Myles Damoah
CYSE 200T
SCADA Systems write-up
27 October, 2024

SCADA Systems

Vulnerabilities of Critical Infrastructure and the role SCADA systems play in it.

Introduction

Supervisory Control and Data Acquisition (SCADA) main purpose is to monitor the system for critical infrastructure. Infrastructure processes like manufacturing, water treatment, transportation, renewable energy, oil and gas, and power distribution and control all rely on SCADA to make sure that the management of these processes are reliable and responding accurately to its intended purpose.

The main role of SCADA is to collect data on the process and send it to a human operator who can then make a real time decision on the current rate of the process. This gives companies autonomy in their manufacturing processes, as SCADA does not control the process but manages it by sending information to the system which organizes the production. This enhances efficiency, and mitigates errors in the industrial process.

The Concept of SCADA

SCADA consists of three components Programmable Logic Controllers (PLC's) or Remote Terminal Units (RTU), and Human Machine Interfaces (HMI). The PLC's or RTU's collect data from industrial equipment and relay that information to the HMI. The human operator can then use the interface to input manual and send automatic controls to the PLC/RTU which then sends commands to the equipment. This process is how SCADA functions; it provides the system with managerial information so that human operators can manage the equipment properly and react to any alarms or errors, without having to bypass automated machinery to fix issues.

Importance of SCADA

The goal of SCADA is to optimize the supervision of production. Having a system in place that can monitor the functionality of equipment 24/7, without having to have personnel on the floor, continuously watching the process promotes efficiency and reduces cost for companies. Which is why the cost of a failure in SCADA could not only be detrimental to a company's finances, but it could cost the lives of the workers. Fortunately SCADA is physically built to withstand high temperatures and voltage, and communication channels like standard protocols of IEC 61850, DNP3, and IEC 60870-5-101 or 104. Redundant hardware so that failings in the system can be identified and relaid in quick time to resolve issues. A well maintained SCADA system can run for up to 10-20 years.

Vulnerabilities of SCADA

As SCADA is used to maintain critical infrastructure, this means that it is a high value target for cyber attacks/ cyber warfare. And while SCADA systems may have strong physical protection. This does not protect the system from the cyber world. In February of 2021 a U.S water treatment facility plant was infiltrated and cybercriminals used the SCADA system to contaminate the water. In a report published by the "Cybersecurity & Infrastructure Security Agency" " *The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system."* The FBI was not able to confirm a cyber intrusion. By using an alleged desktop sharing software which was meant to be used for telework and file sharing.

Cybercriminals can inject malicious code into the system that can rewrite its intended purpose of supervising and trick the system into thinking the HMI is sending a direct command to release chemicals into the water without raising the alarm for such a high volume of lye in the water. This raises the question of the lack of security around what software is able to access such integral parts of the system without proper authorization. Packet control remains lackluster in SCADA systems such attacks like OS Injection or SQL Injection could go unnoticed. SCADA systems are designed to merely receive and follow the commands it's given and not verify if the sender is authenticated to give such commands. This can lead to a critical failure or downtime of

important infrastructure in our everyday lives.

Conclusion

SCADA systems have revolutionized the Infrastructure sector by providing efficient and reliable updates and supervising the manufacturing process. But with the lack of oversight of the security of its software. It raises the question of whether or not we are waiting for a massive strike on our critical infrastructure to finally protect the system that impacts millions of lives everyday. It's time for a review and update on security protocols and implement 2 factor security protocols and policies built around the CIA triad to reinforce the strength of SCADA system security.

Works Cited

International, S. (2024, October 23). Learn all about SCADA systems: What is SCADA?: Scadapedia. SCADA International. https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for,data%20from%20the%20industrial%20equipment.

SCADA SYSTEMS. (2024, January 1). *SCADA systems*. SCADA Systems. https://www.scadasystems.net/

Alanazi, M., Mahmood, A., & Chowdhury, M. (2022, November 25). *SCADA vulnerabilities and attacks: A review of the state‐of‐the‐art and open issues*. Computers & Security. https://www.sciencedirect.com/science/article/pii/S0167404822004205#sec0026

Compromise of U.S. water treatment facility: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2021, February 11). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a