The Importance of SCADA Systems and Mitigating Risks

Camillia Epps

Charles E. Kirkpatrick

CYSE-200

17 March 2024

BLUFF

SCADA systems are very crucial when it comes to looking over infrastructure and they do not go without risks. If software is not up to date, then that is when the vulnerability happens, and cyber-attacks can take place. It is crucial to make sure that measures are taken to look out for and defend again all threats. If we know the issue, we can ensure that the systems are safe from any possible dangers. This paper explores the significance of SCADA systems, highlights the associated risks, and discusses strategies for risk mitigation.

What is SCADA?

SCADA stands for Supervisory Control and Data Acquisition, a system crucial for overseeing various industrial processes by utilizing computer-based data communications and interfaces to provide real-time supervision. SCADA systems are indispensable for ensuring the safety and integrity of operations across different sectors (Gupta, 2015). It is a system that is set up to utilize computers data communications and interfaces that provide real time supervision. We need SCADA because it makes sure that things are safe across different sectors.

Insights FORTINET

Fortinet is a cybersecurity company that provides network security and solutions to business and government all over the world. The company includes firewalls, intrusion prevention systems, and secure access solutions. This company stops things from happening like ransomware, data breaches and making sure the security of our digital assets are safe. The reason I chose to speak on this company y is that they offer solutions that are applicable to SCADA. What they offer can be used in the SCADA environment. According to Fortinet, SCADA (Supervisory Control and Data Acquisition) systems are "control system architectures that use computers, networked data communications, and graphical user interfaces for high-level process supervisory management." These systems are integral to critical infrastructure sectors like energy, water, and transportation (Fortinet).

Mitigating the Risks

Mitigating risk with the SCADA involves heavy monitoring, making sure there is strict access control to prevent unauthorized users. Make sure to do regular updates to make sure that any known vulnerabilities are fixed. Also, when it comes to training and awareness, the operators need to know the best practices that make sure they have the correct response to security threats. With another resource that I chose to read about, Computers & Security, A review of cyber security risk assessment methods for SCADA systems. With mitigating risks, it talks about different risk assessments that were done over the years. Naming one of them and explaining them, SCADA risk assessment method based on grey relational analysis, 2014 (Chen et al., 2014): It utilizes grey relational analysis for risk assessment in SCADA systems.

Conclusion

In conclusion, SCADA systems are very important for making sure essential infrastructure is managed. They need to monitor and control it across the world. Knowing that since it must be across the world it opens them up to risk that includes data breaches, and system disruptions. Mitigating these risks is important to making sure the integrity stays intact and making sure that there is safety throughout the world.

References

Chen, Y., Liao, W., & Chao, H. (2014). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 45, 44-57. https://doi.org/10.1016/j.cose.2014.05.007

Fortinet. (2024). *What is SCADA and SCADA system?* https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems

SCADA systems. (n.d.). Google Docs. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit#heading=h.ckgmz4vfex94

Yulia Cherdantseva Pete Burnap Andrew Blyth Peter Eden Kevin Jones Hugh Soulsby Kristan Stoddart. (2016, February). *A review of cyber security risk assessment methods for SCADA systems*. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0167404815001388