SCADA Systems and Cybersecurity Risks

Marion Watkins

CYSE-200

September 22, 2026

SCADA Systems and Cybersecurity Risks

Before learning about SCADA systems, I mostly thought of industrial control as something that was separate from normal computer networks. SCADA shows why that is not really the case. SCADA stands for Supervisory Control and Data Acquisition, and it is used to monitor and control physical processes from a central location. NIST explains that SCADA systems collect information from field devices, send that information to a control center, and allow operators to monitor or control equipment. These systems can include remote terminal units, programmable logic controllers, sensors, communications equipment, and human-machine interfaces (Stouffer et al., 2023). Basically, SCADA connects computers and networks to real-world equipment, which is useful but also creates a serious cybersecurity problem.

SCADA is important because many of the systems people depend on every day use this type of technology. It can be used in electrical utilities, oil and natural gas pipelines, water and wastewater systems, transportation, manufacturing, and other industrial operations. For example, a water facility can use sensors to monitor things such as water pressure, flow, and chemical levels while operators use SCADA software to control pumps and valves. In manufacturing, SCADA can help monitor production equipment and make sure processes stay within certain limits. The benefit is that operators do not have to physically stand next to every piece of equipment all day. They can see what is happening from a control center and respond much faster when something changes.

The same connection that makes SCADA useful can also make it vulnerable. One major risk is unauthorized remote access. A SCADA system that is connected to another network or the internet gives an attacker another possible way into the system. The EPA has specifically warned that internet-connected operational technology can create major cybersecurity risks, especially

when systems are not patched or protected correctly (U.S. Environmental Protection Agency [EPA], 2023). Weak passwords, default passwords, poor access controls, and exposed remote access services can make this problem worse. Another vulnerability is outdated software or hardware. Industrial systems can stay in operation for many years because replacing equipment can be expensive and can interrupt operations. This means an organization may have old technology that was never designed with today's cybersecurity threats in mind.

Another important risk is that an attack on SCADA can affect physical processes instead of only stealing information. This is what makes SCADA cybersecurity different from some normal computer security problems. If an attacker gets control of a system that operates pumps, valves, electrical equipment, or manufacturing machines, the attacker could potentially change how that equipment operates. NIST points out that operational technology has unique safety, reliability, and performance requirements because these systems interact with the physical environment (Stouffer et al., 2023). In other words, a cyberattack could turn into a physical problem pretty quickly.

A good example is the February 2021 incident involving a water treatment facility in Oldsmar, Florida. According to EPA guidance, attackers used internet-facing remote access software to access the facility's system and attempted to increase the amount of sodium hydroxide being added to the drinking water. The attack was detected and stopped before the water reached the public at unsafe levels, but the incident showed what can happen when remote access to a control system is not properly secured (EPA, 2023). This example is important because it shows that SCADA security is not just about protecting files or passwords. It can also be about protecting public health and physical infrastructure.

There are several things organizations can do to improve SCADA security. First, they should limit who can access the systems and what each person is allowed to do. Strong passwords and multifactor authentication should be used for remote access whenever possible. CISA, NSA, FBI, and the Department of Energy have recommended multifactor authentication, changing default passwords, monitoring OT networks, and keeping known-good offline backups for ICS and SCADA environments (Cybersecurity and Infrastructure Security Agency et al., 2022). Network segmentation is another useful strategy. Instead of allowing the SCADA network to communicate freely with normal business networks or the public internet, organizations can separate the networks and strictly control the connections between them. Regular patching, vulnerability assessments, logging, and employee training are also important.

I also think organizations need to plan for what happens when security controls fail. No system is going to be completely immune from an attack, so having backups and an incident response plan matters. Operators should know how to safely continue critical operations if the SCADA system becomes unavailable. NIST recommends taking the special safety and reliability requirements of OT into account when designing security controls, rather than treating an industrial system exactly like a regular office computer network (Stouffer et al., 2023). This makes sense because shutting down a business laptop for security updates is very different from shutting down a water plant or electrical system.

Overall, SCADA systems are an important part of modern critical infrastructure because they allow organizations to monitor and control large and sometimes geographically spread-out operations. At the same time, connecting physical equipment to computer networks creates vulnerabilities that attackers can take advantage of. The biggest risks include weak access controls, exposed remote connections, outdated systems, and poor network separation. A

successful attack could affect an organization's operations and, depending on the system, could also affect public safety and everyday life. Securing SCADA therefore requires more than installing antivirus software. Organizations need to understand what equipment they have, limit access, monitor their networks, keep systems updated when possible, and have a plan for recovering from an attack.

References

Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, & U.S. Department of Energy. (2022, April 13). APT cyber tools targeting ICS/SCADA devices. https://www.cisa.gov/sites/default/files/publications/AA22-103A_APT_Cyber_Tools_Targeting_ICS_SCADA_Devices.pdf

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V. Y., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

U.S. Environmental Protection Agency. (2023). Evaluating cybersecurity during public water system sanitary surveys. https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf

U.S. Environmental Protection Agency. (2024). Internet-exposed HMIs pose cybersecurity risks to water and wastewater systems. https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf