber attacks to extract lessons learned, perform incident response, and take an intelligence-driven approach to executing a world-leading ICS cybersecurity program to ensure safe and reliable operations.

The course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This approach is important to being able to counter sophisticated threats such as those seen with malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and ransomware. In addition, the efforts are also critical to understanding and running a modern day complex automation environment and achieving root cause analysis for non cyber-related events that manifest over the network. Students can expect to come out of this course with core skills necessary for any ICS cybersecurity program.

The course uses a hands-on approach with numerous technical 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 threats. Students will also interact with and keep a programmable logic controller (PLC), physical kit emulating electric system operations at the generation, transmission, and distribution level, and virtual machine set up as a human machine interface (HMI) and engineering workstation (EWS).

Students will spend roughly half the course performing hands on skills across more than 25 technical exercises and an all day technical capstone. Students will gain a practical and technical understanding of defining an ICS cybersecurity strategy, leveraging threat intelligence, performing network security monitoring, and performing incident response. Frameworks such as the ICS Cyber Kill Chain, Collection Management Framework, and Active Cyber Defense Cycle will be taught to give students repeatable frameworks and models to leverage post class.

The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that ICS defense is do-able.

Author Statement

"This class was developed from my experiences in the U.S. intelligence community, at Dragos and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is do-able."

–Robert M. Lee

GRID
Response and Industrial Defense
giac.org/grid

GIAC Response and Industrial Defense

The GRID certification is for professionals who want to demonstrate that they can perform Active Defense strategies specific to and appropriate for an Industrial Control System (ICS) network and systems. Candidates are required to demonstrate an understanding of the Active Defense approach, ICS-specific attacks and how these attacks inform mitigation strategies. Candidates must also show an understanding of the strategies and fundamental techniques specific to core subjects with an ICS-focus such as network security monitoring (NSM), digital forensics and incident response (DFIR).

• Active Defense Concepts and Application, Detection and Analysis in an ICS environment

• Discovery and Monitoring in an ICS environment, ICS-focused Digital Forensics, and ICS-focused Incident Response

• Malware Analysis Techniques, Threat Analysis in an ICS environment, and Threat Intelligence Fundamentals

ICS612: **ICS Cybersecurity In-Depth™**

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

❚ Gain hands-on experience with typical assets found within an industrial environment, including Programmable Logic Controller (PLC), operator interfaces for local control, Human Machine Interface (HMI) servers, Historian server, switches, routers, and firewall(s).

❚ Gain an understanding of PLC execution through hands-on exercises.

❚ Identify security methods that can be applied to real-time control and Input/Output systems.

❚ Understand the pros and cons of various PLC and HMI architectures with recommendations for improving security postures of these real-time control systems.

❚ Identify where critical assets exist within an industrial environment.

❚ Understand the role and design of an Industrial Demilitarized Zone (IDMZ).

❚ Gain hands-on experience with firewalls placed within the industrial zone to achieve cell-to-cell isolation and perimeter restrictions.

❚ Dissect multiple industrial protocols to understand normal and abnormal traffic used in the operational control of assets.

❚ Gain an understanding of the role of IT network services within ICS and identify security methods that can be applied.

❚ Use the RELICS virtual machine for asset and traffic identification.

❚ Troubleshoot configuration errors within an operational environment.

❚ Understand adversary approaches in targeting and manipulating industrial control systems.

Who Should Attend

❚ ICS410 course alumni – students who have successfully completed ICS410: ICS/SCADA Security Essentials will have the base knowledge considered as a prerequisite for this course.

❚ Process control engineers

❚ Systems or safety system engineers

❚ Active defenders in ICS

❚ Anyone with significant control system experience interested in understanding processes and methods to secure the ICS environment

ICS-AWARE MALWARE AND ATTACKS ON CRITICAL INFRASTRUCTURE ARE INCREASING IN FREQUENCY AND SOPHISTICATION. YOU NEED TO IDENTIFY THREATS AND VULNERABILITIES AND METHODS TO SECURE YOUR ICS ENVIRONMENT. LET US SHOW YOU HOW!

The ICS612: ICS Cybersecurity In-Depth course will help you:

❚ Learn active and passive methods to safely gather information about an ICS environment

❚ Identify vulnerabilities in ICS environments

❚ Determine how attackers can maliciously interrupt and control processes and how to build defenses

❚ Implement proactive measures to prevent, detect, slow down, or stop attacks

❚ Understand ICS operations and what "normal" looks like

❚ Build choke points into an architecture and determine how they can be used to detect and respond to security incidents

❚ Manage complex ICS environments and develop the capability to detect and respond to ICS security events

The course concepts and learning objectives are primarily driven by the hands-on focused labs. The in-classroom lab setup was developed to simulate a real-world environment where a controller is monitoring/controlling devices deployed in the field along with a field-mounted touchscreen Human Machine Interface (HMI) available for local personnel to make needed process changes. Utilising operator workstations in a remotely located control center, system operators use a SCADA system to monitor and control the field equipment. Representative of a real ICS environment, the classroom setup includes a connection to the enterprise, allowing for data transfer (i.e., Historian), remote access, and other typical corporate functions.

The labs move students through a variety of exercises that demonstrate how an attacker can attack a poorly architected ICS (which, sadly, is not uncommon) and how defenders can secure and manage the environment.

"I loved that this course was lab heavy. I feel 100% more comfortable around OT equipment now. That's saying a lot since my background and experience has been strictly IT."

—Jim J., **Pilot Flying J**

"The pods and student kits offered provide a powerful, hands-on learning experience that exceeds expectations far beyond what any software simulation or slide-based lecture could do. Step-by-step instructions are good, but I really enjoyed when we had exercises that didn't have all the answers and forced the student to think critically about how to solve the problem. That's where real learning occurred for me."

—Joseph P., **Deloitte & Touche LLP**

sans.org/ics612

SANS ICS INSTRUCTORS

Tim Conway
Senior Instructor

Tim serves as the Technical Director – ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, performing contract and consulting work in the areas of ICS cybersecurity with a focus on energy environments.

Robert M. Lee
Faculty Fellow | @RobertMLee

Robert is the CEO and founder of his own company Dragos, Inc., that provides cybersecurity solutions for industrial control system networks. He was the first in the industry to publicly confirm the 2015 attack on the Ukraine power grid and wrote an industry-standard report on the attack, lessons learned, and what must be done to protect other infrastructure sites. Robert is the author of ICS515 and FOR578.

Justin Searle
Senior Instructor | @meeas

As the Director of ICS Security at InGuardians, Justin specializes in ICS security architecture design and penetration testing. He led the Smart Grid Security Architecture group in creating the NIST Interagency Report 7628 and has played key roles in the ASAP-SG, NESCOR, and SGIP. Justin is the owner of ControlThings LLC and is the course author of ICS410.

Mark Bristow
Certified Instructor | @kodefupanda

Jason D. Christopher
Certified Instructor | @jdchristopher

Jason Dely
Certified Instructor | @JasonJDely

Monta Elkins
Principal Instructor | @montaelkins

Stephen Mathezer
Certified Instructor | @mathezer

Dean Parsons
Principal Instructor | @deancybersec

Jeffrey Shearer
Certified Instructor

Kai Thomsen
Certified Instructor

Don C. Weber
Certified Instructor | @cutaway

SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

🌐 **ics.sans.org**

👤 **ics-community.sans.org/signup**

🐦 **@SANSICS**

in **linkedin.com/showcase/sans-ics**

▶ **youtube.com/c/SANSICSsecurity**

📞 **301-654-SANS (7267)**   ✉ **support@sans.org**