SCADA Systems Dissection

Jayden Dorey

CYSE 200T

Professor Kirkpatrick

20 September 2026

Definitions

SCADA (Supervisory Control and Data Acquisition) systems are used by physical operators to maintain smooth operations in critical infrastructure and industrial settings through monitoring and controlling physical devices on the network. (Kirkpatrick, n.d.). It helps to think of SCADA as a sort of "command center" that manages the tasks and actions of other hardware processes in the organization or infrastructure. Actions are controlled by SCADA using RTUs or PLCs, depending on what action is being carried out. RTUs (remote terminal units) are used to facilitate automated functions or functions that are meant to be carried out at a specific time. PLCs (programmable logic controllers) are used to carry out actions that are dictated by other actions, like an "if" statement.

Since SCADA is broken up into two sections — supervisory control and data acquisition — the latter process begins in these two controls. Data is gathered from these two controls as points, and points are converted to actionable data, allowing the operator to make decisions about correcting or monitoring a process based on the output data. This process is made possible through the HMI, or Human Machine Interface. The HMI allows the operator to control and communicate with the SCADA system and make adjustments to controls and processes, like RTUs and PLCs.

Use Across the Fields

Healthcare

In the healthcare industry, SCADA systems control almost the entire environment. Aside from the people aspect, like doctors, nurses, and staff, SCADA systems are used to control the machinery that keeps patients and personnel comfortable and alive. Specifically, remote access is heavily used to monitor and make real-time changes to patient technology (Pabalkar & Verma,

2023). A good example of this would be a nurse at a nursing station receiving an alert through their SCADA system's HMI that a patient in room 123 has an oxygen machine that is sending an alert detailing the oxygen level is too low. The nurse could make the decision to raise the amount of oxygen to the patient from this system. Similarly, a maintenance person could use a SCADA system to change and align the temperature of the hospital on a specific floor.

Manufacturing

In a manufacturing setting, SCADA is used to control and automate almost all processes on-site. One common use of this system is energy monitoring of all the components (Process Solutions, Inc., 2025). The SCADA system allows the operator to track the amount of energy being consumed and output by each piece of equipment on the site floor and enables alerts in case either metric spikes. This real-time monitoring allows the control to mitigate any downtime that might come as a result of increased energy output, which could be a sign of a potential overheating problem. Aside from energy, key metric monitoring is another way SCADA is used in this setting. It allows data transmission to the operator to see an overview of the productivity of machinery across the site.

Vulnerabilities & Their Effects

Scenario #1 – Integer Overflow

In this situation, a control is directly compromised at the source. If the attacker is able to flood the data recovery channel with different integer inputs of unacceptable size, it could lead the control freezing/seizing up or cause an operator to have to make a decision that is as a result of an issue that is not present. For example, if the attacker were to flood the input channel for controllers with integers different than 0 and 1, this could trigger an alert to the HMI that a control has stopped relaying data, causing the operator to troubleshoot the device, interrupting

other processes unnecessarily, leading to increased and unnecessary downtime. In drastic cases, the changes made by the operator could impact actions controlled by PLCs down the line. Furthermore, when the data is finally gathered for review, it could mislead the reviewers to believing something inaccurate based on anomalies introduced by the attacker.

Scenario #2 – Evil Twin

An attacker could create an evil twin wireless connection, allowing them to gain access to all the hardware and machinery connected to the original system by forcing them to reconnect and connect to the evil twin. Using their own SCADA, they would be able to wreak havoc on controls and data, effectively destroying the CIA pillars of the company; confidentiality compromised by allowing proprietary data to escape company networks, availability compromised by moving all devices from one network to an illegitimate one, and integrity compromised by allowing for potential intentional alteration of data collected. In a hospital setting, this could lead to severe legal ramifications and sensitive data breaches for PHI of countless patients. If the attacker wanted to make things more severe, they could also transition to a DoS attack, holding the network-connected devices hostage on the evil twin network until their demands were met. Because "a SCADA system is not easy to patch when security vulnerabilities are discovered in one of its embedded software layers," if a threat were to find its way to the network, the damage would be catastrophic and long-lasting (Kirkpatrick, n.d.).

Improvement

Network segmentation would be one option for combatting potential threat actors. In practice, the best course of action would be to place SCADA and their database on separate networks and install firewalls between it and every device it communicates with directly. This would eliminate the possibility of a threat actor gaining access to "command central" if they

managed to infiltrate the general company network. The firewalls between each device and SCADA adds an additional layer of security in case an attack impacts one piece of machinery or one control. If the firewall has an IDS/IPS, the operator would be made aware of the threat and it would either be prevented by the firewall or taken care of by the operator. Placing the database on a separate network would also add to the security stance of the organization, increasing the difficulty for an attacker to impact the integrity of the data gathered by the RTUs and PLCs. Because these controls would need to directly communicate and relay data to the database, their connection would need to be encrypted on both sides, given that the database would need to receive data from the controllers and relay that data to the HMI in order for the operator to make real-time formed decisions.

References

Kim, D., & Solomon, M. G. (2023). *Fundamentals of Information Systems Security* (Fourth ed.). Jones & Barlett Learning. https://reader2.yuzu.com/reader/books/9781284238815

Kirkpatrick, C. (n.d.). *SCADA Systems*. Google Drive. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0

Pabalkar, V., & Verma, R. (2023). SCADA in Healthcare. In *ICT Infrastructure and Computing* (pp. 91-102). 10.1007/978-981-99-4932-8_10

Process Solutions, Inc. (2025, June 22). *What is SCADA and how its used in Manufacturing*. Process Solutions. https://processsolutions.com/understanding-scada-and-what-it-can-do-for-you/