SCADA Systems:

SCADA's Role in Infrastructure and its Associated Vulnerabilities

Andrew Judy

School of Cybersecurity, Old Dominion University

CYSE/IT 200T - Cybersecurity, Technology, & Society

Professor Chris Bowman

September 20, 2026

SCADA systems, which stands for “Supervisory Control and Data Acquisition systems” refer to industrial control systems, or ICS for short, and they are the systems that are used to monitor processes that occur in critical infrastructure. SCADA systems have a few subsystems, which include the Human Machine Interface, or HMI, which is the apparatus that is operated by a human operator and gives processed information to the operator. There is also a system that supervises and gathers the required data about the sensors in the system. Additionally, there are Remote Terminal Units, or RTUs, that are connected to process sensors which convert the signals from the sensor into digital data to then be sent back to the supervisory system. There are also Programmable Logic Computers, PLCs, which are used as field devices. In industries and critical infrastructure, SCADA systems are primarily used to monitor the processes that may occur in such industries and infrastructure. This paper will investigate how SCADA systems are used in industries and critical infrastructure, identify and detail cybersecurity-related vulnerabilities associated with these systems, analyze how a cyberattack on a SCADA system can affect organizations and society, and detail some strategies organizations can take to ensure the security and resilience of SCADA systems.

In industries such as energy, SCADA systems are used to monitor energy infrastructure, and collect data to make certain operational adjustments. In wind turbines and solar PV plants, for example, SCADA systems play a critical role in their operation. According to Enlitia, an asset performance management company based in Porto, Portugal, they say “SCADA systems are essential for overseeing power generation, grid integration, and asset maintenance in wind farms and solar PV plants. They gather extensive real-time and historical data such as: wind speed, turbine power output, gearbox temperature, pitch angle, rotor speed, and grid status. In solar PV plants, they gather data on irradiance levels, module temperature, inverter efficiency,

and power production" (Enlitia, 2025). This shows how SCADA systems are resourceful in the sense that they can process both archival and real-time data to monitor processes and determine if any operational adjustments are needed. Additionally, SCADA systems also play a similar role in the transportation industry. For example, a SCADA system could be used to monitor and control traffic lights based on traffic patterns. Antaira Technologies, a manufacturer of industrial-grade networking and communication equipment, explains "SCADA systems provide the remote monitoring and control capabilities necessary to regulate traffic lights in a way that facilitates a smooth and continuous flow of traffic. In the same vein, these systems can help identify any malfunctions or out-of-order signals from stoplights so that the issue can be rectified immediately before significant traffic jams or accidents occur as a result of a faulty stoplight" (Antaira, 2021). This illustrates how SCADA systems can make operational adjustments when they need to for optimal performance, and in this case, making traffic flow as optimal and smooth as possible to try to avoid traffic jams from occurring.

SCADA systems, however, are not without vulnerabilities and risks. Some vulnerabilities and risks of SCADA systems include human machine interfaces within these systems running on outdated operating systems, such as Windows 7, and weak credentials or factory-default passwords being used and shared across human machine interfaces and programmable logic computers. Additionally, these weak credentials often go unchanged and are not thought about to be updated over the course of time. An example of a SCADA system being breached because of poor credentials would be the cyberattack that affected the water treatment plant in Oldsmar, Florida, which occurred on February 5, 2021. According to the Cybersecurity & Infrastructure Security Agency, the Federal Bureau of Investigation, the Environmental Protection Agency, and the Multi-State Information Sharing and Analysis Center, they say: "On February 5, 2021,

unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility. The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system" (Cybersecurity & Infrastructure Security Agency et al., 2021). This illustrates how a combination of both poor password security and the use of an outdated operating system can leave SCADA systems vulnerable to unauthorized tampering from unknown users. Therefore, it is imperative that SCADA systems are operating on up-to-date operating systems such as Windows 11 and are using multi-factor authentication to better secure these systems to prevent unauthorized access to outside users.

The aftermath of a cyberattack on a SCADA attack can be consequential for both organizations in society as a whole. This can include heightened dangers to public health and safety, and widespread service outages. On December 23, 2015, approximately 225,000 customers in Ukraine experienced a widespread power outage as a result of a cyberattack on Ukrainian power companies. The Cybersecurity & Infrastructure Security Agency says "On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. Through interviews with impacted entities, the team learned that power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers.

While power has been restored, all the impacted Oblenergos continue to run under constrained operations" (Cybersecurity and Infrastructure Security Agency [CISA], 2016). This highlights how impactful a cyberattack can be on both organizations and people alike. In this instance, the Ukrainian power companies suffered due to the need to fix the power outage issues and society suffered because they did not have any power. And, because this occurred in late December, it is likely that the people who were impacted faced frigid early winter temperatures and lacked the means necessary to keep themselves warm without electricity.

SCADA systems have their fair share of vulnerabilities and risks, however, organizations can take actions to improve the overall security and resilience of these systems. Some actions organizations can take include separating corporate information technology networks from SCADA operational networks, and stopping lateral movement by implementing a firewall in between networks to prevent a potential breach in corporate information technology networks from easily being able to reach and manipulate physical utility controls. Medford Water in Oregon is an example of an organization that took action to improve the security and resilience of its SCADA systems, following threats to its operational technology. According to Jeff Kanyuch, the Jacobs Project Manager, and Andy Huffman, the Senior Capital & Special Projects Manager, they say "In recent years Medford Water has taken a proactive approach to our IT and OT security posture including: network isolation of both SCADA systems, and upgrading the server hardware and operating systems running the SCADA HMI graphics" (Kanyuch & Huffman, n.d.). This highlights what actions organizations can take to better secure their SCADA systems, and in doing so, improving the overall security and resilience of them.

SCADA systems play a key role in managing critical infrastructure as their purpose is to monitor and manage systems within such infrastructure. This paper serves to explain what

SCADA systems are, how they are used in industries and critical infrastructure, their risks and vulnerabilities, how a cyberattack on SCADA systems can impact organizations and society, and explain what actions organizations can take to improve security and resilience of such systems. By understanding and properly maintaining SCADA systems, organizations and society as a whole are less likely to face the consequences of a cyberattack on these systems and help to promote the proper maintenance of SCADA systems.

References

Antaira. (2021, January 1). *What is SCADA and where is it used?* https://www.antaira.com/What-Is-SCADA-and-Where-Is-It-Used

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, & Multi-State Information Sharing and Analysis Center. (2021, February 11). *Cyber actors compromise U.S. water treatment facility via remote desktop protocol*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

Cybersecurity and Infrastructure Security Agency. (2016, February 25). *Cyber-attack against Ukrainian critical infrastructure*. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Enlitia. (2025, June 3). *What is SCADA and how it works?* https://www.enlitia.com/resources-blog-post/what-is-scada-and-how-it-works

Kanyuch, J., & Huffman, A. (n.d.). *Creating a resilient and cybersecure SCADA system: Medford Water case study*[PowerPoint slides]. Pacific Northwest Section American Water Works Association. https://www.pnws-awwa.org/wp-content/uploads/2024/06/Creating-a-Resilient-and-Cybersecure-SCADA-System.pdf