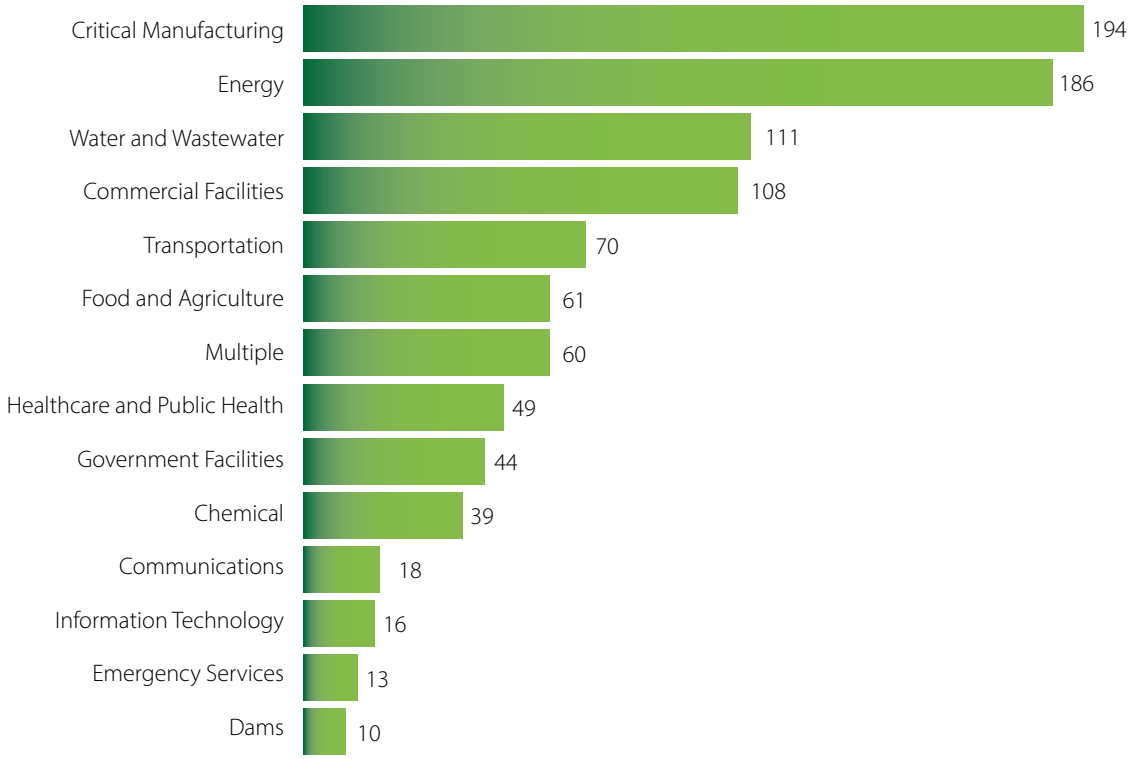

SECURANCE
CONSULTING
the advantage of insight
PROTECT YOUR CONNECTIONS: SECURITY STRATEGIES FOR INDUSTRIAL CONTROL SYSTEMS
www.securanceconsulting.com

INTRODUCTION

Utilities, water districts, transportation agencies, airports, and many other businesses rely on industrial control systems (ICS) to automate and operate critical processes. ICS are easily integrated with business systems and can be implemented on a large scale to increase performance, reliability, and durability. Because ICS are essential to delivering and managing critical resources and infrastructure, they must be protected against cyber threats. Tampering with ICS can lead to dangerous consequences for human lives, a country's critical infrastructure, and the environment.

Top Industries Reporting ICS and IT Security Vulnerabilities



InfoSec, 2021[1]

Even if the ICS itself is reliable and secure, its connections to IT systems create vulnerabilities that, if exploited, could endanger the public and cause millions of dollars worth of damage.

WHAT ARE ICS?

ICS is a general term used for the integration of hardware and software with network connectivity to support critical infrastructure.[2] ICS fall into the broad category of operational technology (OT), which includes various types of control systems used to automate and operate industrial processes. The most common types of ICS include:

Supervisory Control and Data Acquisition (SCADA)

SCADA is a type of control system that automates industrial processes by capturing OT data. The SCADA system connects the sensors that monitor equipment, such as motors, pumps, and valves, to on-site or remote servers.[3]

Distributed Control Systems (DCS)

A DCS allows individual control of numerous dispersed control systems or processes. The system or process is controlled by a network of autonomous controllers, rather than a central unit.

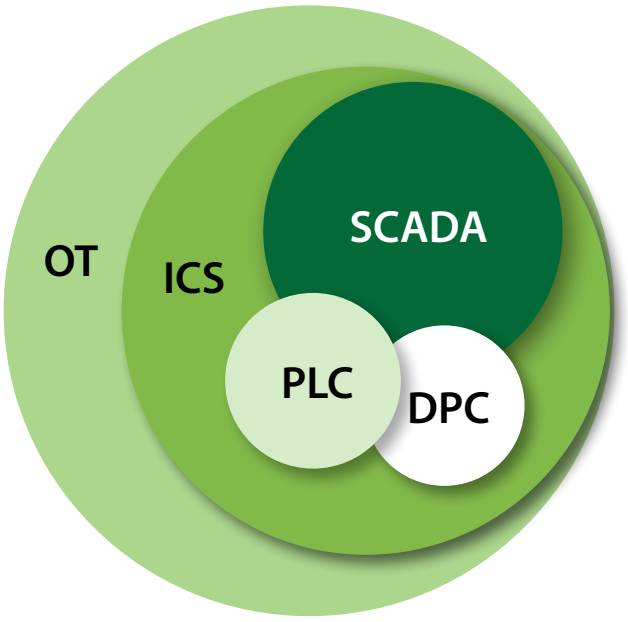
Remote Terminal Units (RTUs)

An RTU is a microprocessor-based electronic device used to link various ICS devices to DCS or SCADA. RTUs route sensor data from input streams to an output stream for transmission to a centralized ICS command center. RTUs are also referred to as remote units of telemetry and | or remote units of virtual control.

Programmable Logic Controllers (PLCs)

PLCs can be networked together to share data and provide centralized monitoring and control capabilities. In many sectors, control systems composed of networked PLCs are replacing both plant DCS and RTU-based systems.[4]

What's The Difference Between OT, ICS, and SCADA?



Kuppinger Cole Analysts, 2015[5]

HOW DO ICS WORK?

An ICS has four primary functions[6]:

Data Acquisition

Most ICS include a SCADA system. SCADA systems acquire data from sensors and network devices connected to PLCs. They measure parameters such as speed, temperature, weight, flow rate, gaseous emissions, and pressure. This raw data is sent to a PLC for processing, then to a human machine interface (HMI) for a human operator to analyze and make decisions.

Network Data Communication

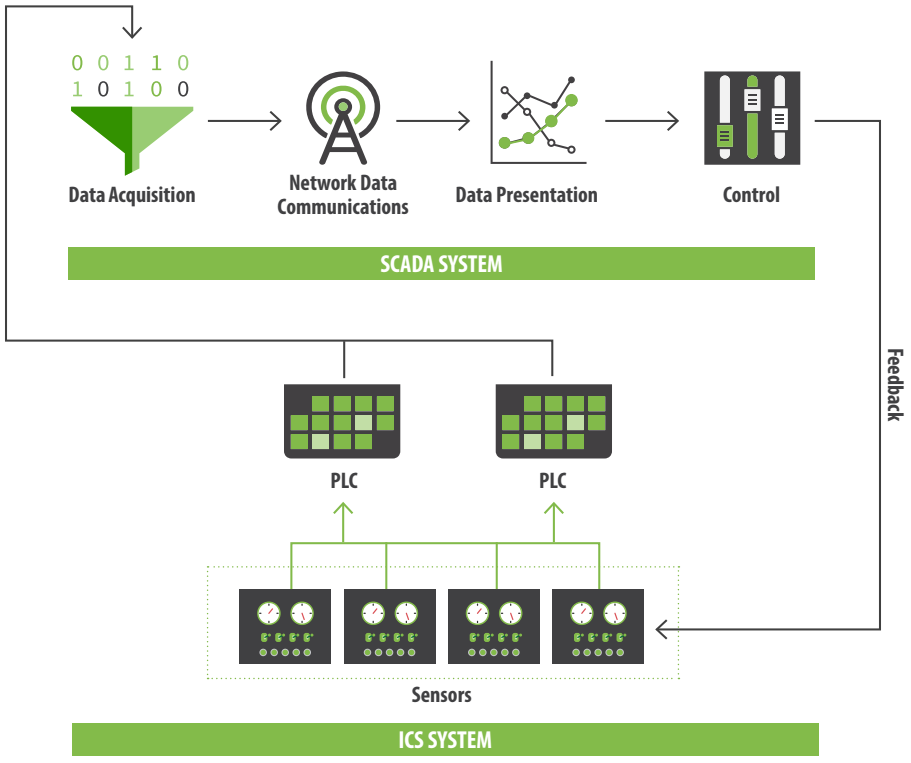
When an ICS controls multiple systems from a central location, the network uses wired or wireless communication to transmit data between machines and operators.

Data Presentation

SCADA systems report data to an HMI where the information is displayed to a human operator. This master station continuously monitors all sensors and alerts the operator when there is an incident or dysfunction, such as when a control factor is not functioning within its normal operational range.

Control

ICS can be programmed to make control decisions based on data collected from the sensors. Control functions may include turning power on and off, adjusting temperature, decreasing or increasing speed, and regulating industrial processes. Frequently, a hybrid model that combines ICS automation with manual techniques is employed.



SECURITY BENEFITS AND CONCERNS

Benefits

The benefits of implementing ICS include:

- **Providing real-time visibility across the OT environment—** ICS are used when there is a need to monitor multi-site operations from a central location. If adequately monitored, ICS can alert operators to a cyber incident and allow them to respond to multiple incidents at once to minimize overall damage.
- **Improving efficiency and minimizing downtime—** ICS allow operators to immediately detect cyber attacks and alert the response team, facilitating a quick and efficient response. When an operational incident occurs, ICS can detect, monitor, and notify operators instantaneously, saving time, resources, and overall costs to the organization and its consumers.
- **Protecting assets—** The primary objective of all ICS is to protect assets and maximize asset life. If critical assets are compromised, there could be significant internal and external repercussions.

> ICS are more interconnected with IT systems than ever. The average hacker has evolved, as well, and the Internet, with its abundance of information, makes compromising increasingly open ICS systems and protocols much easier.

Concerns

Although there are significant advantages to implementing ICS, there are drawbacks to consider, as well, including:

- **The need for availability 24 | 7 | 365—** Since these systems control physical processes that support power, transportation, water, gas, and other critical infrastructure, it is difficult and expensive to shut them down for any period of time. With only five minutes a year of downtime allowed for many ICS, collecting evidence to investigate potential security breaches or malware infections is challenging.
- **Maintaining ICS security on older systems—** Most systems running in the United States are legacy systems that are 15 to 30 years old. These systems are not designed for connectivity, but replacing them with new technologies is often cost-prohibitive. Organizations must find ways to increase the security of legacy systems and the new technologies they connect to. [7]
- **Reliance on other devices and systems—** ICS are no longer isolated. Organizations now have access to more expeditious communication and more robust data collection and aggregation methods. However, integrating ICS with modern IT systems introduces unprecedented risk exposure.

Common Attacks Against ICS

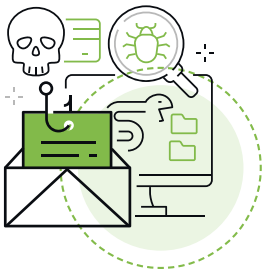
Although the Internet has revolutionized the way the world communicates, it has also provided a forum where malicious attackers can share confidential hacking tools, gain intelligence on their targets' infrastructures, and wage cyber warfare. The following are examples of vulnerabilities and attacks that commonly lead to security breaches in ICS:

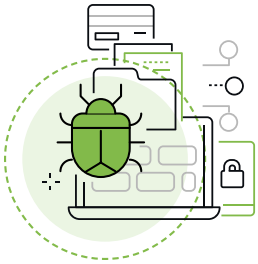
Denial of service (DoS) attacks— DoS attacks involve sending reset, halt, or reboot commands that can significantly slow down control systems.

Insecure protocols— Outdated protocols still used for ICS operations, are inherently insecure. Communication protocols for control devices do not typically require authentication to remotely execute commands, and there are no encryption options available.

Basic access control gaps— ICS devices should have at least basic access controls separating the system software and application program modes, but many fail to meet this requirement. Server and terminal authentication is often nonexistent and, when it does exist, ineffective. Moreover, differentiation of access privileges between administrators and end users is generally unavailable or unenforced.

Man-in-the-middle (MITM) attacks— MITM attacks include spoofing, replay attacks, and network sniffing. When ICS lack proper encryption and authentication controls, malicious attackers exploit these weaknesses to corrupt in-transmission instructions, commands, or alarms.





Control system device corruption— Control logic software is an easy target for malicious actors, and a corrupted device can grant them the ability to damage the system, cause service disruptions, and present safety risks. The firmware for control logic is not protected, meaning configurations can be easily altered by anyone with access.[8]

Internal struggles— All companies, in every industry, have financial concerns around implementation and maintenance costs. Under pressure to streamline and automate processes, and cut costs, businesses run the risk of cutting corners. Each connection between an ICS and the IT network creates new vulnerabilities and attack vectors, so streamlining the relationship between physical and data control must be handled with care.

While there are solutions to deal with these attack vectors for typical IT systems, one size doesn't fit all when it comes to ICS. Special precautions should be taken when implementing any kind of IT solution, such as intrusion detection and prevention systems (IDS | IPS) or data loss prevention (DLP) solutions, in an ICS environment. An organization might even find that entirely new security solutions (network segmentation, a two-port firewall, or boundary protection, for example) are required for the ICS environment.[9]

MAINTAINING ICS SECURITY

Security and reliability are critical to ICS. Conducting regular risk assessments is a best practice for every organization to gain insight into the likelihood of an attack and its possible impact on critical systems. For ICS, this means identifying threats and vulnerabilities in physical processes, digital counterparts, systems, and the environment.

> "Critical infrastructure across all sectors depends on control systems for safe and efficient operation. The security of ICS is among the most important aspects of our collective effort to defend cyberspace."[10]

The U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) developed seven strategies that organizations can implement to counter common exploitable weaknesses in ICS:[11]

1

Implement Application Whitelisting (AWL)
AWL will help detect and prevent the execution of malware uploaded by adversaries, and protect infrastructure from harmful code.

2

Ensure Proper Configuration | Patch Management
Organizations should prioritize patching and configuration management and test updates outside the production environment before installing them.

3

Reduce Attack Surface Area

This will include:

- Isolating ICS from untrusted networks
- Locking down unused ports
- Turning off unused services
- Allowing real-time connectivity to external networks only if there is a defined business requirement or control function

4

Build a Defensible Environment

Installing preventative measures to stop a breach in its tracks is crucial to limiting damage. For ICS, specifically, network segmentation prevents bad actors from escalating privileges and moving laterally, while allowing normal system communications to operate.

5

Manage Authentication

If a bad actor accesses legitimate credentials, the consequences for the organization can be disastrous. Implementing strong authentication methods, such as multi-factor authentication, privileged access for certain users, and strong passwords, are just a few ways organizations can protect themselves from an attack.

> "The state of ICS cybersecurity is not great, but it is improving. With every new attack, an increase in awareness and of the manner in which these attacks are implemented gives us as defenders a greater chance at preventing the next big attack."[12]

6

Implement Secure Remote Access

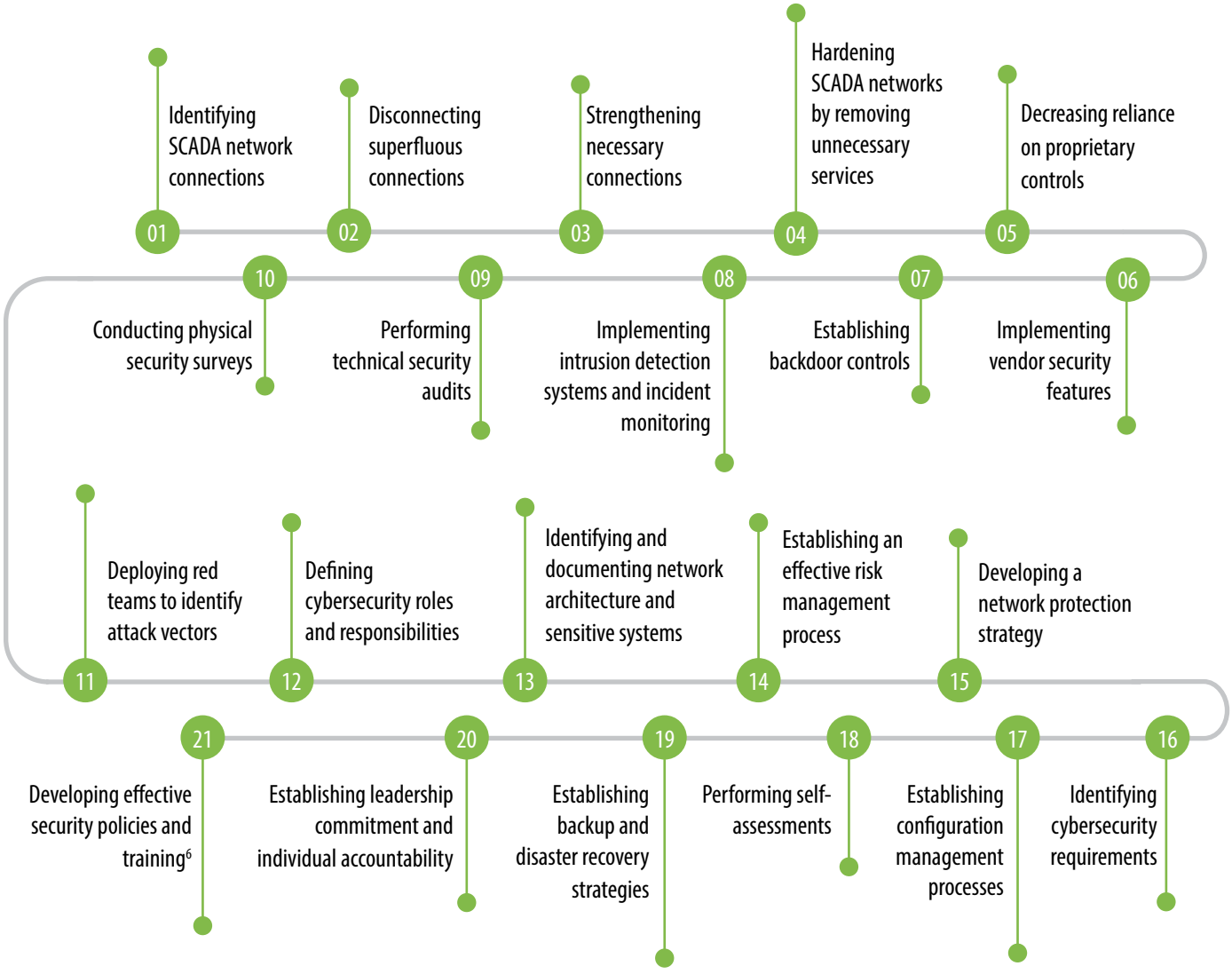
Remote access should be operator-controlled and time-limited. Use the same remote access paths for vendor and employee connections; do not allow double standards.

7 Monitor and Respond

Defending ICS from cyber attacks requires active threat monitoring and a well-defined response strategy. Having an up-to-date incident response plan in place will save resources, time, and costs. When suspicious activity is detected, be ready to respond immediately. Remember that the IT incident response plan may not be adequate for the ICS network.

21 Steps to Secure SCADA Networks

The Department of Energy released a 21-step guide for improving the cybersecurity of SCADA networks. The guide addresses the following essential actions to protect SCADA security[13]:



CONCLUSION

Too Interconnected To Fail

Because ICS depend on other systems for communication and process control, they are vulnerable to a wide range of cyber attacks. Interconnection between devices means that a process failure in one location can turn into a cascading failure across the connected infrastructure. Without layered security defenses, ICS are easy prey for bad actors, whose exploits can cause service disruptions, product contamination, and even harm to the general population.

Although cyber attacks are evolving steadily, so are the strategies for improving ICS security. The key is to establish an ongoing risk management process and follow through by conducting regular risk assessments, evaluating security controls, and instating layered security, so that organizations can ensure both the safety and security of ICS, including the associated physical systems, processes, and environments. The stronger the security measures implemented, the less appealing a system appears to a potential attacker.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://resources.infosecinstitute.com/topic/ics-scada-threats-and-threat-actors/
2. https://www.techtarget.com/whatis/definition/industrial-control-system-ICS
3. https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/
4. https://13sqft.com/blog/industrial-control-system-type-and-benefits
5. https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference
6. https://www.plctechnician.com/news-blog/scada-system-what-it-and-how-it-works#:~:text=%20Functions%20of%20a%20SCADA%20System%20%201,HMI%20or%20a%20HCI%20(Human%20Computer...%20More%20
7. https://www.computerweekly.com/news/2240232680/Industrial-control-systems-What-are-the-security-challenges?_gl=1*cr64z*_ga*MTcwMjk4MzE0NC4xNjEyMzYwMTAz*_ga_TQKE4GS5P9*MTY1NzExOTk4Ny4yLjAuMTY1NzExOTk4Ny4w&_ga=2.200235052.341065631.1657119987-1702983144.1612360103
8. https://www.cse.wustl.edu/~jain/cse571-11/ftp/ics.pdf
9. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
10. https://www.cisa.gov/ics
11. https://www.cisa.gov/uscert/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf
12. https://www.hackthebox.com/blog/ics-cyber-attacks
13. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com