SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

# ICS Cybersecurity FIELD MANUAL

Vol. 1

*Author:*

**Dean Parsons**
**B.SC., GICSP, GRID, CISSP, GSLC, GCIA**

Certified SANS Instructor | Critical Infrastructure & ICS Cybersecurity Leader

# Contents

# What to expect from these ICS security field manuals

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of industrial control systems (ICS) and operational technology (OT).

The ICS Security Field Manual Series contains several sections and volumes, each focusing on a different aspect of industrial control systems and security defense for control environments. The manuals will cover what these systems are used for, how we rely on them, how they are attacked, and practical ways to defend and protect our critical infrastructure.

If you are new to the ICS/OT security area, this guide will get you up to speed quickly, providing long-lasting reference materials, free resources, and a training path for yourself and teams you may manage in engineering and ICS security. Future ICS security field manuals will expand on intermediate to advanced topics.

# Why it's critical to protect critical infrastructure

Many industrial control systems operate critical infrastructure that underpins our modern society. That infrastructure generates and distributes electricity to heat our homes and businesses, refines crude oil for fuel to run key manufacturing facilities and enable transportation, manufactures foods for global consumption, and treats our drinking water and wastewater.

Interacting with control systems is so commonplace we sometimes do not even realize we are doing it. Flipping on a light switch at home or the office, pumping gas into the car, adjusting the thermostat, or pouring water from a tap are all daily activities that rely on industrial control and critical infrastructure systems.

### ICS SECURITY PRO TIP

The National Institute of Standards and Technology defines ICS as systems "... used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes." See **csrc.nist.gov/glossary/term/industrial_control_system**

In short, this interconnected, interdependent, and complex mix of both legacy and modern computer systems is responsible for an array of critical processes in the physical world. Unfortunately, adversaries are all too aware of our reliance on these systems and have been increasingly targeting them, which can cause serious safety and environmental impacts. It is therefore imperative that these systems be protected by modern cybersecurity defenses that go beyond traditional information technology (IT) security.

More complex critical infrastructure examples include the generation, transmission, and distribution of electric power in a power grid system, critical manufacturing, oil and gas refineries and pipelines, and water and wastewater management systems, among many others.

The Cybersecurity & Infrastructure Security Agency (CISA) lists 16 sectors deemed as critical infrastructure, as shown in Figure 1.[1]

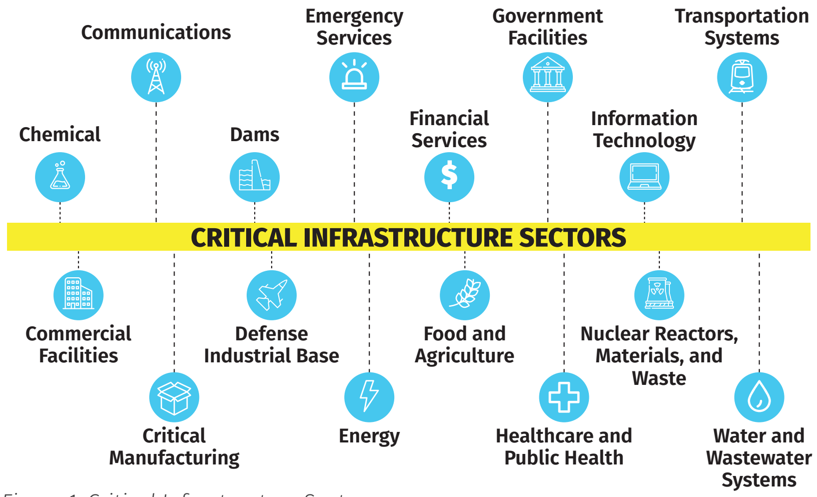
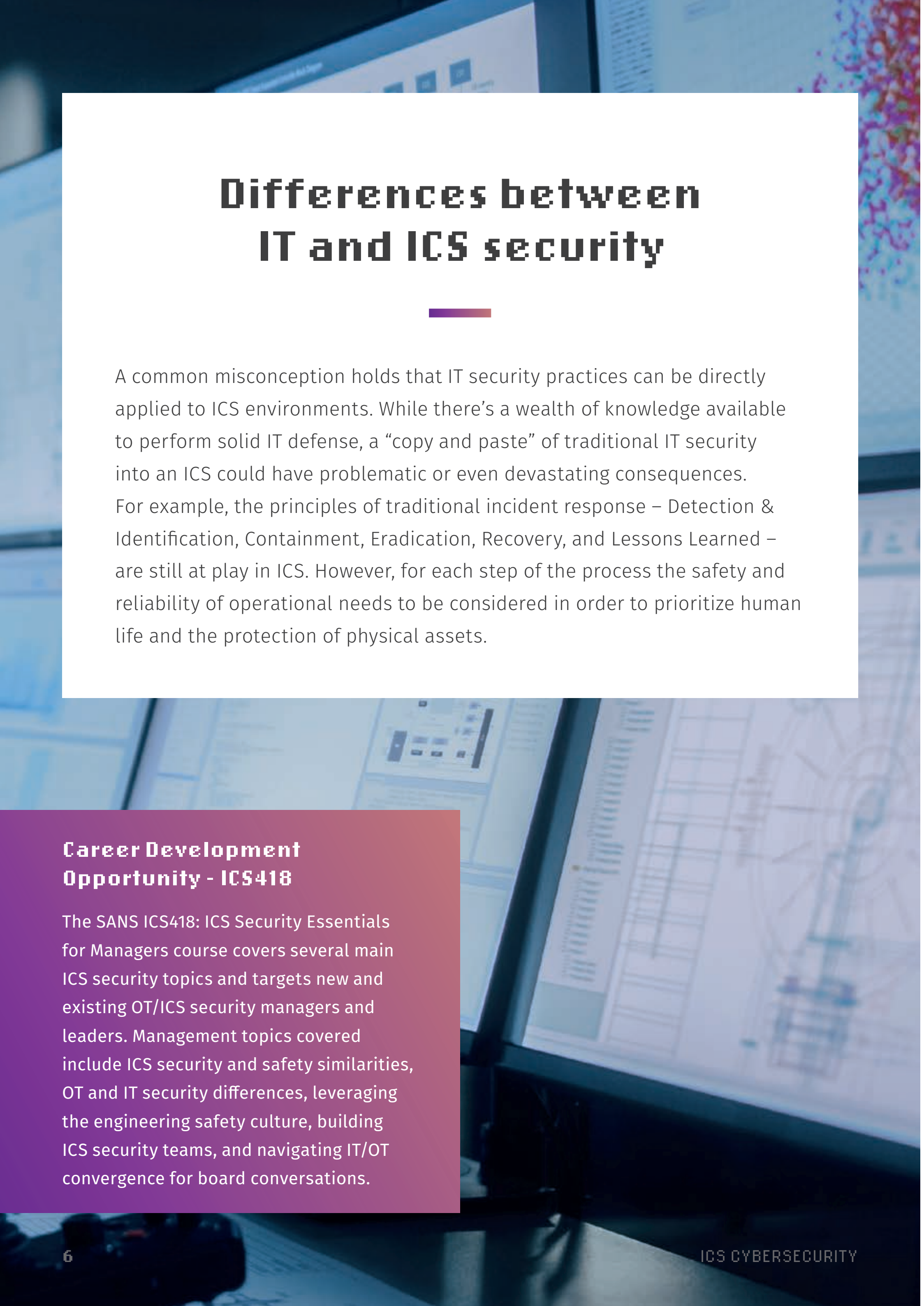


*Figure 1. Critical Infrastructure Sectors*

ICS systems must perform their tasks to read, write, and change the state of the physical world based on values (referred to as "setpoints") established by engineering teams to ensure a smooth process that functions within engineering and safety parameters.

Examples of "sensing" physical world states in an industrial environment are sensing the temperature in a combustion chamber in a petrochemical plant, the line voltage in a power grid (through digital protection control relays to monitor for trips and protect equipment), the pressure on a gas pipeline or at a pump station, water levels in water utility distribution tanks, and a flow rate of water to be treated in wastewater facilities (to ensure that it is less than the settling velocity of participles in primary clarifier systems). Sensing these related parameters or setpoints can indicate that a state should be changed, at which point operators using Human Machine Interfaces (HMIs) adjust the physical processes by using digital equipment and specialized engineering software.

[1] www.cisa.gov/critical-infrastructure-sectors



# Differences between IT and ICS security

A common misconception holds that IT security practices can be directly applied to ICS environments. While there's a wealth of knowledge available to perform solid IT defense, a "copy and paste" of traditional IT security into an ICS could have problematic or even devastating consequences. For example, the principles of traditional incident response – Detection & Identification, Containment, Eradication, Recovery, and Lessons Learned – are still at play in ICS. However, for each step of the process the safety and reliability of operational needs to be considered in order to prioritize human life and the protection of physical assets.

### Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course covers several main ICS security topics and targets new and existing OT/ICS security managers and leaders. Management topics covered include ICS security and safety similarities, OT and IT security differences, leveraging the engineering safety culture, building ICS security teams, and navigating IT/OT convergence for board conversations.

As stated by the U.S. Department of Homeland Security in a document entitled *Developing an Industrial Control Systems Cybersecurity Incident Response Capability*: "Standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents if prior thought and planning specific to operational ICS is not done."[2]

To put it in even starker terms, while cyber incidents in IT environments can lead to undesirable data impacts such as the unavailability of critical business applications, data corruption, and data loss, the impacts in ICS environments range from the loss of visibility or control of a physical process to the manipulation of the physical process by unauthorized users, which can ultimately lead to serious personnel safety risks, injury, or death.

While OT and industrial engineering control system assets are often compared to traditional IT assets, the latter in fact focus on data at rest or data in transit. In contrast, OT and industrial systems monitor and manage data that drives real-time system changes in the real world with physical inputs and controlled physical output actions. It is this primary difference between IT and OT/ICS that drives differing concerns related to security incident response, the environment and safety, cybersecurity controls, engineering support, system design, threat detection, and network architecture, among other critical issues.

### ICS SECURITY PRO TIP

The primary differences between IT and ICS/OT security drive different considerations for security incident response, safety, cybersecurity controls, engineering, support, system design, threat detection, and network architecture.

### Career Development Opportunity - ICS410

The GIAC GICSP certification associated with the SANS ICS410: ICS/SCADA Security Essentials course establishes technical knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

[2] www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

# Adapting IT security to protect ICS facilities

IT focuses on the world of digital data, while ICS and OT focus on the world of physical safety. Therefore, IT security must be adapted if it is to be used for ICS security. There's a wealth of knowledge available to perform IT defense, but for OT/ICS each defensive step needs to consider the safety and reliability of operations to prioritize human life and the protection of physical assets.

Let's define several common IT security defenses and review how they can be used or adapted to provide effective cyber defenses for ICS facilities, while supporting the safety and reliability of operations.

### Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course empowers new and established ICS security managers from all areas to understand the differences between IT/OT from a business, safety, and cyber risk management perspective.

## VULNERABILITY SCANNING

Automating regular vulnerability scans on critical business services in IT is good practice, whereas vulnerability scanning in ICS networks can have unpredictable and undesirable effects on safety. This is largely due to legacy systems that are unable to correctly process vulnerable scanning applications at a technical level.

Active vulnerability scanning in ICS is best performed by testing in development, and by using a phased approach that involves engineering and safety teams. Less invasive methods include reviewing passive network captures, asset inventories, configuration files, and firmware versions against threat intelligence and vulnerability advisories to achieve ICS vulnerability assessments.

## ENCRYPTION

Confidentiality of network traffic inside an ICS is less of a requirement than it is in traditional IT business networks because the two have largely different risk profiles regarding network traffic sniffing by unauthorized users. Encrypting internal ICS traffic can also cause unintended consequences when dealing with legacy devices, potentially low-bandwidth networks, and many remote sites. In addition, full-packet encryption will significantly devalue network security monitoring (NSM) and ICS active defense, leaving only 5-tuple or IPFIX packet information visible to ICS defenders. Availability for secure authentication methodologies for engineering devices for control commands is improving and more available in modern control networks.

### Career Development Opportunity - ICS410

The SANS ICS410: ICS/SCADA Security Essentials course, at a technical level, compares the differences between IT and OT/ICS across cybersecurity, safety, reliability, and support in order to bridge knowledge for IT, OT, and engineering. Students will complete numerous in-class technical labs ranging from programming a fundamental programable logic controller to conducting human machine interface and investigating attack vectors in OT/ICS.

## PATCHING IN INDUSTRIAL ENVIRONMENTS

Patching operating systems and software is an effective security practice that has been commonplace in business networks for decades. There are special circumstances for ICS, where patching may not be feasible or possible within a normally accepted timeframe without impacting safety or increasing the risk to industrial processes. This could be the case with legacy equipment or critical infrastructure systems. However, patching has become more acceptable in ICS environments in recent years given the threat landscape, the availability of patches, patch testing by ICS vendors, and the availability of standards such as the North American Electric Reliability Corporation (NERC) standards for the electricity utility sector. In cases where electricity utilities are following NERC Critical Infrastructure Protection (CIP) standards, patching is clear. Patching is not just nice to have – it is requirement with strict criteria for identifying, reviewing, and applying patches. In extreme cases when patching is not possible within NERC-CIP specified standards, an electricity utility adhering to NERC-CIP could declare an exceptional circumstance under which the case would have to be justified and formally documented. Compensating controls then could be used to reduce risk in some cases.

Many ICS vendors go to great lengths to verify their software on common operating systems not long after patch notifications are released. This process continues to improve across multiple sectors. Thus, patching is becoming more of a positive and achievable part of active ICS defense and preventative maintenance from which facilities can benefit. Remember, when evaluating patch advisories and vulnerability reports, and to drive risk-based mitigation plans, it is best to follow a strategy of threat = capability of the adversary + intent of the adversary + opportunity for the adversary to have an impact. Patch vulnerabilities that are applicable to your environment are best applied using a phased, controlled, and safe approach. When patching is not feasible within a normally accepted timeframe, it is common to add additional monitoring or compensating controls.

### Career Development Opportunity - ICS410

SANS ICS410: ICS/SCADA Security Essentials walks students through the Purdue levels. Then, using the ICS Network Reference Architecture model the course builds security enforcement boundaries to illustrate traffic flows and security controls for modern ICS network defenses in depth. See **www.sans.org/posters/control-systems-are-a-target/**

## ENDPOINT SECURITY FOR CONTROL SYSTEM ASSETS

IT antivirus solutions have signature and behavioral/heuristics-based engines for threat detection that commonly require frequent Internet-based updates. Internet egress and ingress filtering for industrial environments offer more protections but may not feasibly allow frequent Internet connectivity. A false positive in IT can disrupt business flow. A false positive in ICS could stop critical systems, which in turn could cause an unsafe physical situation for workers or environmental concerns.

Where industrial control systems are more static than traditional IT environments, using application whitelisting endpoint protection solutions and allowing only pre-approved applications to execute drastically reduce the potential for malware to run, reduce false positives, support safety, and remove the need for frequent Internet-based updates.

Antivirus on endpoint devices generally does not currently include the protection and installation on engineering assets such as controllers. Rather, endpoint protections are commonly limited to protect OT assets running traditional operating systems with engineering software installed.

## FIREWALLS AND NETWORK SEGMENTATION

The proper use of firewalls is critical in ICS for the same reasons as in IT. Firewalls can be used for containment in incident response and as chokepoints for NSM data collection, segmenting network zones and securely controlling traffic via access control lists. ICS firewalls should not allow any direct connections to or from the Internet.

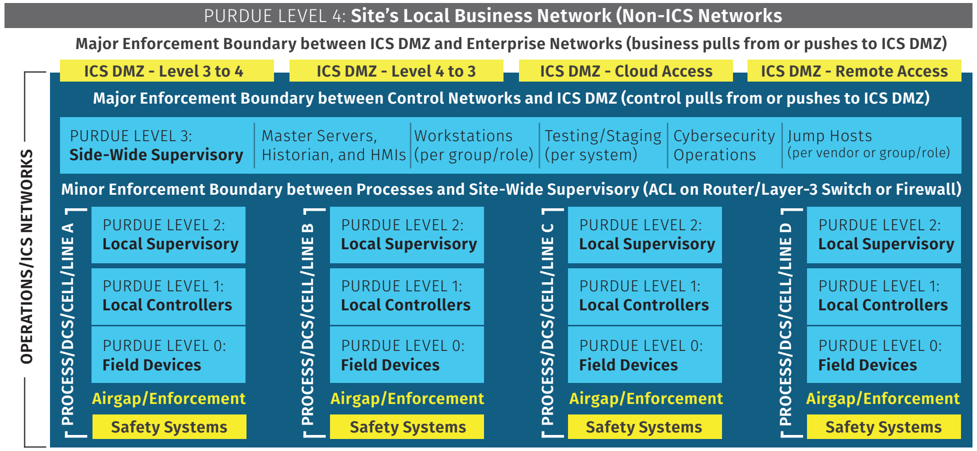

PURDUE LEVEL 4: Site's Local Business Network (Non-ICS Networks
Major Enforcement Boundary between ICS DMZ and Enterprise Networks (business pulls from or pushes to ICS DMZ)
ICS DMZ - Level 3 to 4
ICS DMZ - Level 4 to 3
ICS DMZ - Cloud Access
ICS DMZ - Remote Access
Major Enforcement Boundary between Control Networks and ICS DMZ (control pulls from or pushes to ICS DMZ)
PURDUE LEVEL 3: Side-Wide Supervisory
Master Servers, Historian, and HMIs
Workstations (per group/role)
Testing/Staging (per system)
Cybersecurity Operations
Jump Hosts (per vendor or group/role)
Minor Enforcement Boundary between Processes and Site-Wide Supervisory (ACL on Router/Layer-3 Switch or Firewall)
OPERATIONS/ICS NETWORKS
PROCESS/DCS/CELL/LINE A
PROCESS/DCS/CELL/LINE B
PROCESS/DCS/CELL/LINE C
PROCESS/DCS/CELL/LINE D
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

*Figure 2. ICS410 SCADA Reference Model Illustrating Security Boundaries and Assets in Purdue Levels*

If remote access is needed for maintenance or support, it should be implemented securely and carefully and in multiple layers, such as multi-factor authentication, extremely strict access control, and additional monitoring/ alerting.

An ICS network should generally not accept inbound connectivity. Control networks benefit from deploying network intrusion detection systems that do not drop traffic, rather than running the risk of dropping industrial process or safety commands from false positives, which are more common with intrusion prevention systems.

### ICS NETWORK SECURITY

You may not realize it, or have system visibility to see it, but your organization's ICS environments are a target for cyber attackers. ICS automation, process control, access control devices, system accounts, and asset information all have tremendous value to attackers.

### ICS SECURITY PRO TIP

It is common and advisable for control system designers to segment different control networks from each other. This can be done by using enforcement boundaries to separate the Internet and corporate business networks from control system networks, and by segmenting the control network into levels aligning with a model such as the Purdue network architecture model.

### NETWORK INTRUSION DETECTION AND PREVENTION

All network inspection devices deployed to make decisions on ICS traffic should be able to interpret ICS protocols and commands. As with antivirus solutions on endpoints, false positives and the potential disruption of control system operations can occur in network inspection as well. Thus, an intrusion detection system to provide alerts on suspect network traffic on a control network is more suitable than an  intrusion prevention system that blocks network traffic. Detection over prevention allows for alerting and logging as well as the ability to actively drive an investigation without security introducing risk to operations. Intrusion detection systems in any environment will require dedicated resources to frequently fine-tune and test their rules based on changes and sector threat intelligence in order to enable proactive ICS defense and threat hunting. The volume of network traffic in industrial control networks is significantly less than in IT environments, making the detection of malicious activity more manageable.

### COMPARING SECURITY CONTROLS AND ACTIONS

The table below defines just a few common IT security controls and reviews how they can be used or adapted to provide effective cyber defenses for ICS facilities while supporting the safety and reliability of operations.

| Security Control | IT Action | ICS Action |
|---|---|---|
| **Endpoint Protection** | Signatures, heuristics-based detections – quarantine | Heuristics alerting; allowlisting – alerting, blocking unlearned applications |
| **Firewalls** | Segment – users, servers | Segment from enterprise/IT and Internet, align with Purdue levels 0-5 |
| **Network Intrusion Detection System/ Intrusion Protection System** | Intrusion prevention system | Intrusion detection system, behavioral-anomaly detection – alerting |
| **Vulnerability Scanning** | Regular interval, automated | Tested in development, passive where possible, run during scheduled maintenance windows |
| **Patching** | Monthly, streamlined process | Less frequent, legacy devices, less patch windows |
| **Security Awareness** | Phishing, web, and data protections | IT security awareness + physical safety, transient devices, architecture, engineering |
| **Event Detection** | Windows event logs, traditional endpoint protection, URL inspection, etc. | RTU/PLC changes, ICS protocol abuse, Purdue boundary access detection, remote access by vendors |
| **Incident on Asset** | Wipe, patch, deploy | Fight through attack: maintain safety, contain, completely eradicate during next engineering maintenance window |

# Safety is #1 in industrial control systems

Unlike IT incidents, ICS incidents can involve the potential loss or damage of physical property or engineering assets, as well as safety risks to people and the environment. Thus, industrial incident response is a joint effort with security incident responders, engineers, operators, network architects, and physical safety teams at facilities.

### ICS SECURITY PRO TIPS

- Cyber-kinetic attacks on control systems or control system components can manifest as direct or indirect physical damage to engineering assets, in turn introducing environmental impacts and possibly causing human injury or death.

- The *security* mission in IT is to secure data at rest and in transit to support Confidentiality, Integrity, and Availability (CIA). The safety mission in ICS is to enable and secure physics in engineering processes that could, if compromised, render physical conditions unsafe for the environment and people. The mission in ICS is safety, engineering system and command integrity, and cyber-physical operational availability. In control systems, ICS cybersecurity supports the safety and reliability of operations.

On-site physical safety is always going to be top of mind, even above cybersecurity. In fact, cybersecurity supports safety. While on-site in a facility, it is critical to follow the lead of the safety team and the physical safety protocols to ensure you and your team remain physically safe. This is usually the first of the organization's core values. It means wearing personal protective equipment (PPE), and many sites also require all visitors to have completed safety training and show certificates of completion before entering.

Many ICS security programs leverage the physical engineering safety culture in an organization by drawing parallels between physical safety and cyber safety. Through presentations about security awareness, as an example, the programs share industry case studies to illustrate how cyber-attacks can severely impact operations, and how cybersecurity protects the safety and reliability of engineering operations. It is not uncommon for industrial cybersecurity programs to reword cyber "security" as cyber "safety" in security awareness memos.

# Legacy, modernization, and industrial security

Industrial control systems were not always as connected or as highly automated and complex as they are today. The systems were designed, built, tested, and deployed for a particular purpose, enabling the control system to operate in isolation, and ran on proprietary protocols. This was all done in an isolated network away from other networks, including the outside world of IT business networks and the Internet.

Over the years, advancements in modern network technology and equipment control systems have resulted in a shift from an isolated control environment for ICS to a more connected environment. This has brought about several business benefits such as cost savings, improved efficiency, better safety management, and an improved view and control over engineering processes. However, more external connections also ultimately broke the isolated or "air-gapped" model of the past, rendering industrial control systems less isolated and more exposed to additional cyber risk.

More external connections were enabled for ICS to take advantage of their benefits, including reducing travel costs by allowing external support personnel to access the environment(s) for remote monitoring and control of industrial processes. Today most control systems use modern TCP/IP network stacks, modern network technologies, and a blend of traditional technology and industrial protocols. However, many legacy systems still exist as part of critical subsystems within control systems. In short, with automation and its benefits also comes increased risks.

# ICS cyber threat pool and landscape

With modernization of their systems and increased connectivity to the Internet and business networks, industrial control systems have inherited IT-related security vulnerabilities in addition to inherent control system vulnerabilities, widening the cyber threat pool.

In general, the threat landscape for ICS is continually increasing. Cyber attackers have skills that go beyond traditional IT intrusions and data exfiltration techniques. They have set their sights on OT and control systems, demonstrating an understanding of industrial control systems and an alarming ability to develop ICS-capable attack tools to gain access and cause negative effects.

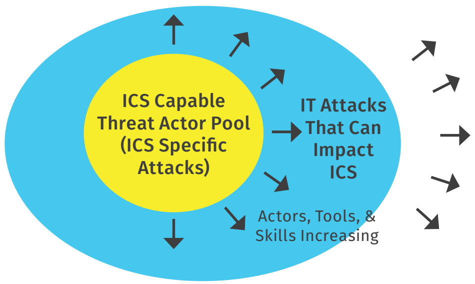

ICS Capable Threat Actor Pool (ICS Specific Attacks)
IT Attacks That Can Impact ICS
Actors, Tools, & Skills Increasing

*Figure 3. The Threat Pool: The Sunny Side Up Egg of Doom*

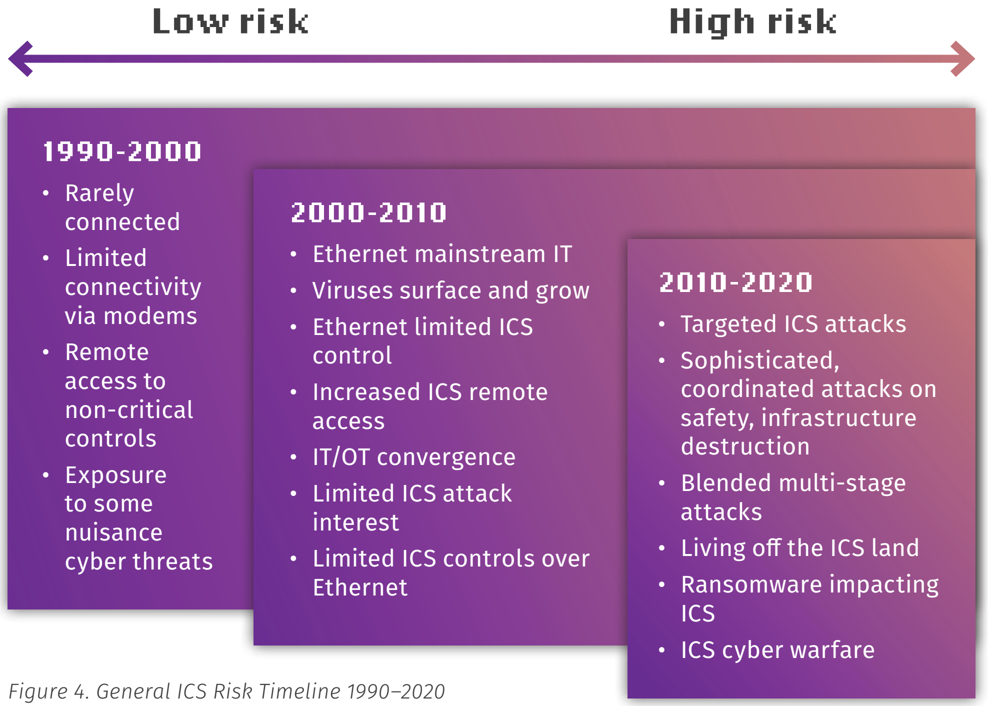
The various threat groups and adversaries and their capabilities to impact an organization are considered a threat pool. The yellow area in Figure 3 represents the number of ICS threat adversary groups capable of conducting ICS-specific attacks with large likely impacts. The blue area represents the number of IT attacks that can impact control systems. As threat groups continue to improve in skill, sophistication, and the targeting of attacks, we will see both the yellow and blue areas grow – in other words, there will be a continuous increase in ICS-specific attacks and in IT attacks that can impact ICS. And as ICS facilities become more interconnected and reliant on IT, we can expect to see more tools and research designed to impact ICS operations through IT attacks.

# ICS attack history at a glance

There is a general increasing trend in the intent and capabilities of threat actors to cause an impact in ICS environments. Cyber-kinetic attacks on control systems or their components can manifest as direct or indirect physical damage to engineering assets, in turn introducing environmental impacts and causing human injury or death.

### Career Development Opportunity - ICS418

The SANS ICS418: ICS Security Essentials for Managers course includes an ICS attack history walk-through for new and existing ICS/OT security managers with a major focus on lessons learned for improved ICS risk management.


Low risk

High risk

1990-2000

- Rarely connected
- Limited connectivity via modems
- Remote access to non-critical controls
- Exposure to some nuisance cyber threats

2000-2010

- Ethernet mainstream IT
- Viruses surface and grow
- Ethernet limited ICS control
- Increased ICS remote access
- IT/OT convergence
- Limited ICS attack interest
- Limited ICS controls over Ethernet

2010-2020

- Targeted ICS attacks
- Sophisticated, coordinated attacks on safety, infrastructure destruction
- Blended multi-stage attacks
- Living off the ICS land
- Ransomware impacting ICS
- ICS cyber warfare

*Figure 4. General ICS Risk Timeline 1990–2020*

## ICS attack history at a glance

Since 2010, there have been a number of high-profile, targeted attacks on industrial control systems ranging from espionage to physical destruction of engineering assets, as shown in Figure 5.

*Figure 5. Notable Attacks on Industrial Control Systems since 2010*

**Stuxnet (2010) - Destructive Malware**
Specific target - Iran Natanz uranium enrichment facility, physical destruction, 0-days, PLC rootkit

**Havex (2014) - Espionage Malware**
Living off the land, espionage only, abused OPC (deployed in many ICS sectors)

**BlackEnergy (2015) - Espionage Malware, Human Adversary - Interaction with Control System**
Used for access to Ukraine, adversary used Human Machine Interface to shut down power

**CRASHOVERRIDE (2016) aka Industroyer- Disruptive Malware**
Abused native industrial ICS (IEC-104) protocol, scalable ICS-specific framework (more than malware)

**TRISIS aka Triton aka Hatman (2017) - Disruptive Malware - Attack on People and Safety Control Systems**
Targeted Safety Instrumented System (SIS)

**EKANS (2020) - Disruptive Malware - Ransomware Targeting ICS Processes**
Ransomware and additional functionality to forcibly stop several running programs, including multiple processes related to industrial operations.

### ICS SECURITY PRO TIPS

- Conduct a simple ICS Attack Tree exercise to identify potential attack vectors. This can also help with ICS incident response exercises and pave the way for advanced ICS threat hunting for more mature environments.

- MITRE ATT&CK for ICS is a practical framework to describe the actions an adversary may take while operating inside a control network. It illustrates previously observed ICS attacks and shares knowledge on related attack tactics and techniques, potential mitigations, impacts, the malicious software used, etc. MITRE ATT&CK can be found at **https://collaborate.mitre.org/attackics/index.php/Main_Page**

# Control system engineering assets

## SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

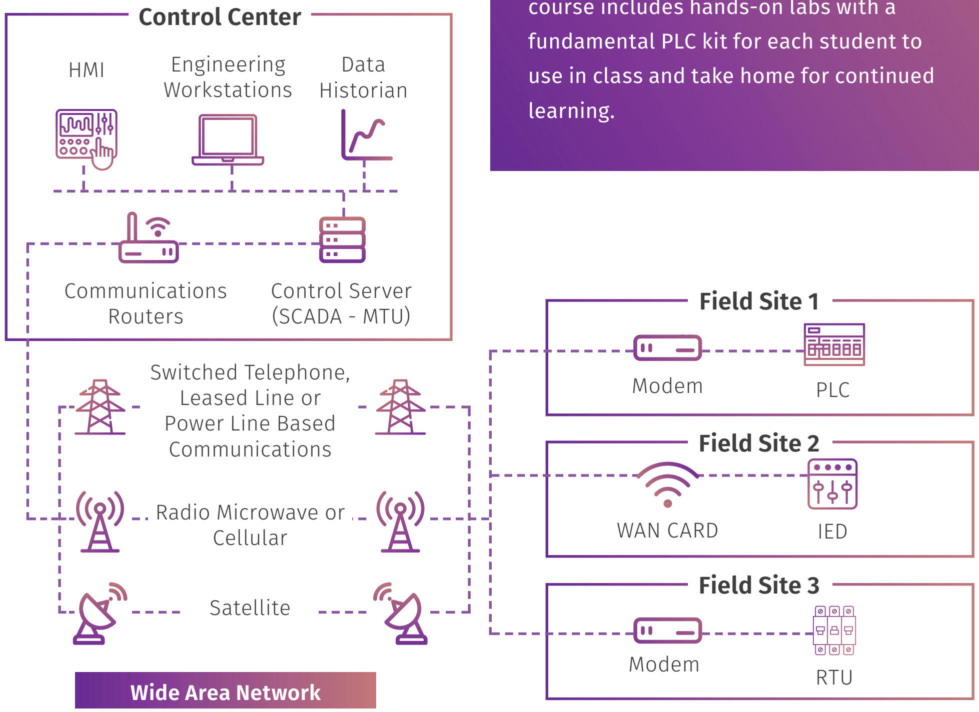
SCADA is a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Its common uses include power transmission and distribution and pipeline systems in industrial environments.

### Career Development Opportunity - ICS410

- ICS410: ICS/SCADA Security Essentials is an introduction to ICS security and SCADA environments. It reviews critical ICS/OT engineering assets, network architecture, and enginering processes, as well as how engineering assets fit and work together, among other critical topics.

- The SANS ICS410: ICS/SCADA Security course includes hands-on labs with a fundamental PLC kit for each student to use in class and take home for continued learning.

*Figure 6. General SCADA System Layout*



## PROGRAMMABLE LOGIC CONTROLLERS (PLCs)

PLCs are solid-state devices that hold and run programmed logic instructions for a control process. They are physically wired to various instrumented devices such as sensors and actuators, including sensors that perceive physical states such as temperature, vibration, fluid levels, pressure, humidity, etc., and actuators such as solenoids, burners, compressors, pumps valves, breakers, etc. For example, the PLC and its input/output modules could sense and communicate to a Remote Terminal Unit (RTU) to physically open or close breakers in a power system, energizing or de-energizing power to a region or city. Controllers are said to “run the plant floor” in control system facilities.

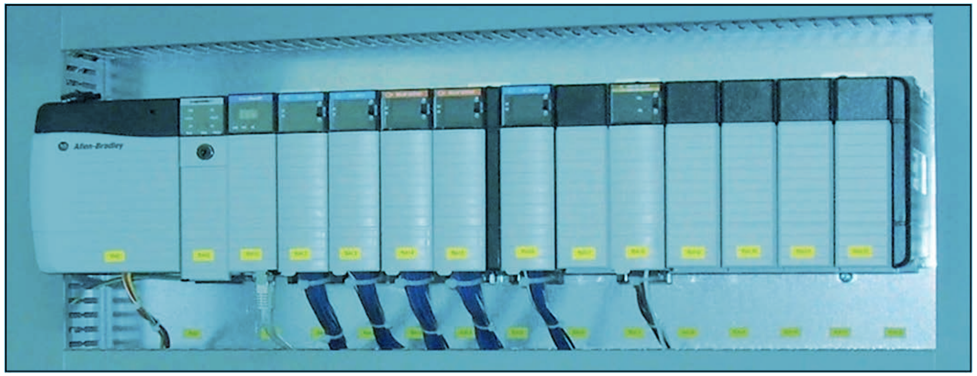


*Figure 7. Chassis with PLC, and input/output Modules*

### ICS SECURITY PRO TIP

Many ICS components can be placed into logic levels or groupings that align with the Purdue Reference Model, but can be further extended with the Network Reference Architecture from the ICS410: ICS/SCADA Security Essentials course to focus even more on security and secure enforcement boundaries.

## SENSORS

Sensor devices physically measure a quantity or physical state of something, then convert the measurements into an electrical or optical signal that other engineering devices can interpret and apply logic to in order to help change the state in a control system environment that ultimately affects and changes the physical world.  For example, sensors detect physical changes such as temperature, humidity, vibration, sound, pressure, etc.

## ACTUATORS

Actuators are mechanical devices and components attached at the end of the industrial process that move and change elements in the physical world. They include but are not limited to valves, solenoids, pumps, agitators, burners, switches, relays, and compressors.

### Career Development Opportunity - ICS410

The SANS ICS410: ICS/SCADA Security Essentials course teaches about ICS attack vectors, the attack tree methodology, and the exploitation of fundamental ICS system vulnerabilities, while identifying critical ICS/OT assets.

## DATA HISTORIAN

Data historian is the database system for control system process information, trending data about the process, and other critical information. For example, a data historian in an electricity generation facility will likely store electricity demand from industry and residential customers, but also the rate at which power is being generated, thus revealing data about how to improve the process. As another example, a pharmaceutical process might store information in the data historian about the amount of different substances needed to create a vaccine, and the rate at which a batch is being produced. A data historian is an asset that may have trusted connections to both IT and ICS. An adversary could abuse this trusted asset to pivot from a compromised asset in IT to the control network. In addition, data stored in this database could be highly sensitive and sought after by adversaries to learn about the industrial process and/or to steal intellectual property from the database.

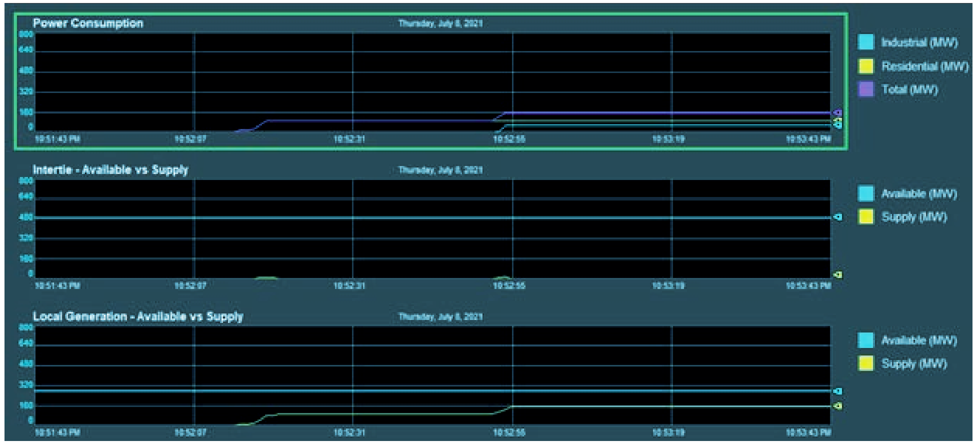
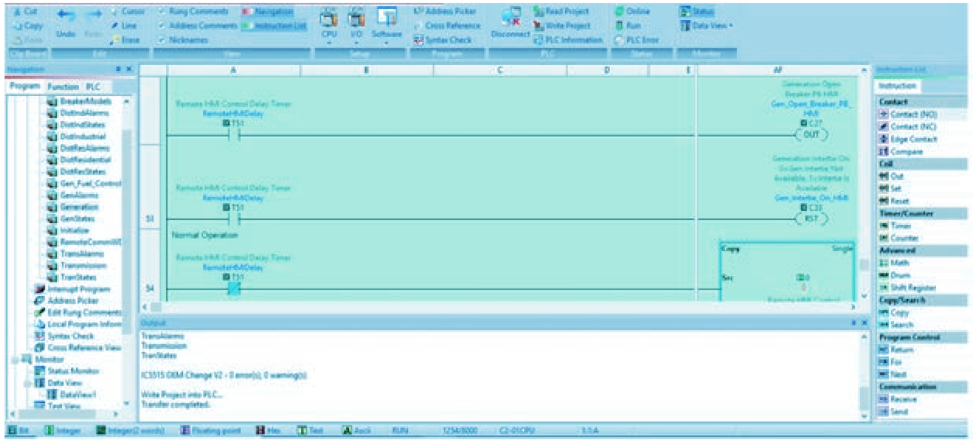


*Figure 8. A Typical Data Historian Tracking and Storing Process Trending Data on a City's Power Grid System*

## ENGINEERING WORKSTATION

An engineering workstation is usually a laptop or power desktop workstation that is used with engineering software to view, manage, and program network devices, PLCs, RTUs, and other field devices at the lower levels of an entire facility operation. The codes to "run the plant floor" are commonly stored on this device, which usually has full access to change plant floor programming. From here an adversary can reprogram and update controllers in operation.



```
TransAlarms
Transmission
TranStates

IC5515 OEM Change V2 - 0 error(s), 0 warning(s)

Write Project into PLC...
Transfer completed.
```

*Figure 9. Typical Engineering Workstation Engineering Software Used to Program and Change PLCs*

### HUMAN MACHINE INTERFACE

A Human Machine Interface (HMI) is a graphical interface used to interact with, change, and control the physical process at a local or remote facility. Operators use the HMI to view and acknowledge system alarms and safety conditions and to monitor whether production is operating as expected. HMIs can run on traditional operating systems on OT assets, or on embedded devices closer to the process in a facility, such as on touch-screen panels. From an HMI an adversary can directly interact with the process and manipulate it.

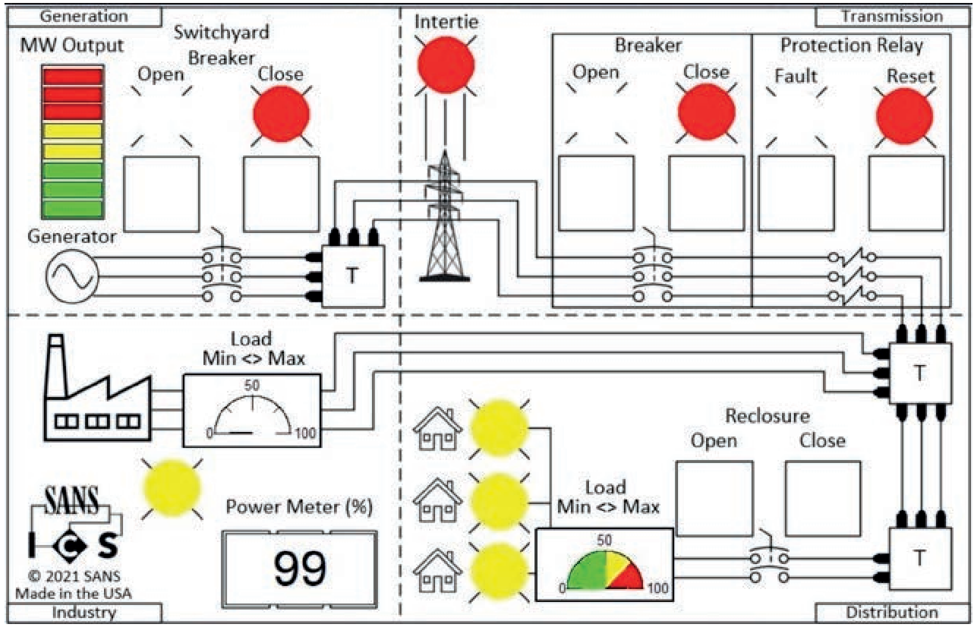


*Figure 10. Typical Human Machine Interface Used by Engineering Operators to View, Change, and Control Industrial Processes*

# Control system network levels

Many ICS components can be categorized into the following zones of systems based on levels from the Purdue Reference Architecture.[3]

**Level 5** - Internet, Cloud Services

**Level 4** - Enterprise IT Systems

**Level 3** - ICS Plant Site SCADA Controls

**Level 2** - HMI, Engineering Workstation

**Level 1** - Process Control, Field Devices

**Level 0** - Sensors, Hardware Actuators

### Career Development Opportunity - ICS410

The SANS ICS410: ICS/SCADA Security Essentials course walks students through technical labs that critique and improve ICS network architecture and system designs.

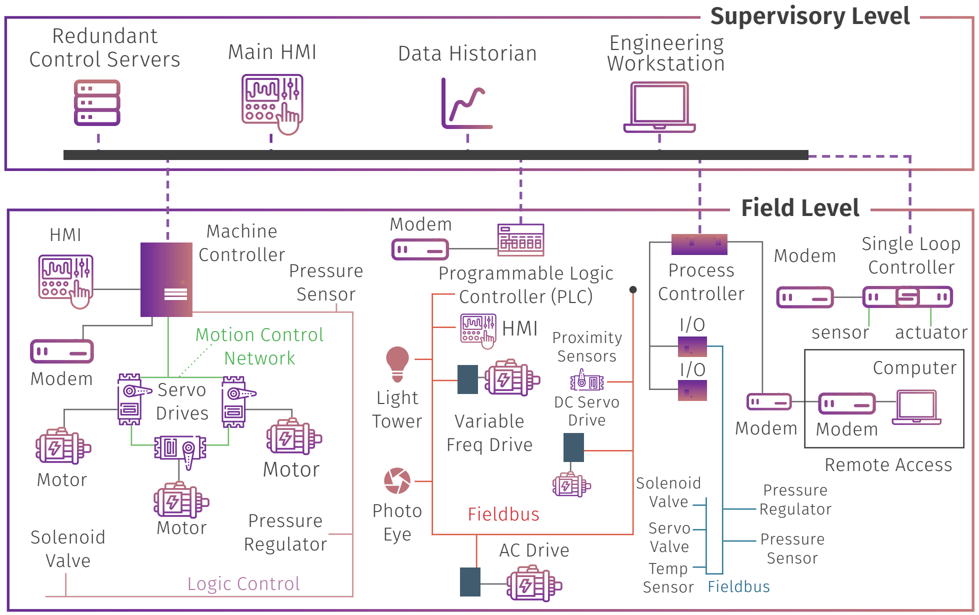


*Figure 11. Levels of an ICS Network with Key Components*[4]

[3] en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

[4] nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

# Epilogue to volume 1

This volume has shown us that there are different approaches to IT and ICS security, and that's ok! While some parts of traditional IT security can help guide the community, a direct "copy-paste" of them is not recommended for ICS. Elements of IT security for OT/ICS should be adopted for ICS security where it makes sense, all the while making adjustments as needed and always prioritizing human life, the reliability of operations, and the protection of physical assets.

Given the volume and sophistication of threats to ICS, the IT/OT convergence movement works well for end-to-end security event correlation from IT through to ICS. The convergence of these IT and OT groups should be embraced as part of efforts to achieve an active defense strategy with network security monitoring and active threat hunting. Physical site inspection and face-to- face cyber discussions literally on the plant floor are also very effective at getting everyone involved in recognizing that cyber safety supports the security and reliability of operations.

As we saw in Figure 5, in recent years the world has witnessed a number of specific targeted ICS attacks, including Stuxnet, Havex, Blackenergy and power outages, and TRISIS/TRITON, the world's first publicly disclosed attack on safety instrumented systems. Attacks against critical infrastructure increasingly impact our daily lives. Through all of the targeted ICS attacks, we must not lose sight that IT-related malware such as Ransomware and Cryptomining, while not designed to physically damage an ICS, have also caused disruptions and downtime if running in an ICS.

# The ICS community forum

You are invited to participate in the SANS ICS Community Forum, where ICS professionals discuss current security events, share tips, ask questions, and connect with others passionate about securing our critical infrastructure. Don't miss an important community event, a great job opportunity, or the latest free resources authored by the SANS ICS practitioner faculty.

**https://ics-community.sans.org/**

News and updates
**ics.sans.org**

Join the SANS ICS Community Forum
**ics-community.sans.org/signup**

Free and open-source tools for ICS
**ControlThings.io**

Join the conversation
**@SANSICS**

Thought leadership
**SANS ICS**

Insights and demos
**SANS ICS Security**

## FREE ICS RESOURCES: CHEAT SHEETS, POSTERS, AND MORE!

**Introduction to ICS Security**

- Defining what industrial control systems are, why they are vital, and the unique challenges of securing them.

**The ICS Site Visit Plan**

- Maximize your efforts to identify critical assets during on-site ICS visits.

**ICS418: ICS Security Essentials for Managers: Step Up, Step Over, In Place**

- This blog describes the newest offering from SANS targeted specifically to managers involved in keeping industrial control systems safe.

**Protect Control Systems and Critical Infrastructure with GRID**

- GIAC Response and Industrial Defense (GRID) is a must-have certification for ICS/SCADA/OT professionals.

**Guidance on defining the differences** between cybersecurity defense methodologies, security controls, safety, impacts, skill sets, and the security missions for ICS/OT (operational technology) compared to traditional information technology (IT) security.

- The Differences between ICS/OT and IT security

**Additional free resources** for the ICS/OT community, including webcasts, blogs, white papers, and more, can be found at:

- https://www.sans.org/industrial-control-systems-security/

# SANS ICS Curriculum

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of industrial control systems  and operational technology. The initiative is equipping security professionals and control system engineers with the security awareness, work-specific knowledge, practitioner resources, and hands-on technical skills they need to secure automation and control system networks and critical infrastructure.

**ICS410: ICS/SCADA Security Essentials**

Provides an understanding of industrial control system components, purposes, deployments, significant drivers, and constraints. Includes hands-on lab learning experiences to control system attack surfaces, methods, and tools.

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

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

Helps deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/

### Career Development Opportunity - ICS GIAC Certifications

- ICS attackers are honing their skills and plotting their attacks. We can up our defensive skills to counter them and protect critical infrastructure that supports our modern way of life.

- ICS GIAC certified professionals have demonstrated they have the skills to help protect critical infrastructure from a technical and/ or strategic level.

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

Empowers students with knowledge of the "what" and the "how" of the NERC CIP standards. The course provides multiple approaches to identify and categorize BES Cyber Systems and helps determine the requirements applicable to specific implementations. It also covers implementation strategies with a balanced practitioner approach to cybersecurity benefits, as well as regulatory compliance.

https://www.sans.org/cyber-security-courses/essentials-for-nerc-critical-infrastructure-protection/

**ICS612: ICS Cybersecurity In-depth**

Provides advanced coverage of security concepts primarily driven by applied learning with hands-on labs. The in-classroom environment simulates a real-world factory and the labs move students through a variety of exercises that demonstrate how an attacker can compromise an ICS environment and how defenders can better secure and manage that environment.

https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth/

**ICS418: ICS Security Essentials for Managers**

Fills the identified gap among leaders working across critical infrastructure and operational technology environments. The course equips ICS managers with the experience and tools to address the business and industry pressures to manage cyber threats and defenses in a way that prioritizes the business as well as the safety and reliability of ICS operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints in cyber-physical environments and will gain a nuanced understanding of how to manage the people, processes, and technologies across their organizations. ICS418 empowers both new and established ICS security managers.

https://www.sans.org/cyber-security-courses/ics-security-essentials-managers/

# Top 100 industrial control system abbreviations for easy reference

ACDC - Active Cyber Defense Cycle

ACL - Access Control List

AD - Active Directory

AGC - Automatic Generation Control

AM - Amplitude Modulation

ANSI - American National Standards Institute

AP - Access Point

APT - Advanced Persistent Threat

ARP - Address Resolution Protocol

BACnet - Building Automation and Control Network

BE2 - BlackEnergy2

BE3 - BlackEnergy3

BES - Bulk Electric System

BGAN - Broadband Global Area Network

BLE - Bluetooth Low Energy

BMS - Building Management System

BPF - Berkeley Packet Filter

C&C - Command-and-Control

C2 - Command-and-Control

CANbus - Controlled Area Network Bus

CART - Complete, Accurate, Relevant, and Timely

CI - Critical Infrastructure

CIA - Confidentiality, Integrity, and Availability

CIP - Common Industrial Protocol

CIP - Critical Infrastructure Protection

CSIRT - Computer Security Incident Response Team

CVSS - Common Vulnerability Scoring System

DCE - Distributed Computer Environment

DCS - Distributed Control System

DDoS - Distributed Denial-of-Service

DFIR - Digital Forensics and Incident Response

DHCP - Dynamic Host Configuration Protocol

DMZ - Demilitarized Zone

DNP - Distributed Network Protocol

DNP 3 - Distributed Network Protocol 3

EEPROM - Electrically Erasable Programmable Read-Only Memory

EMS - Energy Management System

EMT - Electro Magnetic Transmission

ERT - Embedded Device Robustness Testing

ESD - Emergency Shutdown Systems

FAT - Factory Acceptance Test

FEP - Front-End Processor

FIP - Factory Instrumentation Protocol

FM - Frequency Modulation

GNSS - Global Navigation Satellite Systems

GPO - Group Policy Object

GPS - Global Positioning System

HART - Highway Addressable Remote Transducer

HAZOP - HAZard and OPerability

HIDS - Host Intrusion Detection System

HMI - Human Machine Interface

HVAC - Heating, Ventilation, and Air Conditioning

I/O - Input/Output

IACS - Industrial Automation and Control Systems

ICS - Industrial Control System

IDS - Intrusion Detection systems

IED - Intelligent Electronic Device

IIoT - Industrial Internet of Things

IoC - Indicators of Compromise

IPC - Inter Process Communication

IPFIX - IP Flow Information Export

IPv4 - Internet Protocol Version 4

IPv6 - Internet Protocol Version 6

IR - Incident Response

IRP - Incident Response Plan

IRT - Isochronous Real-Time

ISC - SANS Internet Storm Center

ISM - Industrial, Scientific, and Medical

IT - Information Technology

LAN - Local Area Network

LAPS - Local Administrator Password Solution

LD - Ladder Diagram (or Ladder Logic)

LDAP - Lightweight Directory Access Protocol

LLDP - Link Layer Discovery Protocol

LoS - Line-of-Sight

LotL - Living-off-the-Land

MAC - Media Access Control

NSM - Network Security Monitoring

NSTB - National SCADA Test Bed Program

NTP - Network Time Protocol

OLE - Object Linking and Embedding

OSHA - Occupational Safety and Health Administration

OSI - Open Systems Interconnect

OT - Operational Technology

PERA - Purdue Enterprise Reference Architecture

PLC - Programmable Logic Controller

PPE - Personal Protective Equipment

PV - Process Value/Variable

RDP - Remote Desktop Protocol

RT - Real-Time

RTOS - Real-Time Operating Systems

RTU - Remote Terminal (Telemetry) Unit

SAT - Site Acceptance Test

SCADA - Supervisory Control and Data Acquisition

SIEM - Security Information Event Management

SIF - Safety Instrumented Functions

SIL - Safety Integrity Level

SIS - Safety Instrumented System

SPAN - Switched Port Analyzer

ST - Structured Text

STIX - Structured Threat Information eXpression

TAXII - Trusted Automated eXchange of Indicator Information

TCP - Transmission Control Protocol

TEM - Threat and Environment Manipulation

TTP - Tactics, Techniques, and Procedures

TTX - Tabletop Exercise

UA - Unified Architecture

UAC - User Account Control

UDP - User Datagram Protocol

VSAT - Very Small Aperture Terminal

VLAN - Virtual Local Area Network

VM - Virtual Machine

WAN - Wide Area Network

WLAN - Wireless Local Area Network