Deandre Turner

Old Dominion University

CYSE 200T

Professor Chris Bowman

SCADA Systems and the Security of Critical Infrastructure

BLUF

Modern infrastructures are always at a risk of cyber attacks and intrusion. The SCADA system helps protect and prevents these incidents from occurring. This is done by using real-time surveillance, data encryptions, and predictive software.

Infrastructures and their vulnerabilities

In many countries across the world, their infrastructure utilizes certain systems to help regulate them. For example, the power grid is one of the most important aspects of this, as it allows for electricity to power the city. However, these systems are prone to vulnerability and could be sabotaged depending on the situation. If there is a cyberattack and they manage to take out the power grid, this could lead to chaos within the country itself. Other systems such as pipelines and important network servers could be hacked and manipulated for damage or failure. It is vital that we maintain a form of protection and security for our systems and infrastructure (Spiceworks, 2024).

What exactly is the SCADA?

The Supervisory Control and Data Acquisition (SCADA) system helps regulate proper system integrity and security. Most of the time, they use RTUs (Remote Terminal Units), sensors such as PLCs (Programmable Logic Controllers), and HMIs (Human Machine Interfaces) to give information and data to operators (SCADA Systems PDF, p. 1). If the equipment is out of specifications, SCADA will usually send an alarm notifying the operator. The best thing about these systems is that they operate in real-time and are 24-hour based. This is done to help alleviate intrusion and sabotaging acts (Inductive Automation, 2024).

How do they work and how have they advanced?

Many may believe that older systems are immune because of their isolation from network servers. However, they are still susceptible to intrusion and cyberattacks. All it takes is for a hacker to upload malware to a server or network and shut down the equipment. Thus, most SCADA systems must maintain a constantly up-to-date system to regulate security protocols. SCADA systems in the modern day often have password credentials, certain accessibility restrictions, data encryption, and even network blockers. According to Inductive Automation (2024), current SCADA models have advanced systems that can create data logs, run diagnostics, and even assist operators in predicting and preventing attacks before they occur.

Conclusion

To conclude, in the current digital age, it is vital that critical infrastructure systems are protected. Their vulnerabilities need to be alleviated and prevented from future exploitations. SCADA systems are the most important aspect in reducing these risks. By constantly monitoring infrastructures, having fast alarm notifications, and advanced cybersecurity, SCADA systems protect important systems and ensure public safety.

Reference:

1. Inductive Automation. (2024). What is SCADA? https://inductiveautomation.com/resources/article/what-is-scada

2. SCADA Systems. (n.d.). SCADA systems. Retrieved from http://www.scadasystems.net

3. Spiceworks. (2024). What is SCADA? Spiceworks. https://www.spiceworks.com/tech/tech-general/articles/what-is-supervisory-control-and-data-acquisition-scada/