Tyler Henson
11/9/2025

SCADA Systems

Critical infrastructure has many vulnerabilities which include outdated software and hardware, remote access exposure, or insider threats. However, SCADA systems help mitigate these vulnerabilities by doing real time monitoring, remote control and automation, and data logging and analysis

Introduction

SCADA systems are systems which use hardware and software to monitor and control industrial processes from a central location. They gather real-time data from sensors, analyze it, and allow workers to send commands to machinery to manage critical infrastructure operations efficiently and safely.

Critical Infrastructure Vulnerabilities

Critical infrastructure is a term for the assets, systems, and networks that are so vital to a nation that their disruption or destruction would have a massive impact on the country. Examples of critical infrastructure include energy grids, roads, airports, communication systems, water supply, and healthcare. Critical infrastructure provides functions that are necessary for daily life as well as for a nation’s economy. These systems are incredibly complex and interconnected with each other meaning that a change in one area could have lasting effects on the others.

Critical infrastructure has a lot of vulnerabilities that need to be monitored and taken care of in order to stay in good condition. Examples of some of these vulnerabilities include the software or hardware systems being outdated or worn out from use, unauthorized access and remote exploitation, weak authentication systems, and insider threats. All of these vulnerabilities could lead to the damage or destruction of one of the areas of critical infrastructure which could severely damage the economy in one part of a nation if not the entire area. Thus, these vulnerabilities must be heavily monitored and kept up with in order to manage the risks.

SCADA Systems Role

Scada systems play an extremely critical role in mitigating the risks and vulnerabilities of critical infrastructure. SCADA is an acronym which stands for supervisory control and data acquisition. In other words, SCADA systems are used to monitor and collect data as well as control operations and provide support when making decisions. The goal of SCADA systems is to simplify the control and automation of large-scale and complex industrial processes.

The main four ways SCADA systems mitigate the vulnerabilities of critical infrastructure is by using real-time monitoring, remote control and automation, data logging and analysis, and integration with cybersecurity tools. SCADA systems continuously track system performance and alert operators when they detect anomalies in a system. Also, SCADA systems allow centralized control of distributed assets which reduces the need for on-site personnel and enables faster response times for incidents. In addition, SCADA systems collect historical data that can be used for

forensic analysis after an incident or to identify patterns that suggest vulnerabilities. Lastly, SCADA systems can be paired with firewalls, intrusion detection systems, and other networks to enhance the protection of critical infrastructure.

Conclusion

In conclusion, SCADA systems are used to mitigate the risks and vulnerabilities associated with critical infrastructure by using data collection and monitoring to assess incidents and provide support and automation to make better decisions faster.

“References”

SCADA Systems: What They Are & How They Work | Splunk. (2024). Splunk. https://www.splunk.com/en_us/blog/learn/scada-systems.html

Tariq, E. (2025, June 23). *Top 10 Cybersecurity Risks Threatening Critical Infrastructure Today | Certrec*. Certrec | Regulatory & Technology Solutions for the Energy Industry. https://www.certrec.com/blog/top-10-cybersecurity-risks-threatening-critical-infrastructure-today/

Using SCADA to Protect Critical Infrastructure and Systems | cyberpaul. (2020, December 6). Odu.edu. https://sites.wp.odu.edu/cyberpaul/2020/12/06/using-scada-to-protect-critical-infrastructure-and-systems/