Securing Critical Infrastructure: SCADA Solutions

Nathan A Park

Old Dominion University

Course Number: CYSE200 - 17364

Professor Charles E. Kirkpatrick

Due Date: 11/5/23

Table of Contents

Securing Critical Infrastructure: SCADA Solutions

Critical infrastructure cyber defense needs SCADA (Supervisory Control and Data Acquisition) systems with modern security principles and practices in place to protect against emerging threats ranging from state-sponsored agencies, terrorism, espionage, to opportunistic vandalism.

Vulnerabilities

Modern society depends on infrastructure for transportation, power, health care, information, sanitation, defense, and more. The assets and systems supporting these endeavors are vital to a nation-state's security (economic and sovereign), health, and safety (Technology, 2018). The surface area of these combined systems is therefore a tempting target for a multitude of threat actors with examples including sabotage of Iran's nuclear enrichment program, infiltration of a hydroelectric power station, and steel mill production failures (Telecom, 2021).

Like many networked technologies, SCADA systems were not originally designed with cybersecurity as a primary concern. Instead, the types of hardware used to support SCADA systems are engineered with extreme reliability and repeatability as the primary objective. As such, the programming languages and CPUs are often incapable of incorporating security enhancements like encryption and robust authentication due to design constraints (Hadar, 2023). This creates modernization challenges because large capital investments are made over the course of decades and include static legacy hardware with these vulnerabilities. Finally, the specialized communities and proprietary vendors in the SCADA industry make up a small community relative to the wider IT field; the market share for SCADA systems is $10 billion while the computer market is $449 billion (Company, 2023); (Markets, 2022). Consequently, there is a less transparent understanding of the underlying technology and a greater likelihood that vulnerabilities remain undiscovered or unpatched.

Threats

The types of threats that can exploit SCADA systems are especially concerning because of their real-world impacts. Data breaches of personal and business information are important, but a SCADA system compromise has the potential to directly affect human life. SCADA systems are frequently employed in industrial systems that control parameters affecting life-safety systems. For example, many systems work with hazardous temperatures, pressures, electrical currents, and moving equipment with high capacities for potential and kinetic energy. Compromising a system could result in exceeding normal operating parameters which means violating pressure boundaries, electrical power excursions, and other critical limits that can result in equipment damage, personnel injury, or even death. This extends beyond the facility to the consumers as well. For example, an attack that causes a loss of power or fuel to medical and emergency responders can seriously affect large metropolitan areas. The MITRE corporation's CVE database demonstrates the potential for these kinds of attacks as there are currently 1025 SCADA software CVEs and 200 PLC CVEs including multiple possibilities for remote code execution and data integrity violations (Corporation, 2023).

A significant number of threats originate at the geopolitical level from nation-states to terrorist organizations. Current events from 2023 alone demonstrate how useful cyberwar tactics are with targets ranging from rail and military logistical hubs to communications nodes in Ukraine, Russia, Israel, and beyond (Studies, 2023). Clearly, countries realize that significant strategic and tactical advantages can be gained by attacking critical infrastructure and the distributed nature of infrastructure provides a massive surface of attack for threat actors.

SCADA's Role in Securing Infrastructure

SCADA systems provide necessary utilities to operations personnel to control and monitor processes and have potential to provide additional security to protect critical infrastructure. First, SCADA systems can be modernized to incorporate lessons learned from other networks including shifting to secure communications protocols (Stouffer, et al., 2023). Second, network architecture can use principles to separate systems at multiple levels with well-defined interfaces. For example, the manufacturing SCADA network should not have hosts directly connected with software development packages that could modify installed code on PLCs. Next, components such as data diodes that ensure one-way communication can be employed to prevent communication from lower to higher posture systems while still transporting useful data to business intelligence systems. Additionally, intrusion detection systems specialized for IoT monitoring can be installed to provide early warning for possible incursions.

The previously mentioned improvements can help harden critical infrastructure networks. However, there are several principles that can be borrowed from mature industries with a keen awareness of the susceptibility of computer systems. Safety systems may be deemed so critical that they should be independently hardwired into the process to ensure failsafe configurations in worst-case scenarios (Stouffer, et al., 2023). For example, safety relief valves with rugged yet simple pressure detectors and logic circuits will actuate to relieve pressure in a vessel regardless of the state of more complex process control systems. Another common use is emergency stop buttons that remove power to a system like a conveyor belt providing a last resort human intervention. This additional layer of risk mitigation is designed to account for the possibility of simultaneous operator and control system failure.

Conclusion

Critical infrastructure is vulnerable to many threats which have the potential to seriously damage health and public safety. We rely on these high-value investments and need mature modern cybersecurity improvements based on proven frameworks, technology, and lessons learned to effectively mitigate risks. SCADA systems can be engineered using these principles to create defense-in-depth architecture ranging from separated networks, clearly defined data flows, redundant systems, and monitoring systems to improve service continuity in the face of more frequent attacks. Geopolitical conflicts and resurging national rivalries guarantee that critical infrastructure will be a central dimension in the future of cyber-warfare.

References

Company, T. B. (2023, January). *Computers Global market Report*. Retrieved from The Business Research Company: https://www.thebusinessresearchcompany.com/report/computers-global-market-report

Corporation, M. (2023, October 2). *CVE*. Retrieved from cve.mitre.org: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SCADA

Hadar, L. (2023, March 13). *Critical Infrastructure's Silent Threat: Part 1 - The Invisible Enemy*. Retrieved from scadafence.com: https://blog.scadafence.com/plcs-at-risk-part-1

Markets, M. a. (2022, November). *SCADA Market by Offering, Component, End User, and Region - Global Forecast to 2027*. Retrieved from Scada Market: https://www.marketsandmarkets.com/Market-Reports/scada-market-19487518.html

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pilliterri, V., Lightman, S., . . . Thompson, M. (2023). *Guide to Operational Technology Security NIST Special Publication 800-82r3.* Gaithersburg, MD: National Institute of Standards and Technology.

Studies, C. f. (2023, September). *Significant Cybersecurity Incidents*. Retrieved from csis.org: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Technology, N. I. (2018). Framework for Improving Critical Infrastructure Cybersecurity V1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Telecom, D. (2021, December 23). *14 Major SCADA Attacks and What You Can Learn From Them*. Retrieved from DPS Telecom: https://www.dpstele.com/blog/major-scada-hacks.php