Nathaniel W. Lyon

CYSE 200T

February 8, 2026

SCADA Systems and Their Role In Critical Infrastructure

SCADA (Supervisory Control and Data Acquisition) systems are a very important/integral part of our everyday infrastructure. SCADA systems monitor multiple processes at once for things such as, water treatment plants, gas pipe lines, and wind farms. It is safe to say that this system is one that we are very reliant on to keep an orderly and functioning society as most of the processes I listed are of the utmost importance for citizens of the United States. SCADA systems are integrated into these critical infrastructures to help manage their efficiency and safety but they are also a huge target for foreign adversaries. If any of these systems were compromised by a foreign adversary/malicious actor our day to day life would be greatly affected. Imagine one day the water you are drinking stops flowing, the heat in the house stops from the gas being cut off, and the water you are able to get is contaminated as the purification process has been halted.

Components of a SCADA System

SCADA systems are comprised of five major parts. The first part is what's called the apparatus where in the article it is described as being, "used by a human operator; all the processed data are presented to the operator" (SCADA Systems 1). The second major part of the SCADA system is a Supervisory system. The Supervisory System is described as "gathers all the required data about the process" (SCADA Systems 1). The third part is what's known as RTU's (Remote Terminal Units). RTU's are defined as "process censors, which help convert the sensor

signals to digital data and send the data to the supervisory stream" (SCADA Systems 1). RTU's are essentially the translator for the system to convert signals to digital data which is important in allowing humans/computers to evaluate the efficiency of the processes taking place. The fourth major part is PLC's or (Programmable Logic Controllers). PLC's are defined as "specialized industrial computers designed to control and automate various processes and machinery" (Allen-Bradley PLC and SCADA Systems 1). The final part is the Communication infrastructure which is utilized to connect the RTU's to the Supervisory system. The ultimate Goal of a SCADA system is to automate most processes in critical infrastructure so that they might become seamless and easily operated/understood by an individual.

Vulnerabilities to SCADA systems

Ever since the creation of SCADA systems to streamline management of infrastructure, threats to those systems became more prevalent and more advanced. One of the first cyber incidents to happen to a SCADA system is believed to have been the "Siberian pipeline explosion in 1982" (Alanazi 1). Another incident occurred in 1994 when, "an attacker gained unauthorized access to the Salt River project through a dial-up modem" (Alanazi 1). SCADA systems are software and hardware leading them to be attacked from multiple angles. Malicious actors could gain remote access from possible back doors in systems or they could utilize someone on site of the system to inject malicious code in hopes of harming it's normal function for personal gain or just simply to cause mayhem. Due to the nature of how much society relies on infrastructure that utilizes SCADA systems one could deduce that security via cyber/physical means is at the utmost importance.

Conclusion

Scada systems are very important in day to day life for American's as the systems they garner provide us with resources we need for a healthy functioning society/economy. Given the nature of the systems SCADA software/hardware is implemented in they need top level security measures in place. If one of these systems was to be compromised tomorrow everyone would feel the shockwave of it's effect from lack of clean water, no ability to heat a home, all the way to not being able to drive to work due to a lack of gasoline at the pumps.

Works Cited

Marketing, ARP. "The Difference between PLC and SCADA in Industrial Automation." *Automation Ready Panels*, 19 Aug. 2024, www.automationreadypanels.com/plc-systems/the-difference-between-plc-and-scada-in-industrial-automation/.

"SCADA Systems." *SCADA Systems*, www.scadasystems.net/. Accessed 8 Mar. 2026.

Alanazi, Manar, et al. "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues." *Computers & Security*, vol. 125, Feb. 2023, p. 103028, https://doi.org/10.1016/j.cose.2022.103028.