SCADA Systems

Kevin A. Loarca

Old Dominion University

CYSE 200T: Cybersecurity, Technology & Society

Professor Christopher Bowman

June 21, 2026

SCADA Systems

There are vulnerabilities associated with critical infrastructure systems. One of these vulnerabilities is the need for accuracy. The data that is created within these infrastructure systems needs to be carefully examined and documented in case intervention is required. There is a system that can mitigate this type of risk. Supervisory Control and Data Acquisition (SCADA) is used to control infrastructure processes, facility-based processes, or industrial processes ("SCADA Systems," n.d.). The SCADA systems are used for monitoring and controlling physical processes such as the distribution of water, traffic lights, electricity transmission, etc. ("SCADA Systems," n.d.). SCADA systems are important, especially within critical infrastructure systems, as they allow for monitoring and control processes. These systems can also issue warnings when conditions become dangerous ("What is SCADA and SCADA system?," n.d.). This type of technology addresses the accuracy risk as it gathers data, records and logs it, and presents information through Human Machine Interfaces ("What is SCADA and SCADA system?," n.d.).

Vulnerabilities and Solutions of SCADA Systems

The use of a SCADA system is arguably important for this type of environment. However, this type of technology does come with potential vulnerabilities that would affect critical infrastructures. Across industries and vendors, SCADA systems show similar weaknesses constantly. Some reported weaknesses include: legacy protocols and unencrypted traffic, default credentials, poorly segmented networks, etc. ("What is SCADA security? A practical guide for critical infrastructure," 2025). The use of legacy protocols does not provide updated security measures, which may not be capable of encrypting data during transmission. Default credentials are an issue as attackers could guess the login information. Lastly, non-segmented networks

could allow the attacker to move easily and gain higher access to information. These issues could be resolved if security measures were implemented. For securing data during transmission, legacy protocols need to be inside secure tunnels to authenticate endpoints ("What is SCADA security? A practical guide for critical infrastructure," 2025). Having a password policy could help avoid the use of default credentials, as it can provide users with the requirements needed. Then, for segmented networks, a zero-trust architecture would encourage segmented networks, as each user accessing another network would need to be verified.

Conclusion

In conclusion, there are vulnerabilities present within critical infrastructures, including the need for accuracy. The system that is reliable for this type of environment would be SCADA systems, as they are able to monitor, collect information, and issue warnings. However, the technology can present itself with vulnerabilities that could affect critical infrastructures from being breached or tampered with. There are commonly reported vulnerabilities such as legacy protocols, using default credentials, poorly segmented networks, and so on. There are solutions available that address these vulnerabilities, which users of SCADA systems need to be aware of.

References

SCADA Systems. (n.d.). Perusall. https://app.perusall.com/courses/202530_cyse200t_33004-cybersecurity-technol-society/scada-systems?assignmentId=AhyXcdQb6Twdb7ZrB&part=1&filter=all

What is SCADA and SCADA system? (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems

What is SCADA security? A practical guide for critical infrastructure. (2025, June 19). Zero Trust Security for Critical Asset Defense & Enterprise Resilience. https://www.zentera.net/cybersecurity/scada-security