

Zachary Six

March 23, 2024

CYSE 200T

Professor Kirkpatrick

Using SCADA Systems to Mitigate Critical Infrastructure Vulnerabilities

In this brief report, I will discuss the operation of SCADA systems and vulnerabilities of critical infrastructure. I will then discuss the relation of SCADA systems in mitigating those vulnerabilities.

SCADA Systems

SCADA refers to the systems to control industrial tasks on Industrial Control Systems (ICS) such as water treatment, airports, gas pipelines, etc. (scada.net) These systems take information from the tasks such as the speed of a fluid within a pump and display this information in a manner that allows the operator to control and monitor the tasks. Alarms are also implemented in the event a piece of equipment malfunctions or performs the task outside of the regular operating window.

Critical Infrastructure Vulnerabilities

In modern critical infrastructure, the threat of a cyber-attack has become a matter of when it will happen rather than IF it will happen. Critical infrastructure poses a major target to attackers as weakening critical infrastructure has a large impact. Maliciously controlling the efficiency and effectiveness of a process can result in weeks-worth of repair and recovering data. In the example of the Colonial Pipeline attack, the company was shut down for nearly 6 days and lost \$4.4 million due to the ransomware attack. (Duffy)

Mitigations

With the multitude of Cyber Security Vulnerabilities on the control systems for critical infrastructure, SCADA systems are able to help in the defense line of a cyber-attack. Attacks on critical infrastructure can often come in forms of manipulating the processes of a critical infrastructure organization. By providing alerts for when systems reach critical levels, managers for the process can remotely control them and bring levels to normal. (scada.net) They can be programmed to send alerts when process are changed or access within a certain time-frame and many other situations where managers should be alerted for suspicious activity.

Conclusion

SCADA systems provide diagnostic data and control manipulation for critical infrastructure processes. Critical Infrastructure organizations are constantly being cyber-attacked to potentially pay the attacker a sum to be brought back to normal. These SCADA systems are able to be manipulated to counteract the attacks and can even be controlled remotely by a manager for the specific process. By alerting managers and having the ability to control processes on-site and remotely, SCADA systems are able to provide additional defenses to critical infrastructure.

References

SCADA Systems

<https://www.scadasystems.net/>

Duffy C., Edgan M. (2021). “Colonial Pipeline Launches Restart after Six-Day Shutdown”.

CNN. <https://www.cnn.com/2021/05/12/business/colonial-pipeline-restart>

CISA (2006) “Mitigations for Security Vulnerabilities Found in Control System Networks”. ISA.

https://www.cisa.gov/sites/default/files/2023-01/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf