Name: Jestina Hill

Date: 11/2/2024

Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition denotes industrial control systems employed to manage infrastructural, facility-based, or industrial activities. Examples of these processes include water treatment, gas pipelines, airports, space stations, manufacturing, and power generation (SCADA Systems, n.d.). Almost all control actions are executed automatically by remote terminal units (RTUs) or programmable logic controllers (PLCs) (SCADA Systems, n.d.). SCADA systems primarily utilize distributed databases referred to as tag databases, which encompass data items known as points or tags (SCADA Systems, n.d.).

Vulnerabilities Associated with Infrastructure Systems

The infrastructure systems are of utmost importance due to the numerous challenges they must withstand. Due to the variability of vulnerabilities stemming from complex digital interconnections and networks. The databases of the SCADA system are utilized to deliver diagnostic data, management information, and trending information; however, they are now aligned with standard networking technology. The diverse responsibilities increase the likelihood of various cyberattacks, unauthorized access, and other threats. Several vulnerabilities include outdated networks, weak passwords, and the use of default credentials, as these are frequently associated with corporate IT networks (Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, 2024). Some of these systems utilize outdated networks, which may lack updated security features (Recent Cyber Attacks on US Infrastructure

Underscore Vulnerability of Critical US Systems, 2024). The use of weak passwords can lead to unauthorized access to SCADA systems, potentially resulting in an attack (Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, 2024). Additionally, the presence of default credentials provides an easy pathway for unwanted access (Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, 2024).

The Role of SCADA Applications in Risk Mitigation

The SCADA system serves as a security measure to protect vital infrastructure from assaults and threats. Implementing essential protocols to regulate, monitor, and protect processes will furnish information regarding hazards to lessen risks posed to SCADA systems (Admin, 2022). The system has policies that generate alarms and alerts to notify users about processes, enabling the force to halt or modify procedures as necessary. Documenting reports on automated machinery and industrial processes, while gathering data, enables the SCADA system to monitor their operations (Admin, 2022). Finally, data gathering, and display facilitate the aggregation of data from various sensors throughout an industrial floor (Admin, 2022). Data analysis and interpretation facilitate real-time comprehension of circumstances inside the machinery and industrial environment (Admin, 2022).

Conclusion

Critical infrastructure monitoring, control, and security are just a few of the many duties that SCADA systems have. Additionally, they must be updated and have procedures in place to guard against threats and intrusions. As they fluctuate attacks to make sure there aren't many vital infrastructures, SCADA security gets stronger. It describes the complicated systems dispersed over wide areas or the centralized systems that manage and keep an eye on the entire

site. Programmable logic controllers or remote terminal units carry out control actions automatically.

References

Admin. (2022, September 28). Complete Guide to SCADA Security [2022 Updated] | Sectrio. Sectrio. https://sectrio.com/blog/complete-guide-to-scada-security/#:~:text=Breakdown%20of%20the%20SCADA%20Security%20Framework%3A%201%201.,Monitoring%20Controls%3A%20. . .%206%206.%20Peripheral%20Controls%3A%20

Krehel, O. (2021, September 21). Threat Vulnerabilities and Prevention in Critical Infrastructure. Security Info Watch. Retrieved November 1, 2024, from https://www.securityinfowatch.com/critical-infrastructure/article/21233430/threat-vulnerabilities-and-prevention-in-critical-infrastructure

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems. (2024, April 22). Office of the Director of National Intelligence. Retrieved November 1, 2024, from https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf#:~:text=Outdated%20software%2C%20poor%20password%20security%2C%20the%20use%20of,corporate%20IT%20networks%20and%20increasingly%20to%20the%20Internet.

SCADA Systems. (n.d.). Google Docs. Retrieved November 1, 2024, from https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0