~ SCADA Write up assignment ~

Task: <u>Explain the vulnerabilities associated with critical infrastructure systems, and the role SCADA applications play in mitigating these risks.</u>

      To explain the vulnerabilities associated with critical infrastructure systems, it is important to know what exactly critical infrastructure systems are.

      Critical infrastructure systems are the systems, facilities and assets that are fundamental to the functioning of society as well as the economy (IBM, 2023). Examples of such systems include energy and power systems, water and wastewater systems, airports, production, etc. Managing these systems is crucial because they are vital in preserving public safety, security on local, state and national levels, and the overall wellbeing of all citizens. To deal with critical infrastructure systems efficiently, a variety of software solutions and systems such as asset management, SCADA control systems, network monitoring and security, and so on need to be imposed (IBM, 2023). These solutions and systems manage critical infrastructure systems by keeping track of all assets, monitor or control processes, and detect as well as respond to potential threats.

      Now while critical infrastructure systems may have a lot of solutions and systems in place to ensure its success, there are still some limitations or vulnerabilities associated with these systems. These limitations and or vulnerabilities include outdated or weak systems, inadequate maintenance, lack of safeguards against extreme weather conditions, and so on (Noya, 2024). Such weaknesses if and when not handled properly can lead to severe failures within the infrastructure systems. But even though these systems have many limitations and the effect of these vulnerabilities can cause catastrophic failures, there are other applications out there such as SCADA applications to assist in mitigating these risks.

      SCADA which stands for *Supervisory Control and Data Acquisition* systems are computer based applications that allow organizations to control and monitor industrial processes (Inductive Automation, 2018). These applications are crucial because with SCADA, organizations can monitor and control their industrial processes in real time, catch the early detection of issues, manage resources efficiently, have more robotic control of processes rather than manual labor, and so on (IEEE Public Safety Technology, n.d.). These applications could be

useful for industrial processes, specifically industrial control systems because of the varying risks associated with them. SCADA applications would be very efficient with industrial control systems because they minimize risks and support the continuation of operations regardless of what challenges may arise. Specifically, SCADA mitigates the vulnerabilities within critical infrastructure systems (outdated or weak systems, inadequate maintenance, lack of safeguards against extreme weather conditions) by providing real time data and monitoring, promoting preventative maintenance, and providing automated solutions for system vulnerabilities and external hazards like extreme weather.

Sources:

IBM. (2023, July 5). *Critical Infrastructure*. Ibm.com.

https://www.ibm.com/think/topics/critical-infrastructure

Noya. (2024, June 24). *How Critical Infrastructure Vulnerabilities Stall Businesses*. EIS.

https://eiscouncil.org/how-critical-infrastructure-vulnerabilities-stall-businesses/

Inductive Automation. (2018, September 12). *What is SCADA?* Inductive Automation.

https://inductiveautomation.com/resources/article/what-is-scada

IEEE Public Safety Technology. (n.d.). *Cybersecurity of Critical Infrastructure with ICS/SCADA*

Systems - IEEE Public Safety Technology Initiative. Publicsafety.ieee.org.

https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-

systems