ICS310: **ICS Cybersecurity Foundations™**

1 Day Course	6 CPEs	Laptop Required

You Will Be Able To

- Master the key security measures to protect industrial systems
- Gain insights into IEC 62443, NIST 800-82, NIS2, and NERC CIP frameworks
- Learn common industry terms, system components, and digital versus analog operations
- Understand key trends, device fundamentals, and system inputs/outputs in OT environments
- Analyze case studies to see how ICS principles apply to real industry challenges

Business Takeaways

- Equip employees with the knowledge to identify common ICS components and implement effective cybersecurity measures across your operations.
- Prepare your workforce to counter adversarial tactics by leveraging insights from global case studies and proven defense strategies.
- Enable your team to implement customizable ICS controls that address industry-specific and regulatory challenges, improving overall resilience.

Hands-On ICS Security Training

The hands-on portion of ICS310 will utilize a course VM environment to examine an example process and the hardware, software, and protocols involved. Additional labs will examine approaches to manipulate a system to understand failure potential and misuse opportunities. The ICS310 exercises are designed to reinforce the implementation of the five Critical Controls, collection management framework, and ICS network analysis.

In this Industrial Control System (ICS) course, students will begin by developing a necessary understanding of mechanical and operational systems, which is further expanded upon to better understand how asset owners and operators have automated these environments. Multiple sectors are explored to highlight the commonalities across process environments from various industries and sectors. Understanding the common building blocks and operational criteria that exist in numerous sectors will help inform defenders on the essential areas to focus risk-based prioritized cybersecurity actions that support the larger operational mission.

We'll reference case studies from multiple sectors around the world that highlight cyber events in which a variety of adversarial tactics were employed to achieve their goals. These case studies cover IT attacks that impacted operations, attacks on operational targets based heavily on adversary manual activity, and attacks on operational targets that incorporated ICS-enabled malware. Through the analysis of these case studies, we'll uncover lessons learned and recommendations for successful defense strategies, including defender-focused actions that can be prioritized and pursued.

Sectors in different geographies will face unique regulatory requirements and standards, while some are lacking in any guidance. Practitioners and leaders alike who are looking for appropriate security controls will learn about the ICS five critical controls that can be customized and implemented across any environment.

Authors' Statements

"This course represents SANS's and our commitment to the community by providing a low-cost, fast-paced course that is perfect for introducing people to OT/ICS cybersecurity. It is our hope that people take this course to learn the fundamentals of automation and industrial environments while also gaining exposure to the latest cyber threats and security efforts. Students that take this course will be empowered to immediately apply what they learned and continue their journey to help protect our communities from the jerks that mean them harm."
—Robert M. Lee, SANS Fellow

"I believe a foundational course like ICS310 has been needed for a very long time in our community. Early on, some great introductory resources were made available to industry, and as we have seen expanding job roles and growing training needs for individuals entering the field of ICS/OT, we felt it was time to introduce a course that provided fundamental learning topics, informed by the work experiences of an author team with a diversity of perspectives on the topic of ICS/OT cybersecurity."
—Tim Conway, SANS Fellow

"You can't be expected to defend what you don't understand. With the right instruction, you can quickly understand the basic ICS building blocks that will serve you well as you move forward with more in-depth and complex ICS topics. It's much like learning a language—your foundation starts by learning the letters associated with the language. You then learn how letters form words, which lead to the creation of sentences, which are used to create paragraphs and eventually books. Just like learning a language, you shouldn't assume you can skip the fundamentals of industrial control systems as they are applied to control mechanical and process systems and successfully secure it. Everyone wants to jump into discussions about technical controls like firewalls or how ICS protocols work without understanding how an industrial control system works. It's where everyone should start their journey as an ICS security professional to get grounded on how industrial control systems work. Once you gain this knowledge, you'll be standing on a solid foundation to apply security controls in an industrial environment."
—Jeffrey Shearer, SANS Certified Instructor

What Is ICS Security?

ICS security practices and programs help defenders protect critical infrastructure systems like SCADA, DCS, and PLCs from cyber threats, physical attacks, and exploitation. It involves measures like network segmentation, access control, monitoring, vulnerability management, and incident response to ensure operational safety and reliability. With the increasing targeting of ICS by cybercriminals and state sponsored actors, robust security practices are essential to safeguard infrastructure, prevent disruptions, and protect public safety.

Section Descriptions

SECTION 1: Why ICS310 and ICS Curriculum View

The ICS310 course has been developed as a foundational course for those new to the ICS/OT field. In this section we'll cover who this course is intended for, where the course fits in a broader ICS cybersecurity practitioner training program, how the course was developed across multiple author perspectives, and where we see the course as a fit for those students taking any of the other SANS ICS security higher-level courses.

TOPICS: Meet the Author Team; Foundational Industrial Control System (ICS) Course Topic Areas; SANS and ICS History; Where Does ICS310 Fit Across the Broader Curriculum; Content Focus Areas; Lab and Exercise

SECTION 2: ICS and Automation Topics

In Section 2 we will establish an understanding of the basic building blocks of industrial control systems, how and why they are used, as well as cover some essential concepts in the design and maintenance of these environments. We'll build on this knowledge of the foundational components that make up our ICS/OT environments, highlighting how these systems are interconnected and interdependent, creating systems of systems that necessitate careful design considerations and operational practices to ensure safe, reliable, resilient systems.

TOPICS: Brief History of Automation; What are the Basic Building Blocks of an Automation System; Human Brain, Sensory and Muscle Reference; What are the Main Components Found in ICS; What is Digital Versus Analog; Product Development Lifecycle; What is a System of Systems

SECTION 3: ICS Trends and Threats

Section 3 layers in learning objectives that have a cybersecurity focus, along with discussions on the drivers and constraints facing both offensive and defensive teams dedicated to achieving goals and objectives throughout ICS/OT environments. This section addresses the cybersecurity-specific considerations across critical infrastructure and key resource sectors, as well as differentiation across IT and OT systems, terminology, and trends.

TOPICS: Critical Infrastructure Sectors; IT and OT Focus Areas; Common Terms; IT/OT Trends

SECTION 4: ICS Case Studies and World Events

Some of the most meaningful learning opportunities available are those that are shared or experienced, and in Section 4, the course will utilize case studies and world events to highlight specific lessons learned that can be implemented within your operational environments. While the case studies covered may not be specifically from within your sector of interest, there are most likely common devices, protocols, threat vectors, or response approaches that are directly applicable to you. What can be learned from real-world attacks and case studies will aid system defenders in prioritizing actions that matter.

TOPICS: Case Studies: Colonial Pipeline, Ukraine 2015, Ukraine 2016, World Events

SECTION 5: ICS Cybersecurity Standards and Guidelines

For those working in ICS/OT environments, there are often references to regulation, standards, or guidelines for a particular country, sector, or technology. Section 5 introduces the topic of security guidelines and standards that you will commonly encounter across industrial control systems, anywhere, any sector, in any geography. While there are full 5- and 6-day dedicated courses or a suite of courses for some of the standards that exist, this section simply highlights the different types of standards for familiarity and reference.

TOPICS: Security Guidelines and Standards Commonly Encountered Within the ICS/OT community; Top Three: IEC62443, NIST 800-82, NERC CIP: European Union Regulation NIS2: Industry Approach

SECTION 6: ICS Five Critical Controls

With so many options to pursue across standards, regulations, guidelines, and industry recommendations, often organizations and leadership are looking for a clear path of what to do. Section 6 addresses this question and provides guidance on the ICS five critical controls. The authors of this course considered existing controls frameworks and asked, "If we wrote the critical controls (like the SANS 20 critical controls for IT) for OT, what would they be?" This section considers the prioritization, implementation, and customization of the critical controls for your organization and provides background on the selection of these controls as the minimum preventive and detective controls that are threat informed, have been identified based on attacks that have been seen, and consider the capabilities available to system defenders.

TOPICS: The Five Critical ICS Security Controls; Leadership Role

Who Should Attend

- Students who are new to ICS
- Future ICS curriculum students
- OT security professionals from regulated industries and critical infrastructure
- OT security professionals from non-regulated industries
- Vendor/integrator professionals
- Anyone in the critical infrastructure/key resource industries (electric, water, nuclear, telecom, oil, natural gas, manufacturing, chemical, rail, transportation, etc.) specifically, the operational technology environments within these organizations
- DoD personnel interested in operational environments that utilize or support cyber to physical assets