SCADA Systems

Aaron Jones

CYSE 200T

Professor Kirkpatrick

10/30/2023

SCADA Systems

SCADA systems oversee and regulate vital infrastructure systems, such as power plants, water treatment facilities, and transportation networks (SCADA Systems, 2018, p. 1). These systems frequently exhibit complexity and interconnectivity, rendering them susceptible to cyber-attacks that can interrupt service or inflict physical harm.

The vulnerabilities associated with critical infrastructure systems.

A SCADA system is a technology utilized for monitoring and controlling vital infrastructure, including water and wastewater systems (Alanazi et al., 2022, p. 3). Critical infrastructure systems refer to the assets, techniques, and networks that are crucial to the United States. Their incapacitation or destruction might extensively affect security, national monetary security, country-wide public fitness, or protection. Those systems are especially prone to cyberattacks due to their reliance on outdated hardware that lacks state-of-the-art protection capabilities.

Internet connectivity has led to a developing interdependence amongst infrastructure systems, rendering them susceptible to cyber threats. Adversaries can exploit the most vulnerabilities, rent malicious software programs, or provoke distributed denial-of-service (DDoS) attacks to disrupt or seize control of these systems. Furthermore, some critical infrastructure systems utilize antiquated hardware but depend on computer programming languages currently regarded as old-fashioned, such as C and Pascal. Due to these two issues, critical infrastructure systems frequently fail to sufficiently safeguard themselves against hackers who want to infiltrate their networks and influence them through remote access.

The electricity grid is susceptible to its intricate computer networks that employ standard technology across several corporations. Furthermore, the grid encompasses essential systems that directly influence the well-being of individuals. Consequently, it becomes an appealing objective for malevolent assailants.

The role SCADA applications play in mitigating these risks.

According to Alanazi et al. (2022, p. 3), SCADA is a system that uses a central computer to store data about local or distant devices to manage industrial operations and facilities. SCADA systems need to be effectively protected using contemporary best practices to reduce this danger. Legal mandates are present at the state level in the United States and several other nations globally. However, implementing and enforcing these regulations may only sometimes be consistently carried out in reality (SCADA Systems, 2018, p. 4). Furthermore, due to their preexistence before the emergence of cloud computing, SCADA systems often need help to fully use the benefits provided by cloud computing, such as automatic upgrades, identity management solutions, and security monitoring tools.

Companies must allocate resources toward implementing SCADA applications that incorporate cutting-edge cybersecurity protocols and leverage automation technologies to mitigate the risk of human mistakes (SCADA systems, 2018, p. 6). SCADA systems offer instantaneous data organizations may use to safeguard their tangible assets and control system networks. SCADA systems effectively limit the dangers associated with these assaults by actively monitoring and managing the transmission of data in real-time inside a critical infrastructure system.

SCADA applications use redundant systems and employ secure communication channels to facilitate the exchange of information between remote sites, similar to other effective security systems (Alanazi et al., 2022, p. 8). Furthermore, these systems need robust authentication protocols to ensure only authorized users are granted access. Consequently, any modifications made from a remote location must undergo authentication by an administrator before being executed.

In conclusion, despite SCADA systems being crucial in risk reduction it is essential to acknowledge that they are not infallible. A comprehensive strategy for cybersecurity is necessary to maintain the resilience and security of critical infrastructure systems. This approach entails frequent risk assessments, penetration testing, and coordination with government authorities.

References

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 103028.

SCADA systems. (2018, July 25). SCADA Systems. http://www.scadasystems.net