Tgen Hampsher
March 23, 2025
CYSE 200T
Professor Duvall

SCADA Security is Essential for Protecting Critical Infrastructure

BLUF: Most of the technology found in critical infrastructure can be easily exploited by cyber criminals; however, SCADA security technology is working to fix many of the vulnerabilities found in legacy systems.

Introduction

The sixteen sectors of critical infrastructure in the US have grown to cover the entire country. This infrastructure includes things such as “airports, seaports, power grids, power plants and the like” (Paul, 2020). These infrastructures supply the nation with its water, electricity, gas, food and other critical needs. With these infrastructures being so wide and complex, modern technology created industrial control systems (ICSs) to largely control the processes involved in critical infrastructure. The problem with many ICS, as with many new technologies designed for usability without security in mind, is that they are designed with various vulnerabilities that could give bad actors the opportunity to disrupt and modify parts of our critical infrastructure and cause large scale chaos (Paul, 2020).

Common Vulnerabilities in ICS

One of the most notable sources of vulnerabilities in ICS is the use of legacy systems that are outdated and not equipped with technology like firewalls to protect against basic intrusion methods such as malicious code (Paganini, 2021). These systems are left with various software and hardware technologies that are easily accessible to modify and use. Additionally, many ICS devices are connected to large corporate networks,

which leave them vulnerable to being remotely accessed by attackers who can gain access to the network (Office of the Director of National Intelligence, 2024).

Additionally, the human errors persist in that many of the credentials and passwords used to access these systems are often default or weak, making them vary easy to crack and exploit (Paul, 2020). Some professionals have also noted that many outdated ICS technology lacks proper security training on important factors such as managing configuration changes and access controls (Paganini, 2021).

The issues that exist in poorly secured ICS technology have been researched, and some statistics are alarming. For example, researchers found 449 vulnerabilities in ICS technology in 2020, with 70% of the vulnerabilities being rated as “high or critical Common Vulnerability Scoring System (CVSS) scores” (Paganini, 2021). They noted that most of these vulnerabilities could be taken advantage by criminal hackers to either remotely disrupt systems through remote code execution (RCE) and potentially trigger a DoS attack to interfere with the infrastructure processes.

How SCADA Addresses These Vulnerabilities

Supervisory Control and Data Acquisition (SCADA) security has been integrated into ICS technology and is becoming more enhanced to defend against many common cyber attacks through various methods (Virkkula, 2025). For example, SCADA systems connect ICS technology to the internet; however, ICS technology managers have now started segmenting the internetwork of IoT devices, implementing security methods like firewalls and stricter access controls in between these technologies to prevent hackers from breaching the network (Virkkula, 2025).

Additionally, SCADA security can disable and remove devices not being used from the network and make changes as necessary to credentials in the system, to prevent hackers from getting into the network through default passwords (Virkkula, 2025). SCADA also allowed continuous updates and patches to be installed on the technology to ensure it maintains proper security controls.

Even further, SCADA systems can use TLS or SSL protocols when transmitting data from the ICS technology to remote locations, which ensures that the data not only cannot easily be viewed by hackers, but even if they do so the data will be encrypted, therefore both confidentiality and integrity are protected (Virkkula, 2025). Lastly, SCADA allows for continuous monitoring of systems to quickly detect attempts at intrusion of the network, which then allows for countermeasure to quickly start against the attack (Virkkula, 2025).

Conclusion

Our critical infrastructure is essential in ensuring that our daily needs for water, electricity, gas, and many others are available to us every day. Many of the ICS technologies created to control these processes over previous decades were not designed with security in mind. Therefore, the 21st century showed the world that greater security was needed urgently to protect our infrastructure from cyber-attacks. With the development of SCADA systems that connect these technologies to the internet, enhanced security features within SCADA are working to prevent many of the common cyber attacks on ICS technology. As

SCADA security becomes more enhanced, we should continue to see our critical infrastructure be more protected from future attacks.

References

Office of the Director of National Intelligence. (2024). *Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems*. https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

Paganini, P. (2021, March 23). *Understanding ICS/SCADA Threats: Protecting Critical Infrastructure | Infosec*. Www.infosecinstitute.com. https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-threats-and-threat-actors/

Paul. (2020, December 6). *Using SCADA to Protect Critical Infrastructure and Systems | cyberpaul*. Odu.edu. https://sites.wp.odu.edu/cyberpaul/2020/12/06/using-scada-to-protect-critical-infrastructure-and-systems/

Virkkula, J. (2025, January 15). *SCADA Security Essentials: Your Need-to-Know Guide*. Ssh.com; SSH Communications Security. https://www.ssh.com/academy/operational-technology/scada-security-essentials-need-to-know-guide