Name: Treyvien Kirk

Date: 11-1-2022

SCADA Systems

The article gave a descriptive overview about SCADA systems and their role in industrial organizations. Furthermore, the article describes the different components that make up the SCADA systems and how they've evolved over time. SCADA systems help to maintain and process data throughout critical infrastructures.

What are SCADA systems?

Supervisory control and data acquisition (SCADA) systems are software and hardware elements within industrial organizations that maintain efficiency, process data, and communicate issues to mitigate risk (Inductive Automation, 2018). SCADA systems incorporate subsystems which include a supervisory system to gather data, remote terminal units (RTU), programmable logic controllers (PLC), and a communication infrastructure (SCADA Systems, n.d.). Additionally, SCADA systems allow for direct interaction with devices through the human machine interface (HMI) software. SCADA systems are used in a variety of industrial fields such as energy, oil, water, food, and manufacturing to list a few.

Vulnerabilities in critical infrastructure

According to compuquip, the main attack vectors that critical infrastructures are at risk of are network vulnerabilities, operating system vulnerabilities, processing vulnerabilities, and human vulnerabilities (Dosal, 2020). Network vulnerabilities include poor firewalls or issues that expose the hardware or software to third party intrusion while operating system vulnerabilities include potentially hidden backdoor programs. Furthermore, processing vulnerabilities include

lacking processing controls due to things like a poor password while human vulnerabilities can expose sensitive data, create openings for exploitation, or disrupt data.

The role of SCADA systems

SCADA systems play the role of controlling and monitoring industrial processes along with reacting appropriately to different attack vectors. For instance, the RTUs and PLCs have the job of controlling and monitoring any process needed while also communicating the data to the HMI. The HMI is an apparatus for human operators to adjust the controllers based on the processed data. The SCADA systems may also respond to threats through an alarm system to alert human operators to intervene (SCADA Systems, n.d.). Generally, the alarm system may activate when there is an anomaly in the processed data.

The risk of SCADA systems

In today's generation, SCADA systems are open to network attacks due to communication being through WAN protocols. Although there are many advancements to these security protocols, SCADA systems are more vulnerable to internet attacks than ever before. Additionally, SCADA systems are heavily relied upon, so if any failure in the system were to occur, then it could cost the company money or even be the cause of a death (SCADA Systems, n.d.). There are many other possible attack vectors to SCADA systems but many improvements to reduce them are being made. For instance, industrial VPNs and firewalls are being implemented into systems to further reduce the risk of a network attack.

Conclusion

To summarize, SCADA systems are systems within industrial organizations to maintain efficiency, process data, and communicate issues to reduce risks. They are heavily built on

hardware and software technology such as RTUs, PLCs, and HMI. SCADA systems have become a critical part in maintaining critical infrastructure as without them money, lives, and daily operations can suffer.

References

Dosal, E. (2020, March 10). *Top 5 Computer Security Vulnerabilites - Compuquip*. Retrieved November 1, 2022, from Compuquip: https://www.compuquip.com/blog/computer-security-vulnerabilities

Inductive Automation. (2018, September 12). *What is SCADA?* Retrieved November 1, 2022, from Inductive Automation: https://inductiveautomation.com/resources/article/what-is-scada

SCADA Systems. (n.d.). *SCADA Systems*. Retrieved November 1, 2022, from http://www.scadasystems.net/