ICS SCADA: their Role & Importance in Today's World

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

April 5, 2025

Assignment:

In this write-up you will research **SCADA systems**, describing how they work, explaining the vulnerabilities associated with critical infrastructure systems, and the role SCADA applications play in mitigating these risks.

ICS SCADA: their Role & Importance in Today's World

What is ICS SCADA, and what are its Components?

Industrial Control Systems (ICS) is a broad overarching term for the entire setup that controls and automates industrial processes. The ICS is the "whole brain" that includes all the hardware, software, and systems working together to manage everything. Typical industries include electric power generation, transmission and distribution systems/grids, water treatment and distribution systems, and oil and gas pipeline monitoring and control systems (ICF, 2016). ICS components include controllers, sensors, actuators, networks, and Human-Machine Interfaces (HMIs) (Parida, 2023). Controller elements may include Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and Supervisory Stations.

The Distributed Control System (DCS) is a network of interconnected controllers, computers, and other automation devices that monitor, and control geographically distributed industrial processes (Parida, 2023). PLCs and RTUs are similar, acting like "local translators" for gathering and converting raw data into a digital format for SCADAs. PLCs control manufacturing processes like assembly lines to ensure each step of the manufacturing process is proper and efficient; RTUs are directly connected to physical equipment like sensors and actuators, converting electrical signals from the equipment into digital values and providing control over the sensory equipment. A Supervisory Station refers to the software and servers responsible for communication with the field (PLCs, RTUs), while HMI software runs on the workstations in the control room.

Subcomponents of ICS

The other components of ICS help gather and display data for the controllers to use in their communications and decision-making. Sensors monitor the conditions within the systems, like temperature, pressure, or flow rate, and send this data to the controller; actuators carry out

commands from the controllers, like motors, pumps, valves, and relays (Parida, 2023). For example, suppose a sensor in a manufacturing plant detects an overheating machine. In that case, the controller may send a command to an actuator to turn on a cooling system or to turn off the system machine altogether.

Networks are the backbone of ICS, enabling the ICS to communicate with all the other components, and they can be wired or wireless while using various protocols. HMIs allow human operators to view, monitor, and interact with the ICS. They provide virtual representations of the system, displaying the sensory data and allowing operators to control the system from that one "master" control room or device (ICF, 2016). They are like standard software applications using Graphical User Interfaces (GUIs) to better assist users with essential operating functions rather than using things like the Command Line Terminal, making software application usage more user-friendly. Therefore, ICS is the big picture: it encompasses various components, technologies, and methods to keep operations properly running by gathering data from the field, processing the data, and sending control commands to the field.

What is SCADA?

Supervisory Control and Data Acquisition (SCADA) is a specific part of ICS designed for monitoring and controlling geographically dispersed industrial processes (Parida, 2023). It is the "eyes and ears" of the ICS "brain": it focuses on gathering real-time data (i.e., temperature, pressure, and flow rates) from the field through the sensors and machines while virtually displaying it through HMIs to human operators. Human operators can remotely monitor and control those host devices, like managing a factory's machinery or power plant's turbines. SCADAs and HMIs allow the operator to communicate with different machinery through commands like "shut down

pump A." Thus, ICS controls the entire system and makes most decisions while SCADA only supervises and transmits communication.

ICS SCADA Workflow Scenario

For example, let us use the scenario of managing water flow in a hydroelectric dam. The dam has multiple sensors for gauging water levels in the reservoir and comparing the information to predetermined baselines. The RTUs collect information from sensors with the help of PLCs and send it to the SCADA server over a fiber optic leased line. The server processes the information and displays it on the HMI for the operator to review and monitor.

Then one day, a storm strikes the area and elevates the reservoir's water level to a dangerous height. Using the SCADA system, the operator quickly opens the dam gate to release water in a controlled and efficient manner. The operator's command travels back to the RTU, triggering the gate open and increasing the water flow. Eventually, sensors confirm the water level has returned to a safe range.

Vulnerabilities Associated with Critical Infrastructure Systems

First, modern-day critical infrastructures may have weak physical protection and limited computational power (Homeland Security (DHS), 2016b). Weak physical protection can include unsecured perimeters, lack of surveillance through commercial cameras and guards, exposed equipment to the elements, poor access control like weak locks, and lack of redundancy and physical deterrence from natural disasters. Weak devices with limited computational power tend to have little security coded within or surrounding them, making them easy targets for threat actors using spoofing, replay attacks, or DDoS attacks.

Second, some devices may be obsolete or antique/legacy, behind modern technology and society, taking years to upgrade or conduct simple refreshes/resets (ICF, 2016). The devices of the past were not built or engineered with a "security-first" mentality, making them especially vulnerable to modern-day cyber threats. That includes using poor passwords, key management software and practices, and data at rest and transit in plain sight rather than standard encryption protocols like VPNs.

Third, remote devices are sometimes too complex to upgrade, especially when they are hard to reach places by human intervention (ICF, 2016). The weather may become a factor in how updates and data are transmitted because the weather may obstruct such communications, resorting to incomplete or corrupted updates and gaps within firewalls. Also, some devices may not be able to be updated remotely; instead, their OS may only contain the necessary applications to conduct their work, but they can only receive updates through physical interaction with a small form factor media device. Fourth, all traffic may be routed to just one port, not providing any redundancy should the single point of failure fail (ICF, 2016). Lastly, eliminating or closing unused and unnecessary ports is usually good cyber hygiene and makes it easier to control and manage the data traffic; however, it does make it easier to hack and disrupt a single location of data flow.

SCADA's role in mitigating those vulnerabilities and risks

Organizations can use a broad and deep range of tools, policies, and procedures to help mitigate vulnerabilities and risks (Homeland Security (DHS), 2010a and 2016b; ICF, 2016; CISA, 2025). First, real-time monitoring helps human operators catch anomalies that might signal a physical or cyber threat. Early detection of problems can help prevent their escalation. Second, a centralized control connection allows operators to remotely and swiftly adjust equipment without needing to be on-site, especially when there are physical access delays, or it is too dangerous for a

human operator. Third, integrating SCADA with physical security provides more “eyes” on the physical structures, allowing a more holistic approach using cameras, motion sensors, and alarms. Fourth, SCADA provides automated responses without direct human intervention. Automatic responses based on predetermined rules and coding scripts can prevent processes from reaching dangerous levels or reducing damage to infrastructures should they bypass the first lines of defense.

Fifth, SCADA helps with data logging and analysis in an easily digestible manner with the help of HMIs and GUIs. Logging and analyzing the data helps human operators create baselines, learn from past successes and mistakes, and adjust for future operations to better protect and improve industrial processes. Lastly, SCADA provides cybersecurity support, protecting against cyber threats targeting different applications and technologies associated with modern industrial processes. SCADA can implement encryption, user authentication, network monitoring, detection, and prevention (e.g., edge Firewalls, IDS, IDS) against unauthorized access, both insider and outsider actors.

References

CISA. (2025, April 1). *Recommended Cybersecurity Practices for Industrial Control Systems*. Retrieved from Cybersecuirty & Infrastructure Security Agency (CISA): https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

Homeland Security (DHS). (2010a). Configuring and Managing Remote Access for Industrial Control Systems. *Centre for the Protection of National Infrastructure (CPNI)*, 66. Retrieved from https://www.cisa.gov/sites/default/files/2023-01/RP_Managing_Remote_Access_S508NC.pdf

Homeland Security (DHS). (2016b). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies. *Industrial Control Systems Cyber Emergency Response Team*, September.

ICF. (2016). Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. *U.S. Department of Energy*, 145.

Parida, B. (2023, December 15). *ICS SCADA: A Comprehensive Guide to Industrial Control Systems and Supervisory Control and Data Acquisition*. Retrieved from WEVOLVER: https://www.wevolver.com/article/ics-scada