Industrial Control Systems (ICS) Security Resources

Sponsors

To get your free vendor-sponsored whitepaper, visit ***www.sans.org/tools.php***

INDUSTRIAL DEFENDER® — *WHITEPAPER:* ***SANS 20 Critical Controls: Key Considerations for Industrial Control Systems***
www.industrialdefender.com

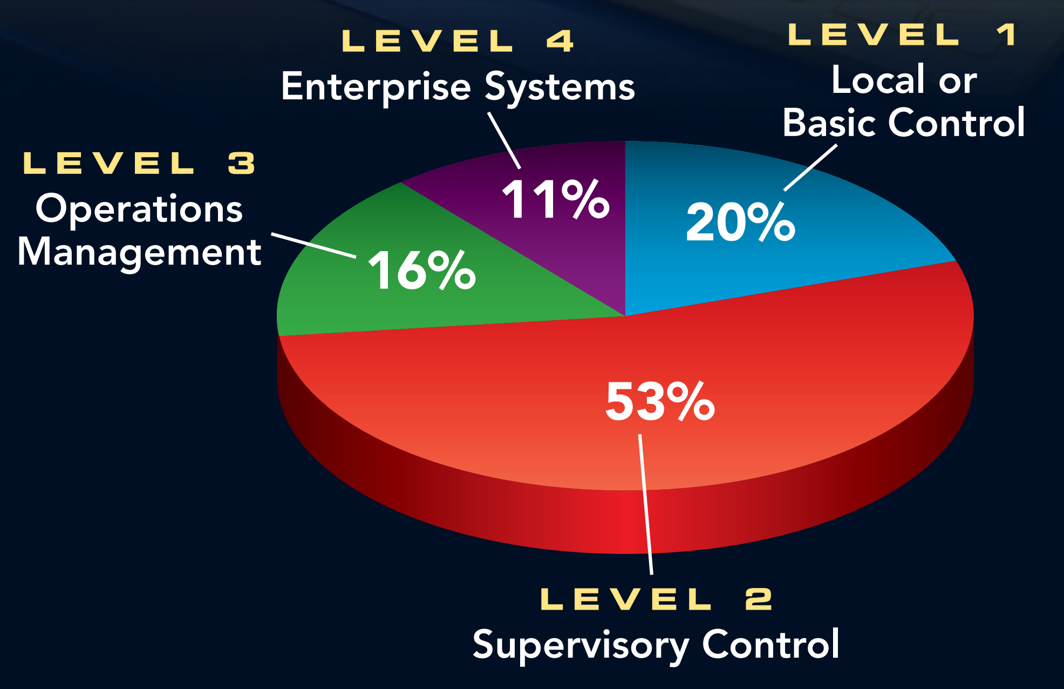
TREND MICRO™ | Securing Your Journey to the Cloud — *WHITEPAPER:* ***The SCADA That Didn't Cry Wolf: Who's Really Attacking Your ICS Equipment?***
www.trendmicro.com

WATERFALL *One Way to Connect* — *WHITEPAPER:* ***Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security***
www.waterfall-security.com

Rockwell Automation
www.rockwellautomation.com/security

CONTROL ENGINEERING
www.controleng.com

DHS Common Cybersecurity Vulnerabilities in Industrial Control Systems



SANS ICS

Industrial Control Systems

Security Resources

POSTER

FALL 2013 | 26TH EDITION

SANS, working with industry experts, is making a difference in the Industrial Control System (ICS) cyber security front. SANS has joined forces with industry leaders to, change the game, by equipping both security professionals and control system engineers with the security awareness, work specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS ICS team is working to provide ICS focused curriculum and certifications, as well as community resources including posters, white papers, and security practice application guidance. SANS has engaged the dedicated practitioner community that assembles during our global and regional ICS summits, and leverage leaders from enterprises, governments, and vendors from around the globe to tackle our common challenges and share working solutions.

BUSINESS ZONE

LEVEL 5

Enterprise Business Network

Corporate level applications used to support Enterprise Business and User Goals. Items typically found in this zone include; Internet access points, Email servers, customer facing web servers, internal web servers, CRM systems, HR systems, corporate directory architectures, enterprise document management systems, and remote access VPN endpoints.

LEVEL 4

Business Unit or Plant Network

IT shared services for a local site, business unit, or subsidiaries. Items typically found in this zone include; local file and print servers, local phone systems, site directory replicas, site specific remote access solutions, security event aggregators, and site specific Internet access points.

DEMILITARIZED ZONE

DMZ

Provides a series of function specific zones where services and data can be shared between the zones. Items typically found in this zone include; patch management servers, Anti-Virus management systems, site specific application servers, jump host environments, business intelligence systems, backend databases for site specific applications, and development systems.

OPERATIONS ZONE

LEVEL 3

Operations Support DMZ

Includes the functions involved in managing the operations environment. Items typically found in this zone include; operations scheduling resources, reliability tracking tools, operations simulation and modeling tools, contingency analysis tools, replicated historians, and data visualization utilities. There may also be dedicated operations specific IT services such as DHCP, LDAP, DNS, and file servers.

PROCESS CONTROL/ SCADA ZONE

LEVEL 2

Supervisory Control LAN

Includes the functions involved with operating the real-time control system. Items typically found in this zone include; control center operation workstations, Human Machine Interfaces (HMI), engineering workstations, security event collectors, operations alarm systems, communications front ends, data historians, and network / application administrator workstations.

LEVEL 1

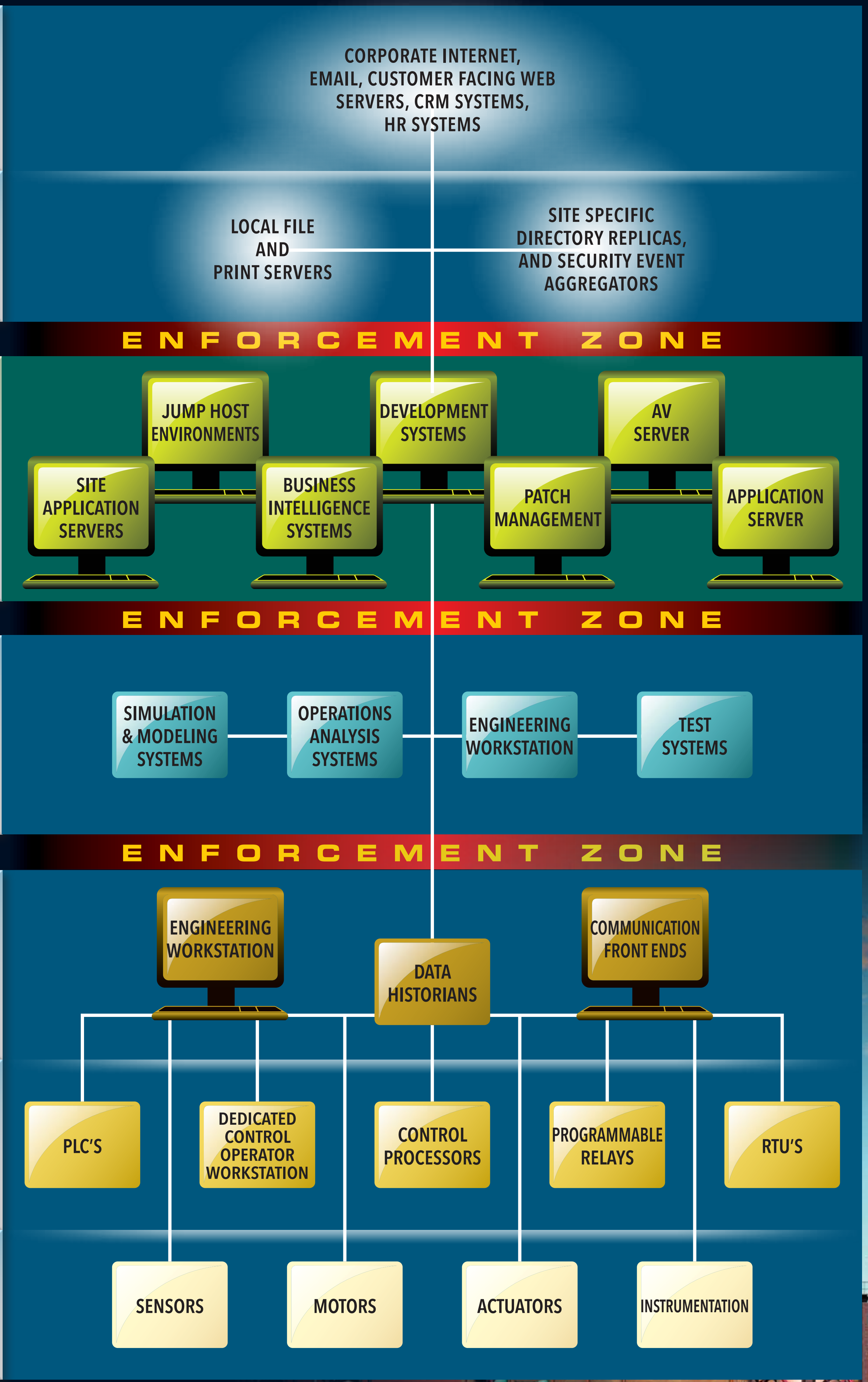
Control Devices

Includes the functions involved at site specific operating environments. Items typically found in this zone include; dedicated operator workstation, Programmable Logic Controllers, control processors, programmable relays, Remote Terminal Units, and process specific microcontrollers.

LEVEL 0

Process Control Instrumentation Bus Network

Includes the functions involved in transitioning from cyber to physical and from physical to cyber. Items typically found in this zone include; sensors, actuators, motors, process specific automation machinery and field instrumentation devices.



SAFETY ZONE

Safety Zone

Safety specific systems that are engineered for a specific protective function. Items typically found in this zone include all items identified in Level 0 and 1 with a dedicated purpose for a safety control function like; acoustic monitoring, liquid chemistry monitoring, vibration monitoring, emission monitoring and in most safety systems there exists a control function that serves to protect the operation and personnel.

ENFORCEMENT ZONE

Enforcement Zone

Includes the functions necessary to segment and protect the various zones within an ICS environment. Items typically found in this zone include; Firewalls, Routers (with ACL's), Application Firewalls, Data Guard technology, and unidirectional data diode technology. Technologies implemented may differ at the various enforcement zones within an ICS environment depending on the business needs and the level of risk determined at a specific enforcement zone.

SANS ICS410: ICS/SCADA Security Essentials

Five-Day Program | Laptop Required | 30 CPE/CMUs

The SANS Industrial Control Systems Team is working to develop a curriculum of focused ICS courseware to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures. The entry-level course in the SANS ICS Curriculum is ICS410: ICS/SCADA Security Essentials

This course provides students with the essentials for conducting security work in Industrial Control System (ICS) environments. Students will learn the language, the underlying theory and the basic tools for ICS security in industrial settings across a diverse set of industry sectors and applications. This course will introduce students to ICS and provide the necessary information and learning to secure control systems while keeping the operational environment safe, reliable, and resilient.

Global ICS Professional Certification

GIAC, working with industry experts, has developed a vendor neutral, practitioner-focused Industrial Control System certification.

The Global Industrial Cyber Security Professional Certification (GICSP) assesses 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. This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that an IT, engineer, and security professional should know if they are in a role that could impact the cybersecurity of an ICS environment.

Securing the Human

SANS has expanded the focus of the popular Securing the Human product into two ICS focused areas. First, **Securing the Human for Utilities** is a computer-based training program with specific focus on the NERC CIP Standards. This training consists of seven core modules that provide an overview of NERC and FERC, an Introduction to the NERC CIP Standards, and a series of topics on physical and electronic access controls, as well as information protection and incident response.

In addition, SANS has developed **Securing the Human for Engineers**, which focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. This training consists of 10 core modules and provides an ICS overview, an understanding of ICS attacks, and covers basic system and network defense approaches in an ICS environment, as well as governance and policy resources.

These programs were developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also change human behavior and reduce risk.

SANS ICS Resources

SANS ICS Homepage
http//www.sans.org/ics

DHS ICS-CERT
http://ics-cert.us-cert.gov

DHS Cybersecurity Evaluation Tool
http://ics-cert.us-cert.gov/Assessments

NERC ES-ISAC
http://www.esisac.com/SitePages/Home.aspx

ICS-ISAC
http://ics-isac.org

Cybersecurity Vulnerability NSTB Program
http://energy.gov/oe/downloads/common-cyber-security-vulnerabilities-observed-control-system-assessments-inl-nstb

Vulnerability Analysis of Energy Delivery Control Systems
http://energy.gov/oe/downloads/vulnerability-analysis-energy-delivery-control-systems

NIST SP 800-82 Guide to ICS Security
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

ISA-99 Control System Security Committee
http://isa99.isa.org/ISA99%20Wiki/Home.aspx

NERC CIP Standards
http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

Control Systems Are a Target

www.sans.org/ics

www.securingthehuman.org

Network Access

- Internet accessible systems are being mapped by ERIPP or SHODAN, or are easily locatable through search engine queries
- Malware can spread vertically through the network by trusted system to system connections or VPN
- It is very easy to maneuver undetected throughout a control environment
- There is potential to leverage non-routable trusted communication paths

Interconnects

- ICS systems can be attacked by exploiting applications that communicate through network segmentation
- Connections to other organizations, plants or systems
- Many ICS environments are susceptible to network-based Man in the Middle Attacks

Dial-Up

- ICS assets can be remotely accessible through traditional dial-up modems that have little access control protections
- Numerous ICS assets at a location can be accessed through a single dial-up access point with a multiplex device that enables connections to many ICS assets
- Old attack vectors can still be successful in ICS environments

System Management

- Attackers can take advantage of long delays in patching and operating system upgrades
- Attackers can take advantage of systems with no anti-virus, or out-of-date signatures
- Attackers will leverage default usernames and passwords or weak authentication mechanisms
- Attacks will be difficult to detect due to minimal asset security logging capability
- Attackers will leverage file access techniques to move data in and out of the ICS environment through physical removable media or trusted communication paths utilized for system maintenance

Supply Chain

- Third party vendors, contractors or integrators can be attacked in an attempt to ultimately attack an ICS asset owner or multiple asset owners
- ICS hardware and software can be directly breached or impacted prior to arriving in the production ICS environment

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reenforce secure behaviors when interacting with an Industrial Control System.

In many cases these are not one-off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and operators to be vigilant and recognize when something is not right.

ICS Security goal: Ensure the safe, reliable and secure operation of ICS environments from procurement to retirement

Abnormal activity or unexplained errors deserve a closer security look

Governance

- Attackers can leverage the lack of corporate security policies, procurement language, asset inventory and standardization that exist in many ICS environments
- Attackers can have greater impacts on ICS environments, as ICS assets are often not considered in the preparation phase of security incident response planning and containment approaches
- ICS risk and hazard assessment are not always evaluated with the loss of cyber integrity which, can lead to a loss of availability, impacts due to interdependencies and misuse of critical components or functions
- In some sectors ICS assets are often architected or assessed from a compliance perspective and not always assessed from a security perspective

Social Engineering

- Request for Proposals often contain a wealth of information regarding an ICS environment
- Vendors frequently post information about a project they are working on for an ICS customer
- Employee social media sites often contain technology architecture information and, possibly, images of ICS work environments
- Engineer professional bios can provide a helpful map of your ICS
- Publically available information regarding an ICS asset owners' vendor relationships, conference attendance, committee participation and domain registrations can all be leveraged against the organization

Physical Security

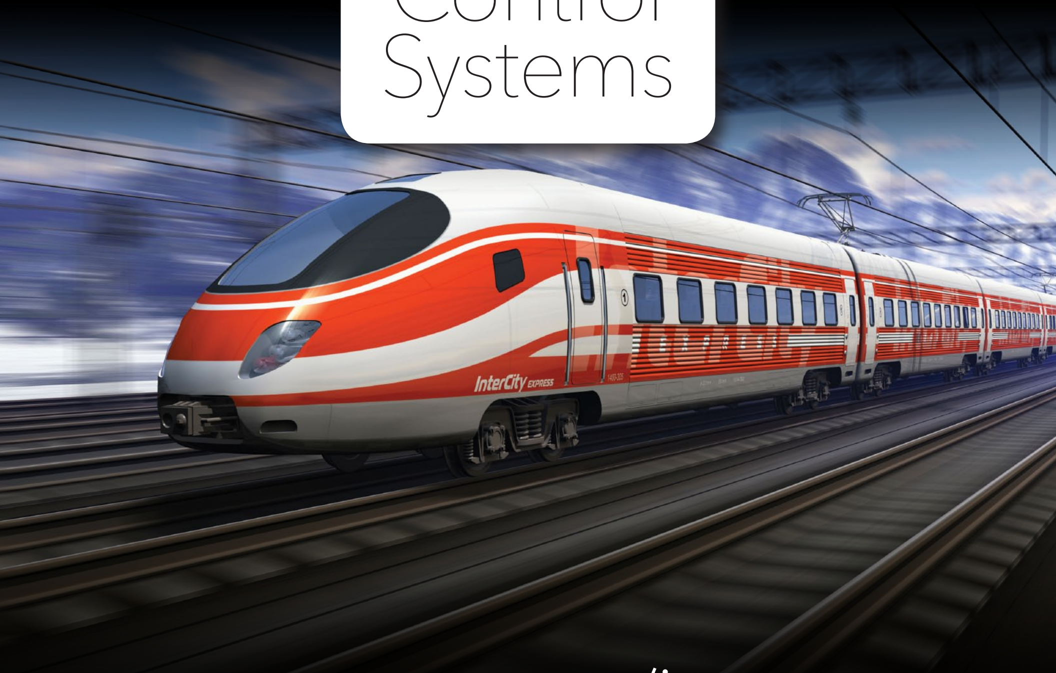
- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access to sensitive information that could be used in planning an attack
- Physical changes or alterations to ICS devices are often difficult to detect

Cyber Actors

- Nation States
- Insiders and other trusted parties (such as contractors / vendors / integrators)
- Criminal Hacker
- Politically motivated attackers (hacktivists)
- Script Kiddies

SANS ICS

Industrial Control Systems

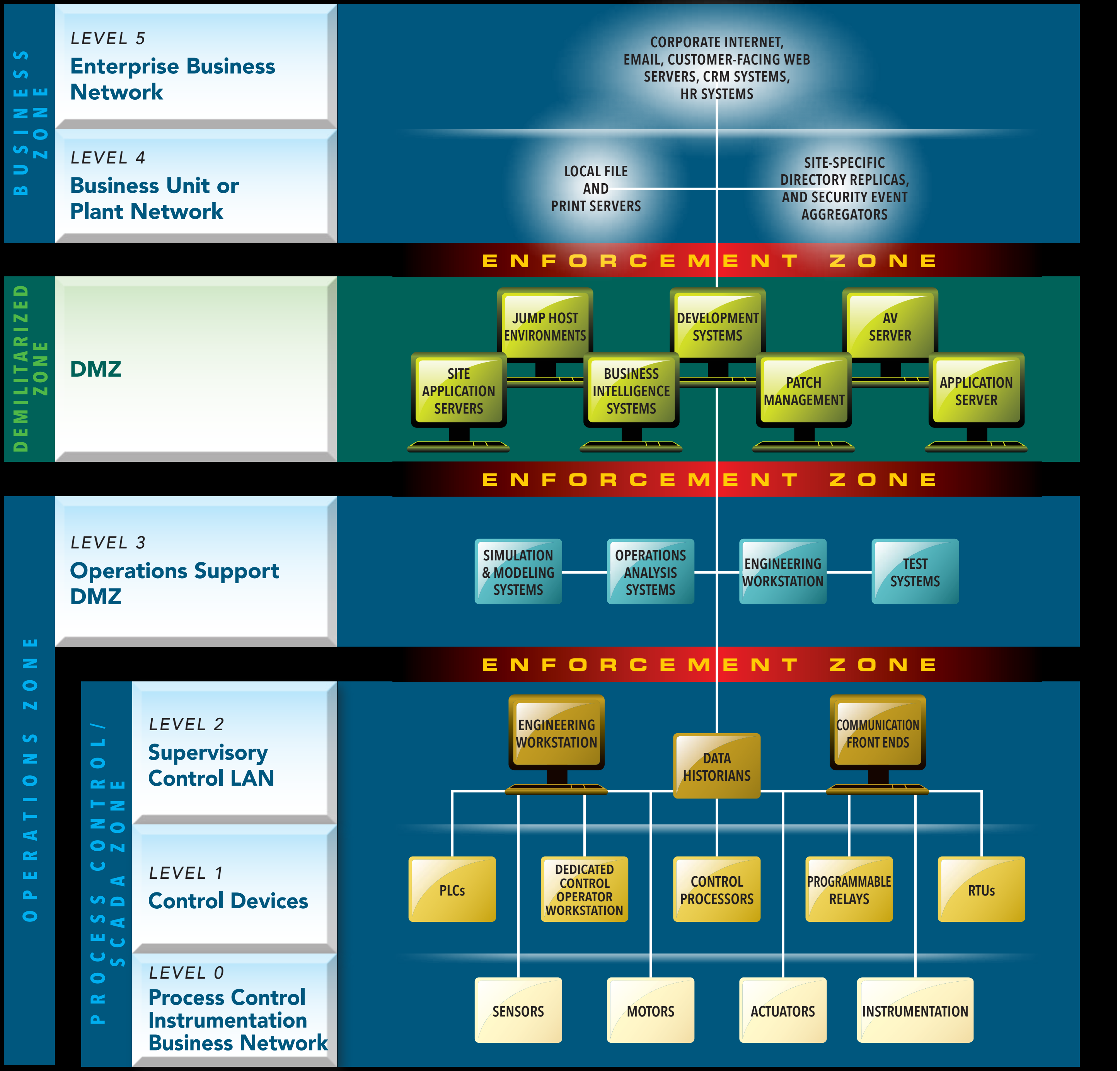


www.sans.org/ics

Why ICS?

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of Industrial Control Systems (ICS). The initiative is equipping security professionals and control system engineers with the security awareness, work-specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS team is working to provide ICS-focused curricula and certifications, as well as community resources such as promotional materials, white papers, and security practice application guidance.

Industrial Control Systems Architecture



BUSINESS ZONE

LEVEL 5
Enterprise Business Network

CORPORATE INTERNET, EMAIL, CUSTOMER-FACING WEB SERVERS, CRM SYSTEMS, HR SYSTEMS

LEVEL 4
Business Unit or Plant Network

LOCAL FILE AND PRINT SERVERS

SITE-SPECIFIC DIRECTORY REPLICAS, AND SECURITY EVENT AGGREGATORS

ENFORCEMENT ZONE

DEMILITARIZED ZONE

DMZ

JUMP HOST ENVIRONMENTS

DEVELOPMENT SYSTEMS

AV SERVER

SITE APPLICATION SERVERS

BUSINESS INTELLIGENCE SYSTEMS

PATCH MANAGEMENT

APPLICATION SERVER

ENFORCEMENT ZONE

OPERATIONS ZONE

LEVEL 3
Operations Support DMZ

SIMULATION & MODELING SYSTEMS

OPERATIONS ANALYSIS SYSTEMS

ENGINEERING WORKSTATION

TEST SYSTEMS

ENFORCEMENT ZONE

PROCESS CONTROL/ SCADA ZONE

LEVEL 2
Supervisory Control LAN

ENGINEERING WORKSTATION

DATA HISTORIANS

COMMUNICATION FRONT ENDS

LEVEL 1
Control Devices

PLCs

DEDICATED CONTROL OPERATOR WORKSTATION

CONTROL PROCESSORS

PROGRAMMABLE RELAYS

RTUs

LEVEL 0
Process Control Instrumentation Business Network

SENSORS

MOTORS

ACTUATORS

INSTRUMENTATION

Why Is the ICS Initiative Important?

- Tremendous gains are being achieved in industrial applications by sharing and analyzing data, but we need professionals who can address the security challenges.
- Preparation is critical because ICS incidents are occurring with increasing frequency and damaging systems.
- Control systems are widely deployed and need your attention – there is no such thing as a system that is too small.
- Up-to-date ICS knowledge and security skills can help keep our critical systems safe.
- Shared learning translates into results – effective security requires the integration of cybersecurity professionals, ICS support staff, and engineers.

SAFETY ZONE

Includes safety-specific systems that are engineered for a particular protective function. Items typically found in this zone are all those identified in Level 0 and 1 with a dedicated purpose for a safety control function, including: acoustic monitoring, liquid chemistry monitoring, vibration monitoring, and emission monitoring. In most safety systems, there is a control function that serves to protect the operation and personnel.

ENFORCEMENT ZONE

Includes the functions necessary to segment and protect the various zones within an ICS environment. Items typically found in this zone include Firewalls, Routers (with ACLs), Application Firewalls, Data Guard technology, Unidirectional Gateways, and Data Diodes. Technologies implemented may differ in the various enforcement zones within an ICS environment depending on business needs and the level of risk.

ICS410: ICS/SCADA Security Essentials

NEW

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

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 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 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 industrial control system 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.

Because of the dynamic nature of industrial control systems, 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 does system reliability throughout the system lifecycle.

Who Should Attend:

Individuals who influence the attack surface and are responsible for or support efforts to maintain a secure, safe and reliable Industrial Control System environment. The roles performed by personnel specific to this field can be divided in four domains:

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

GICSP Global Industrial Cyber Security Professional

www.giac.org

When personnel working in one of the domains above complete this course, they will have an appreciation, understanding and common language for industrial control system security that will enable them to work together with others in these domains to better secure their common 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.

Course Day Topics

Day 1 ICS Overview

- History of ICS
- Overview of ICS
- Field Components
- Network Components
- Communications
- ICS Application Overview
- Industry Models
- ICS Drivers and Constraints
- Physical Security and Safety Systems

Day 2 ICS Attack Surface

- Overview of Attacks
- Attacks on HMIs
- Attacks on Control Servers
- Attacks on Network Communications
- Attacks on Remote Devices

> "Excellent content and very informative."
>
> –Khalid Alsomaly, Saudi Aramco

Day 3 Defending ICS Servers and Workstations

- ICS Server and Workstation Technologies
- Microsoft Windows Based Systems
  - The Security Infrastructure
  - Security Policies and Templates
  - Service Packs, Patches, and Backups
  - Auditing and Automation
- Unix and Linux Based Systems
  - Linux Landscape
  - Linux Command Line
  - Linux Security Tools
  - Maintenance, Monitoring, and Auditing Linux

Day 4 Defending ICS Networks and Devices

- Network Fundamentals
- IP Concepts
- IP Behavior
- Firewalls and Perimeters
- Wireless
- Cryptography for ICS
- Controller and Field-Device Security

Day 5 ICS Governance and Resources

- Information Assurance Foundations
- Computer Security Policies
- Contingency and Continuity Planning
- Risk Assessment and Auditing
- Password Management
- ICS Incident Handling
- Resources

HOSTED: SCADA Security Training

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

This is a hands-on SCADA Security course with more than 20 exercises and labs that are performed on a portable SCADA lab that contains over 15 different PLCs, RTUs, RF, and telemetry devices. The course has already trained more than 1,300 professionals around the world, and has been constantly refined over the past four years. It was designed to bridge the skill sets of Control System Engineers, Technicians, and IT Security professionals. The first day is spent diving deep into teaching how ICS and SCADA Systems work from the ground up. Instrumentation, I/O, control techniques, automation theory, HMI visualization, and data archival systems are broken down at their functional level. Several SCADA protocols are taught, captured, dissected, and then used to hack into the embedded devices. OPC, ModbusTCP, and EthernetIP are some of the ICS protocols that are used in live hands-on exercises and labs.

Everyone in the course builds their own SCADA system by implementing and designing their own OPC servers, data tags, and HMI graphics. RF and telemetry systems used in SCADA, ICS, and Smart Grid applications are covered, and live demonstrations are provided on the following RF systems: 900 MHz Spread Spectrum, Zigbee (802.15.4), WirelessHART, Bluetooth, and WiFi (2.4 and 5.6 GHz). Wireless hacking demonstrations convey the weaknesses and security hardening required when using wireless systems in ICS and SCADA applications.

Once all of the ICS and RF concepts are completely understood, the course shifts into a penetration and exploitation mindset. The students are taught how to find security vulnerabilities in ICS and SCADA system components, how to safely conduct penetration testing against live ICS and SCADA systems, and how to conduct Cyber Vulnerability Assessments that satisfy the NERC CIP and DHS CFATS regulations. The Metasploit framework is taught using the BackTrack environment. The hands-on exercises start with basic Linux commands, and by the end of the course, students are creating their own buffer overflows and other exploits using Metasploit, NETCAT, HPING, and other open-source tools.

After everyone has built their own SCADA system, and spent time learning how to attack these real-time systems, the course rounds out the process by explaining how to defend these systems from similar threats. The defense techniques include how to design secure SCADA architectures, where to place firewalls, how to implement secure remote access into SCADA environments, where to deploy IDS/IPS systems, and tips for implementing centralized log aggregation and network monitoring solutions.

The instructors for this course collectively have more than 20 years of experience conducting Cybersecurity Penetration Testing and Vulnerability Assessments on live operational ICS and SCADA Systems. This makes them uniquely qualified to provide the tips and feedback necessary to address the complex problems brought to them by students during the course.

This Course Will Answer the Questions Below – and Many More – Related to SCADA Security

- What are the unique vulnerabilities and security risks of ICS systems?
- What approach should be used to test Internet, Enterprise IT, and ICS systems for security vulnerabilities?
- What are the common security weaknesses in Internet and Enterprise IT Systems that pose the greatest risk to ICS systems?
- Can poorly managed ICS systems pose an even greater risk to Enterprise IT and Internet-connected systems?
- What is a solid approach to testing SCADA systems for security vulnerabilities?
- When and how do you conduct penetration testing on live SCADA equipment?
- How do you use open-source security tools to research and discover unknown vulnerabilities with ICS equipment?
- What are solid techniques for securing SCADA systems that are not vendor-specific, and require low administrative overhead?
- Can social networking information about employees found on sites like Facebook, Linkedin, MySpace, and Twitter be used to compromise critical industrial facilities?
- What is a Red Team or Tiger Team Attack Exercise, and how can these scenarios simulate a targeted attack on a SCADA facility?

HOSTED: Assessing and Exploiting Control Systems

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

This is not your traditional SCADA security course! This course teaches hands-on penetration testing techniques used to test embedded electronic field devices, network protocols, RF communications, and controlling servers of ICS and Smart Grid systems like PLCs, RTUs, smart meters, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. The course is structured around the formal penetration testing methodology created by the National Energy Sector Cybersecurity Organization Resource (NESCOR), a U.S. Department of Energy project.

Using this methodology and SamuraiSTFU (Security Testing Framework for Utilities), an open-source Linux distribution for pentesting energy sector systems and other critical infrastructure, we'll perform hands-on penetration testing tasks on embedded electronic field devices, their RF communications, and the myriad of user interfaces used throughout smart grid systems. We'll tie these techniques and exercises back to the smart grid devices that can be tested using these techniques. We will also do exercises on dissecting and fuzzing smart grid protocols like modbus, DNP3, IEC 61850, ICCP, ZigBee, C37.118, and C12.22. The course exercises will be performed on a mixture of real-world and simulated devices to give students the most realistic experience possible in a portable classroom setting.

> *"Very practical. An outstanding course!"*
>
> –Terry Ingoldsby, Amenaza Tech

You Will Be Able To:

- Explain the steps and methodology used in performing penetration tests on Industrial Control and Smart Grid systems
- Use the free and open-source tools in SamuraiSTFU to discover and identify vulnerabilities in web applications
- Exploit several hardware, network, user interface, and server-side vulnerabilities

What You Will Receive

- Latest version of SamuraiSTFU (Security Testing Framework for Utilities)
- A PDF version of the course slide deck
- Student hardware kits to use in class that must be returned at the end of class
- List of hardware items in the student kits and links to where students can purchase their own kits

HOSTED: Critical Infrastructure and Control System Cybersecurity

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

This is an intermediate-to-advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. The course will provide hands-on analysis of control system environments, allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls.

Who Should Attend:

- Security personnel whose job involves assessing, deploying, or securing control system components, communications and operations
- Programmers and network and system administrators supporting control systems
- Process engineers and field technicians
- Operations and plant management personnel
- Control system vendor personnel
- Penetration testers
- NERC CIP, DHS CFATS and other auditors who need to build deeper technical skills
- Computer emergency response teams

What are the security risks of control system components, communication protocols, and operations?

Whether the control system is automating an industrial facility or a local amusement park roller coaster, the system was designed to operate in a physically, cyber and operationally secure domain. This domain extends throughout the facility using a combination of Programmable Logic Controllers, Programmable Automation Controllers, Embedded Logic Controllers, Remote Terminal Units, and Human Machine Interfaces interlinked with one or a variety of SCADA systems and communication protocols across local and long-distance geographic regions. The risks vary from simple eavesdropping or electronic denial of service to more sophisticated asset misuse and destruction. To further compound the challenge, today there are not enough professionals with security skills to sufficiently deter, detect and defend against active threats to our critical infrastructure's control systems.

How can you progress from control system security policy development to design, deployment, and assessment?

This course was designed to help organizations struggling with control system cybersecurity by equipping personnel with the skills needed to design, deploy, operate, and assess a control system's cybersecurity architecture. The course begins by quickly describing the risks and then introducing the participants to a customizable actuator and sensor control system trainer and programmable logic environment. This automation programming analysis creates the platform to identify logic flaws that, combined with active cyber, physical, and operational procedures, may lead to increased risk. The participants then use this knowledge to analyze the cyber, physical, and operational risks to control system architecture through:

- **Control system component engineered, programmed and firmware logic flaws**
- **Wired and wireless communication protocol analysis**
- **Physical, cyber and operational procedures**
- **Deterrence, detection and response to threats**

The participant's knowledge is challenged through non-kinetic and kinetic analysis associated with common industry components as well as red team/blue team exercises of both physical and simulated control system environments such as traffic lights, chemical storage and mixing, pipelines, robotic arms, heavy rail, and power grids.

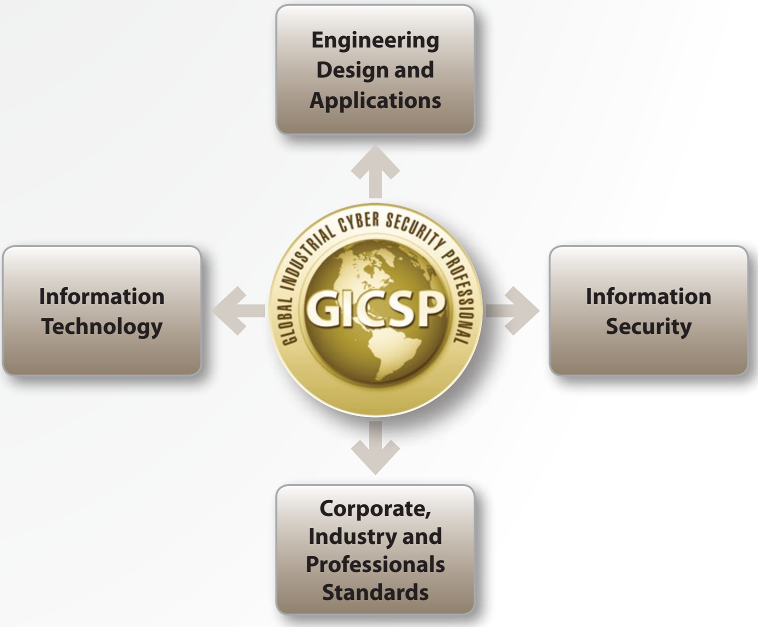
GIAC Global Industrial Cyber Security Professional (GICSP)

The GICSP exam has 115 questions and a time limit of three hours. Once achieved, the GICSP certification is valid for four years.

The GICSP certification focuses on the knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity 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.

This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineering, and security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment.


Engineering Design and Applications
Information Technology
GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP
Information Security
Corporate, Industry and Professionals Standards

GICSP Certification Objectives

- ICS Architecture
- ICS Security Assessments
- Industrial Control Systems
- ICS Modules and Elements Hardening
- Cybersecurity Essentials for ICS
- Configuration/Change Management
- ICS Security Governance and Risk Management

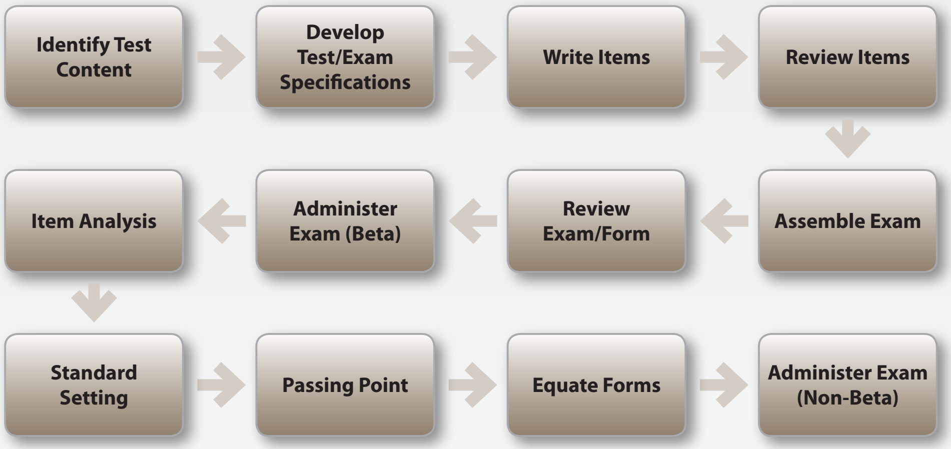
For a complete list of GICSP certification objectives, visit ***www.giac.org***

The GIAC Certification Process

GIAC has the most technical certifications in the information security field. A GIAC certification demonstrates that holders have the skills and knowledge associated with the certifications they hold. The development of the GIAC exams involves a team of dedicated subject-matter experts (SMEs), volunteers who are leaders in the information security field, and a rigorous validation process. The GIAC certification process is also used to develop other exams, including eight ANSI ISO/IEC 17024:2003 accredited exams. The ANSI-approved certifications are GSEC, GCIA, GCIH, GCFA, GPEN, GSLC, and GSNA.

The certification process includes 12 steps and takes about 16 months from conception to completion.

Test Development/Assessment Certification Process



Identify Content

GIAC researches information security topics and collaborates with SMEs to determine the topics and contents of new exams.

Develop Specifications

GIAC technical directors and SMEs develop the exam specifications.

Write Items

SMEs write all of the GIAC exam items and each item is reviewed across three levels, using a minimum of three SMEs.

Level 1: Reviewed by another SME

Level 2: Reviewed by a second SME

Level 3: Reviewed by a GIAC technical director who is also a SME.

The GIAC Certification Exam Review Process:

- Review format, clarity, style, grammar, and spelling
- Properly cite and use appropriate references
- Provide rationale
- Assign the proper certification objective
- Determine cognitive level
- Verify key as the correct answer among the other options
- Develop plausible and attractive distractors
- Avoid negative phrasing of stem (e.g., NOT)
- Avoid trivial information in the stem and options

Review Items

At each review level, SMEs determine if each item should be accepted, revised or rejected. All items are banked and maintained in GIAC's Exam Management System (EMS). The GIAC EMS also maintains exam and item performance criteria and statistical information for quality measures and metrics.

Assemble Exam

Items are assembled into an exam format.

Administer Beta Exam

Once the exam is assembled, GIAC recruits beta testers. These beta testers take the exam and provide feedback. The GIAC technical directors review the feedback and make any necessary adjustments to the exam to assure that it meets test performance criteria and metrics.

Item Analysis

GIAC also conducts item analysis reviews at least once a year. Three indices are used when assessing item performance.

1. **Item Difficulty** – The percentage of candidates who answer the item correctly
2. **Item Discrimination** – Measured using the point-biserial correlations (RPBi). The RPBI suggests whether candidates with high scores are answering the questions correctly and vice versa.
3. **Distractor Response Distributions** – Distribution of the items, which includes the number of candidates answering for each option and the point-biserial correlations.

Standard Setting and Passing Point

A standard setting study using SMEs determines a recommended cut score or passing score. GIAC's scheme committee determines the passing point for the certification exam.

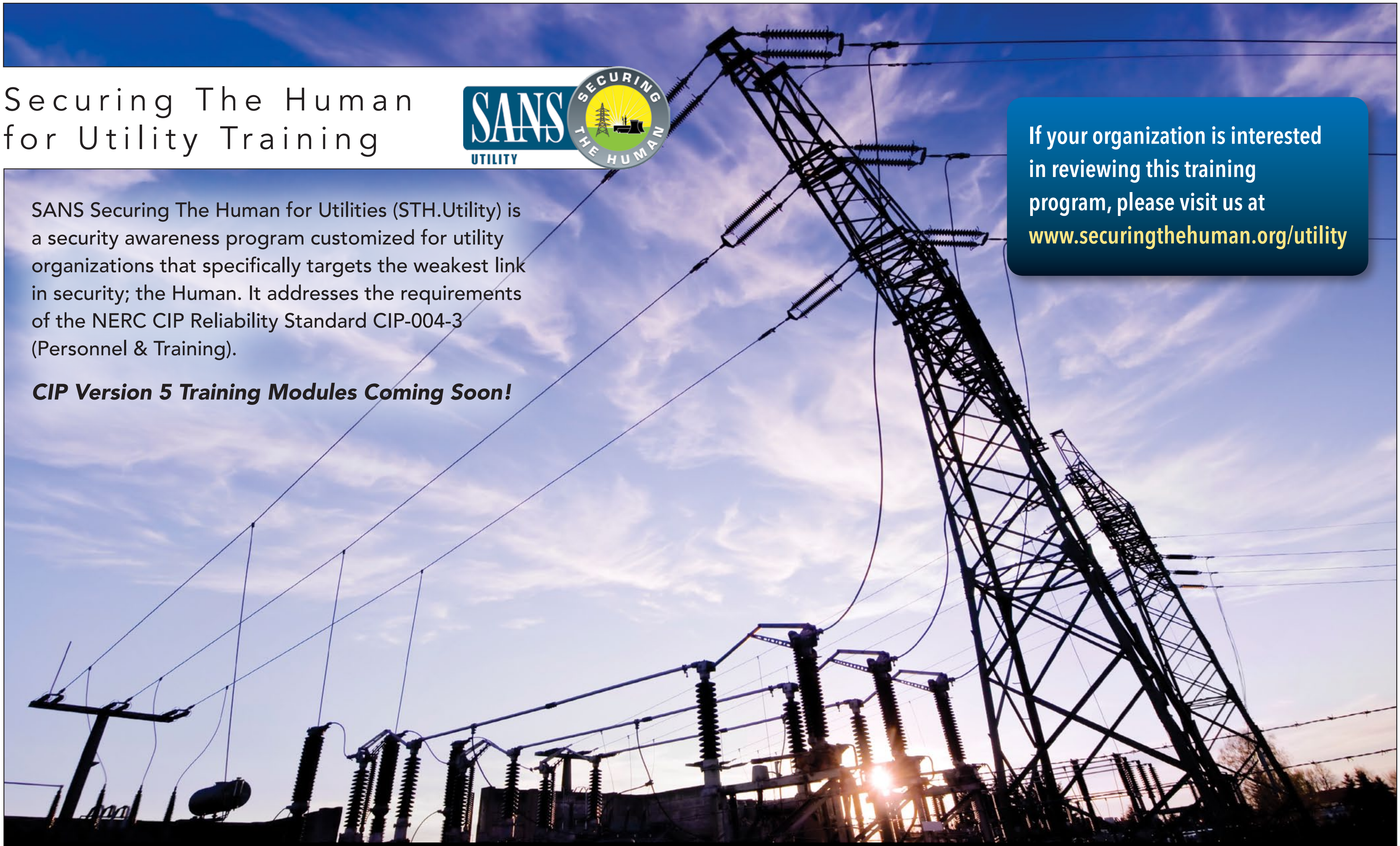
Equate Forms

GIAC employs an equating methodology to assure all candidates receive an exam form of equivalent difficulty.

Exam Goes Live!

GIAC exams are delivered in a proctored examination center. GIAC's partner for exam delivery is Pearson VUE, which has over 3,500 global examination centers for GIAC certification exams.

Securing The Human for Utility Training



SANS Securing The Human for Utilities (STH.Utility) is a security awareness program customized for utility organizations that specifically targets the weakest link in security; the Human. It addresses the requirements of the NERC CIP Reliability Standard CIP-004-3 (Personnel & Training).

CIP Version 5 Training Modules Coming Soon!

If your organization is interested in reviewing this training program, please visit us at www.securingthehuman.org/utility

Securing The Human for Utility Computer-Based Training (CBT) program contains 23 security modules that address the most common attack vectors by using a proven framework based on the 20 Critical Security Controls. This covers the quarterly training requirement for CIP-004-3 R1. In addition, seven CIP-specific compliance video modules address the requirements for CIP-004-3 R2.

Your organization can customize the training program by adding direct links to your own security policies following each module. Each module also includes an online quiz to test the user's comprehension of the CBT video content.

Keeping the training content updated and relevant is critical to the success of any security awareness program. STH.Utility addresses this by updating the training content once per year. These updates are delivered free of charge to all active CBT license holders.

Training is delivered through the SANS-hosted Virtual Learning Environment (VLE). Students can access their assigned training via any Internet-enabled browser. Student progress through the training program can be tracked via the VLE's administration web interface. Note that a utility organization may also choose to host the training on its own SCORM-compliant LMS.

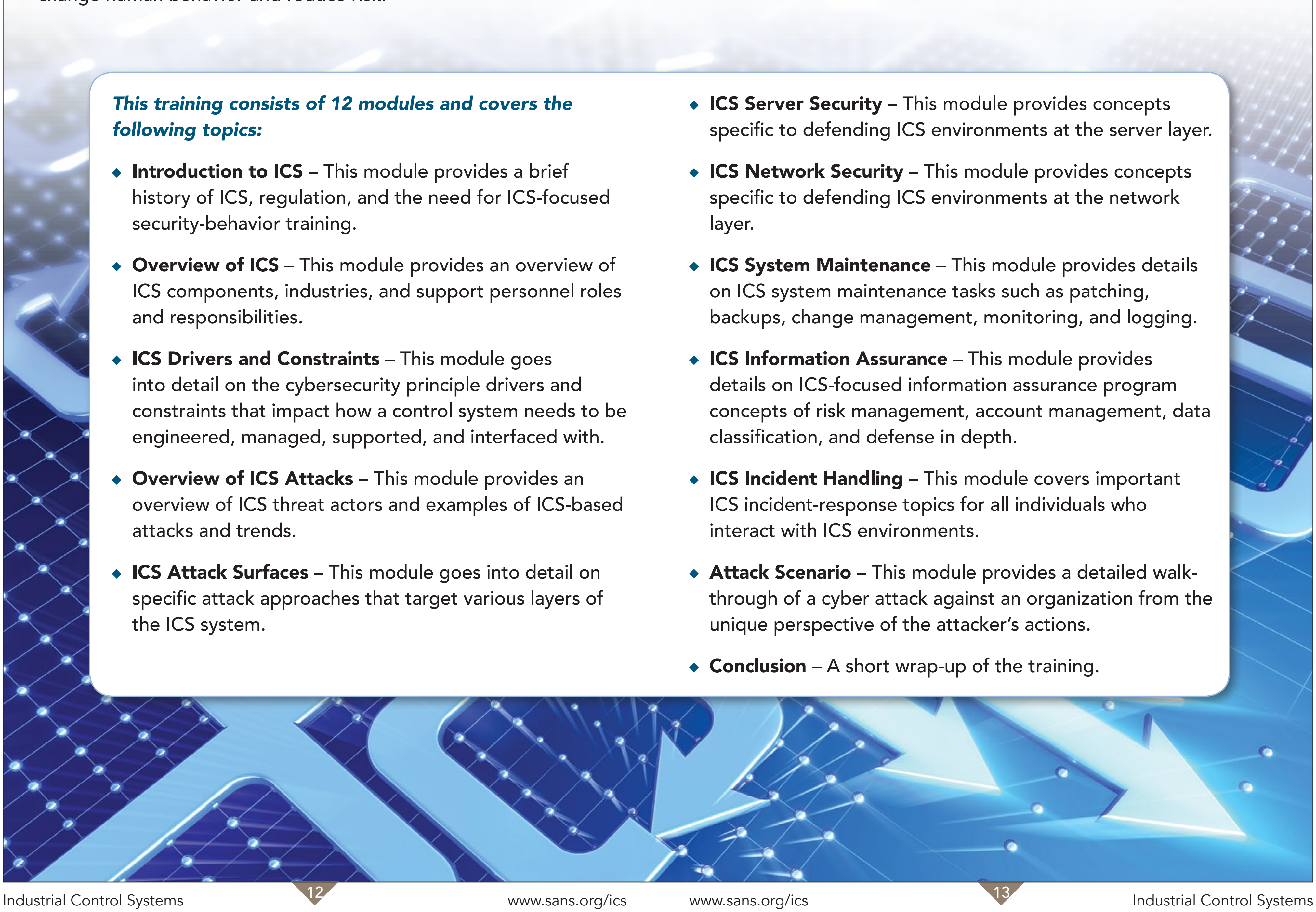
All of the CBT training is U.S. Federal 508/ADA compliant.

Optional purchase: Each of the R1 security awareness video modules also has an associated newsletter, poster, and screensaver to help reinforce the CBT training. The support materials package is customized with your organization's name, logo, and security team contact information. It is delivered in electronic format ready for printing or other distribution channels.

Securing The Human for Engineers

For additional information please visit,
www.securingthehuman.org/engineer

SANS Securing the Human for Engineers focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. This program was developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also to change human behavior and reduce risk.



This training consists of 12 modules and covers the following topics:

- **Introduction to ICS** – This module provides a brief history of ICS, regulation, and the need for ICS-focused security-behavior training.
- **Overview of ICS** – This module provides an overview of ICS components, industries, and support personnel roles and responsibilities.
- **ICS Drivers and Constraints** – This module goes into detail on the cybersecurity principle drivers and constraints that impact how a control system needs to be engineered, managed, supported, and interfaced with.
- **Overview of ICS Attacks** – This module provides an overview of ICS threat actors and examples of ICS-based attacks and trends.
- **ICS Attack Surfaces** – This module goes into detail on specific attack approaches that target various layers of the ICS system.
- **ICS Server Security** – This module provides concepts specific to defending ICS environments at the server layer.
- **ICS Network Security** – This module provides concepts specific to defending ICS environments at the network layer.
- **ICS System Maintenance** – This module provides details on ICS system maintenance tasks such as patching, backups, change management, monitoring, and logging.
- **ICS Information Assurance** – This module provides details on ICS-focused information assurance program concepts of risk management, account management, data classification, and defense in depth.
- **ICS Incident Handling** – This module covers important ICS incident-response topics for all individuals who interact with ICS environments.
- **Attack Scenario** – This module provides a detailed walk-through of a cyber attack against an organization from the unique perspective of the attacker's actions.
- **Conclusion** – A short wrap-up of the training.

ICS Resources

SANS Industrial Control Systems

SANS ICS Homepage

www.sans.org/ics

Twitter

@sansics

DHS Cybersecurity Evaluation Tool

http://ics-cert.us-cert.gov/Assessments

DHS ICS-CERT

http://ics-cert.us-cert.gov

NERC ES-ISAC

www.esisac.com/SitePages/Home.aspx

ICS-ISAC

http://ics-isac.org

Cybersecurity Vulnerability NSTB Program

http://energy.gov/oe/downloads/common-cyber-security-vulnerabilities-observed-control-system-assessments-inl-nstb

Vulnerability Analysis of Energy Delivery Control Systems

http://energy.gov/oe/downloads/vulnerability-analysis-energy-delivery-control-systems-2011

NIST SP 800-82 Guide to ICS Security

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

ISA-99 Control System Security Committee

http://isa99.isa.org/ISA99%20Wiki/Home.aspx

NERC CIP Standards

www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

ICS Resources

SANS Webcasts

Industrial Control System (ICS) Cybersecurity Response to Physical Breaches - A How-To Guide
www.sans.org/webcasts/industrial-control-system-ics-cybersecurity-response-physical-breaches-how-to-guide-97487

Improving Security Through IT/OT Collaboration
www.sans.org/webcasts/improving-security-it-ot-collaboration-97700

Building an ICS Security Program: Where to Begin
www.sans.org/webcasts/building-ics-security-program-96167

Results of the SANS SCADA Security Survey
www.sans.org/webcasts/results-scada-security-survey-95745

Traditional Attack Motives Must Be Tailored for the ICS World
www.sans.org/webcasts/traditional-attack-motives-tailored-ics-world-96707

Understanding Control System Cybersecurity
www.sans.org/webcasts/understanding-control-system-cyber-security-96630

SANS Industrial Control Systems Security Briefing
www.sans.org/webcasts/industrial-control-systems-security-briefing-live-houston-tx-96727

Why Every CSO Needs to Know Industrial Control Systems (ICS)
www.sans.org/webcasts/cso-industrial-control-systems-ics-96867

ICS Component Security Testing – Field Devices
www.sans.org/webcasts/ics-component-security-testing-field-devices-96560

Absence of the Normal, Presence of the Abnormal
www.sans.org/webcasts/absence-normal-presence-abnormal-97097

Prioritizing Security Resources
www.sans.org/webcasts/prioritizing-security-resources-96570

ICS/SCADA Honeypot Pros & Cons
www.sans.org/webcasts/ics-scada-honeypot-pros-cons-97477

More added monthy! For the latest, go to
www.sans.org/industrial-control-systems/resources

Author and Instructor Bios

Dr. Eric Cole

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers address the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Sight*, *Network Security Bible 2nd Edition*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting, where he provides leading-edge cybersecurity consulting services, expert witness work, and leads research and development initiatives to advance the state of the art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware.

Eric Cornelius

Eric Cornelius is currently a Technical Director at Cylance, Inc. and has recently served as the Chief Technical Analyst for DHS CSSP. As an active researcher in the field of cybersecurity since 2002, Mr. Cornelius supported many "boots-on-the-ground" engagements involving penetration testing, forensics, and malware analysis. Through these engagements, Mr. Cornelius aided multiple government, military, and private-sector organizations in protecting their networks and industrial control systems.

Mark Heard

Mark Heard is a native Tennessean and graduate of Auburn University with a degree in electrical engineering. He worked at Eastman Chemical Company in Kingsport, TN, as a control systems engineer for over 30 years. Mr. Heard has experience with a variety of Industrial Control Systems and applications and a continuing interest in computer and network technologies. He has been active in ACC Cybersecurity Program teams and ISA99 standard working groups since 2002. Mr. Heard has also represented the chemical sector on the DHS Process Control Systems Forum and Industrial Control Systems Joint Working Group. He helped write the "Roadmap to Secure Control Systems in the Chemical Sector" and chartered the Roadmap Implementation Working Group for that sector. Mr. Heard spent a year in the IT Security Group at Eastman before working at Red Tiger Security providing ICS cybersecurity assessment, consulting, and training.

Matthew Luallen

Matthew E. Luallen is a well-respected information professional, researcher, instructor, and author. Mr. Luallen serves as the president and co-founder of CYBATI, a strategic and practical educational and consulting company. CYBATI provides critical infrastructure and control system cybersecurity consulting, education, and awareness. Prior to incorporating CYBATI, Mr. Luallen served as a co-founder of Encari and provided strategic guidance for the Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office. In an effort to promote education and collaboration in information security, Mr. Luallen is an instructor and faculty member at several institutions. Mr. Luallen is adjunct faculty for DePaul University, teaching the Computer Information and Network Security master's degree capstone course. He is also a certified instructor and CCIE for Cisco Systems, covering security technologies, such as firewalls, intrusion prevention, virtual private networks, and general secure information architecture. As a certified instructor for the SANS Institute, Mr. Luallen teaches infrastructure architecture, wireless security, web application security, regulatory and standards compliance, and security essentials. Mr. Luallen is a graduate of National Technological University with a master's degree in computer science, and he also holds a bachelor of science degree in industrial engineering from the University of Illinois, Urbana.

Jonathan Pollet

Jonathan Pollet, Founder and Principal Consultant for Red Tiger Security, USA has over 12 years of experience in both Industrial Process Control Systems and Network Security. After graduating from the University of New Orleans with honors and receiving a B.S. degree in Electrical Engineering, he was hired by Chevron and designed and implemented PLC and SCADA systems for onshore and offshore facilities. In 2001 he began to publish several white papers that exposed the need for security for Industrial Control Systems (ICS), and is still active in the research of vulnerabilities within real-time ICS systems. Throughout his career, he has been involved with SANS, IEEE, ISA, ISSA, UTC, CSIA, and other professional organizations. Mr. Pollet has developed and presented workshops on SCADA Security to the FBI, Department of Homeland Security, and Utility Telecom Council, and has spoken at many conferences and workshops around the world.

Justin Searle

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Mr. Searle led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). He has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Mr. Searle is currently a certified instructor for the SANS Institute. In addition to electric power industry conferences, he frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Mr. Searle co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. He has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Daniel Michaud-Soucy

Mr. Michaud-Soucy has over five years of experience in the fields of Computer Engineering, Systems Engineering, and Computer Programming. Over the past few years, he has focused on conducting cybersecurity assessments specifically on SCADA and Industrial Control Systems. He has been the lead technical role in several field assessments, and is well versed in the proprietary SCADA and APT Assessment methodology used by Red Tiger Security for both on-site data collection and offsite data analysis.

ICS Team

Michael J. Assante

Michael Assante is currently the SANS lead for training on Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security. Mr. Assante was most recently Chief Executive Officer of NBISE and Chair of NBISE's National Board. He previously held the position of Vice President and Chief Security Officer at the North American Electric Reliability Corporation (NERC) and oversaw the implementation of cybersecurity standards across the North American electric power industry. Prior to joining NERC, Mr. Assante held notable positions at Idaho National Labs, was Vice President and Chief Security Officer for American Electric Power, and pioneered the security intelligence landscape in his role as Chief Operating Officer of LogiKeep. A former U.S. Navy intelligence officer with experience in information warfare and information security management, Mr. Assante recognized the need to bring intelligence-type analysis to the networks of the corporate world by identifying risks and threats specific to the hardware, software and systems used by individual organizations.

Tim Conway

Tim Conway is Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He formerly served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). He was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. He also served as an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. Mr. Conway is the former Chair of the RFC CIPC, current Chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, current Chair of the NERC CIPC GridEx Working Group, and Chair of the NBISE Smart Grid Cyber Security panel.

Derek Harp

Derek Harp is currently the business operations lead for the Industrial Control System (ICS) programs at SANS. Mr. Harp has served as a founder, CEO, or advisor of early-stage companies for the last 16 years with a focus on cybersecurity. Mr Harp is also a co-founder and a board member of NexDefense, Inc., a company focused on the security technology needs of ICS asset owners. Previously, he was the CEO and co-founder of LogiKeep, Inc., where he was the co-inventor of Intellishield™, a pioneer IT security product – which was subsequently acquired. Mr. Harp is a former U.S. Navy Officer with experience in combat information management, communications security, and intelligence.

SANS ICS
Industrial
Control
Systems

Upcoming ICS Events

Security Leadership Summit 2014
Boston, MA | May 2-6

ICS410 London 2014
London, England | May 12-16

ICS Security Training – Houston
Houston, TX | July 21-25

SANSFIRE 2014
Baltimore, MD | June 23-27

ICS Amsterdam 2014
Amsterdam, NL | September 21-27

SANS Network Security 2014
Las Vegas, NV | October 20-24

ICS Security training events will be added throughout the year. Please check www.sans.org/ics for a complete listing of locations and dates.