Ava McLaughlin

CYSE 200T

March 30, 2025

SCADA Systems

Supervisory Control and Data Acquisition (SCADA) Systems oversee and coordinate large-scale infrastructure, facilities, and industrial operations (Using SCADA to Protect Critical Infrastructure and Systems). SCADA consists of both hardware and software that collects, processes, and monitors data continuously so that processes can be controlled externally.

SCADA Components

There are many parts to a SCADA system, among the most notable are hardware devices called Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). RTUs deal mostly with data collection, while PLCs can perform simple programmed tasks to automate a process remotely (What are the differences between PLC and RTU?). While a SCADA system typically does not directly control processes in real time, it coordinates and monitors them as they occur. There are also sensors and field instruments that monitor physical variables like temperature, pressure, flow rate, and level, which the RTUs and PLCs detect and process (Malisko, 2024). This information is sent to the SCADA server, which collects and stores data and interacts with the Human-Machine Interface (HMI). The HMI is software that allows a person to interpret collected data and perform control functions. It presents data in mimic diagrams, so that the operator can see a visual representation of the monitored system (Using SCADA). For instance, a graphical display of a conveyor belt in a manufacturing plant can show that it is actively transporting materials, along with the speed and load being carried; the operator can then stop or adjust the belt's operation as needed.

SCADA in Cybersecurity

Although SCADA Systems are extremely beneficial and efficient when it comes to critical infrastructure operations, they also introduce some Cybersecurity concerns. A cyberattack would have severe consequences, as an attacker could disrupt the water supply or shut off electricity to a city; they could even tamper with nuclear reactors, which would undoubtedly be extremely dangerous (A comprehensive guide to SCADA cybersecurity). Because SCADA uses hardware and software interdependently, there must be strong Information Technology (IT) and Operational Technology (OT) precautions in place to protect the various entry points. As Mr. David Price discussed, OT is particularly vulnerable because these systems were not designed with security in mind and are difficult to replace. SCADA Systems should be implemented with “regular assessments, strong access controls, network segmentation, and advanced encryption” (Asplund, 2024). Network segmentation is an important protection because it creates isolated segments within the network, preventing unauthorized access between IT and OT systems.

“Using SCADA to Protect Critical Infrastructure and Systems” notes that there are two main SCADA Systems security threats, those being “unauthorized access to software” and “the packet access to network segments that host SCADA devices” because there is often little “security on actual packet control protocol;” SCADA providers are mitigating these risks with industrial VPNs, firewalls, and whitelisting solutions (Using SCADA). Since cyber threats are constantly evolving, systems can likely never be fully secure. Therefore, employees should receive training on cybersecurity best practices, backups should be conducted regularly and securely stored, and businesses must always have an incident response plan in place.

References

A comprehensive guide to SCADA cybersecurity. *Claroty*. (2024, February 1). https://claroty.com/blog/a-comprehensive-guide-to-scada-cybersecurity

Asplund, A. (2024, July 1). Is your SCADA system secure? A deep dive into network and cybersecurity. *APCO Inc*. https://www.apco-inc.com/resources/is-your-scada-system-secure-a-deep-dive-into-network-and-cybersecurity

Malisko. (2024, September 5). What is SCADA?: SCADA Systems explained. https://malisko.com/scada-systems-explained/

Using SCADA to Protect Critical Infrastructure and Systems. *Scada Systems*. (n.d.). https://docs.google.com/document/d/1VnMlL2YmcW5Jg4MdDa1dt5fJpmQM0KVH/edit?tab=t.0#heading=h.one1gay4uxf3

What are the differences between PLC and RTU? *Mikrodev*. (2024, February 14). https://www.mikrodev.com/what-are-the-differences-between-plc-and-rtu