SCADA Systems and Infrastructure Security

Shayla Harmon

Old Dominion University

CYSE 200T

Charlie Kirkpatrick

September 20, 2026

SCADA Systems and Infrastructure Security

Supervisory Control and Data Acquisition (SCADA) systems are an important part of many industrial operations. SCADA systems are a type of industrial control system (ICS) that is used to monitor and coordinate physical processes, which include water treatment, wastewater treatment, gas pipelines, wind farms, transportation systems, manufacturing, refining, and power generation (SCADA Systems, n.d.). Cybersecurity is important for these systems because they interact with physical equipment and processes. An attack could affect not only an organization's computer systems but also the physical operations that people and communities depend on daily. SCADA systems provide centralized monitoring, data collection, alarms, and control but have vulnerabilities when it comes to connectivity and outdated technologies.

SCADA Systems and Infrastructure

SCADA systems are centralized systems that monitor and control processes across a facility or across large geographic areas. A typical SCADA system includes a supervisory system, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), communication infrastructure, and a Human Machine Interface (HMI). RTUs connect to physical equipment and convert signals from the equipment into digital information. That information includes the status of a valve or measurements of pressure, flow, current, or voltage. RTUs can also send commands to the equipment, such as opening or closing a valve or changing the speed of a pump (SCADA Systems, n.d.).

These systems are used in many industries that are important to everyday life. In water and wastewater treatment, they can monitor and control processes involved in the distribution and treatment of water. In energy, SCADA can be used in the transmission of electricity, power generation, and wind farms. In addition, gas transportation, oil pipelines, traffic lights, and

railway systems depend on SCADA Systems. Manufacturing and industrial facilities can use SCADA to monitor production processes and equipment. The document also describes SCADA applications in facilities like airports, ships, and space stations (SCADA Systems, n.d.). To summarize, these examples show why protecting SCADA systems is important because they directly support services used by our society.

Cybersecurity Risks

One major vulnerability associated with SCADA systems is unauthorized access to software and control systems. The document identifies unauthorized access as a significant threat. Unauthorized access can include human access, intentional changes to software, viruses infections, or other problems that affect the control host machine (SCADA Systems, n.d.). If an unauthorized person gains access to a control system, they can change settings or interfere with normal operations.

Another vulnerability involves the communication networks that are used to connect multiple SCADA devices. According to the document, many SCADA control protocols have little or no security built directly into the packet control protocol. As a result, someone who can send packets to a SCADA device may potentially be able to control it (SCADA Systems, n.d.).

The transition from older isolated systems to modern networked SCADA systems has also increased risk exposure. Modern SCADA systems use network technologies and Internet Protocol (IP), which can allow greater connectivity but can increase vulnerability when systems are accessible through networks or the Internet. The document explains that although networked SCADA systems had increased vulnerability, standard protocols, and security techniques can also make security improvements possible (SCADA Systems, n.d.). This creates a serious risk,

because SCADA systems depend on communication between RTUs, PLCs, supervisory systems, and other devices.

Effects of a Cyberattack

A cyberattack against a SCADA system could have consequences beyond the loss of computer data. Since SCADA systems monitor and control physical processes, an attack could interfere with the operation of the infrastructure. For example, an attack on a water system could affect water distribution, while interference with electricity could disrupt power services. The document emphasizes that SCADA systems control physical processes such as water distribution, traffic lights, electricity transmission, gas transportation, and oil pipeline, making their security extremely important (SCADA Systems, n.d.).

A cyberattack could also create operational downtime and financial losses for an organization. The document notes that control system failures can have extremely high costs and that, in some circumstances, lives could even be lost (SCADA Systems, n.d.). This means that an attack could affect employees, customers, infrastructure, and the broader community. The potential impact is serious when an organization depends on continuous operation of its industrial processes.

Strategies for Improving SCADA Security and Resilience

Organizations can use several strategies to improve the security and resilience of SCADA systems. One strategy is implementing specialized industrial firewalls and VPN solutions. The document explains that vendors have developed specialized industrial VPN and firewall solutions for SCADA networks for SCADA networks using TCP/IP. These technologies can help protect communication between SCADA components and limit unauthorized network access (SCADA Systems, n.d.).

Organizations can also use application whitelisting to help prevent unauthorized software or application changes. The document identifies whitelisting as a security solution because it can prevent unauthorized application changes (SCADA Systems, n.d.). This can be useful for control environments where systems are expected to run specific applications and processes.

Finally, organizations should recognize that physical security alone is not enough. SCADA networks require protection of both their physical infrastructure and their software and communications. Limiting access to network switched and connections, protecting control hosts, and securing communication protocols can help reduce opportunities for attackers to reach SCADA devices. A layered approach that combines network security, access controls, application protection, and physical security can improve the overall resilience of these systems.

Conclusion

SCADA systems have a vital role in monitoring and coordinating critical infrastructure and industrial processes. They connect operators with physical equipment through components such as RTUs, PLCs, supervisory systems, communication networks, and HMIs. The system's use in water management, energy, transportation, pipelines, manufacturing, and other industries makes their security important to organizations and society. However, unauthorized access, insecure communication protocols, increased network connectivity, and weakness in physical and network security can create significant risks. An attack could disrupt physical processes, cause financial losses, and affect public safety. Organizations can reduce these risks by using industrial firewalls and VPNs, whitelisting applications, and stronger protection of network access. As SCADA systems continue to become more connected, protecting these systems will remain an important part of protecting critical infrastructure.

References

SCADA systems. (n.d.). [Course document].