Name: Khalia Douglas

Date: 4 November 2022

How SCADA Can Mitigate Vulnerabilities Within Critical Infrastructures

SCADA systems are a collection of both software and hardware components that monitor and control entire sites and systems in real-time. Critical infrastructures are essential to a nation and must be protected to sustain the economy and the quality of life. SCADA systems can be used to support the protection of our most critical infrastructures.

What is SCADA?

First coined in the 1970s, SCADA is the birth child of automation (*SCADA*, 2018). SCADA, Supervisory Control And Data Acquisition, falls under the umbrella term Industrial Control System (ICS), referring to a group of process automation technologies (Lamba et al., 2017). SCADA was created to be the solution to the many manufacturers, industrial plants, and remote site problems. Before SCADA, these industries relied heavily on personnel to monitor equipment. As these industries grew in size, it became more and more difficult to manage and control the equipment. SCADA was the solution, it allows supervision and control of plants, both locally and remotely, examining, collecting, and processing data in real-time. Some of the most important features include data acquisition, remote control, network data communication, data presentation, real-time data, alarms, and reporting (Loshin, 2021).

Critical Infrastructure and The Vulnerabilities

There are 16 major sectors considered critical by the U.S. government: chemical, dam, energy, food and agriculture, transportation, healthcare and public health, and information technology sectors to name a few (*Critical*, n.d.). The protection and security of these sectors are partially owned and operated by the private sector (*Critical*, n.d.). To modernize their infrastructures, overseeing companies are increasing their operational technology with traditional, modern IT systems (Labus, 2022). The digitization of critical infrastructures paired with the increased dependency on third parties has heightened the vulnerability of cyberattacks, specifically supply chain attacks (Labus, 2022). The biggest threat to these infrastructures is the legacy systems that

are still in use, increasing security risk (*Critical*, n.d.). Despite the evident risk to critical infrastructure, the security of ICS is not considered a significant investment area (Lamba et al., 2017). Martin Naedele argues the main obstacle to control system security is not technical, but financial (Naedele, 2007). Energy, water, transportation, and healthcare systems are needed every day to survive, making core infrastructures the most vulnerable considering the massive impacts an attack would have on citizens. Citizens would be affected greatly with limited access to critical resources.

How SCADA Mitigates Vulnerabilities

One of SCADA's components is the Human Machine Interface (HMI), software that facilitates interaction with field devices such as pumps, valves, etc. It gives processed data to the human operator to control processes. Among the aforementioned features is the ability to alarm and alert SCADA operators to potentially significant conditions in the system (Loshin, 2021). SCADAs alarm system consists of two digital status points, ALARM or NORMAL. If requirements are met for the alarm, it is activated along with an alert to operators and managers on top of sending out text messages and emails (SCADA Systems, n.d.). If an intruder can bypass security mechanisms, any attempt to alter critical settings would alert the system. Data collection allows SCADA systems to collect data in real-time for a better understanding of current operations. Anything deviant or unusual can be detected through this, mitigating the risk of manipulation, unauthorized access, and/or catastrophic disaster. Through remote control, SCADA systems can control industrial floor processes. This allows for early intervention of malicious attempts to override critical systems. With the ability to collect and log data, applying appropriate context gives an in-depth perspective of the industrial plant in real-time (Sectrio, 2019). Having this feature grants operators, administrators, and managers to compare and study historical and real-time data, allowing the ability to observe perhaps discrete data resulting from cyber criminals with ill intent.

Conclusion

Critical infrastructure systems are national priorities as it is a foundation for an effective economy, and supports and maintains the quality of life. Challenges arise as infrastructures are struggling to keep up with the latest technologies, causing them to be more vulnerable to cyber-attacks. They must be protected to secure our national security and the livelihood of all citizens. We must err on the side of caution in protecting our most valuable and critical infrastructures. SCADA systems are an effective tool to ensure that the security of critical infrastructures is protected from cyber threats and vulnerabilities.

References

Critical Infrastructure Vulnerability. (n.d.). Senstar. Retrieved November 1, 2022, from https://senstar.com/senstarpedia/critical-infrastructure-vulnerability/

Labus, H. (March 15, 2022). *The massive impact of vulnerabilities in critical infrastructure*. Help Net Security. https://www.helpnetsecurity.com/2022/03/15/critical-infrastructure-security/#:~:text=The%20digitalization%20of%20critical%20infrastructure,being%20compromised%20as%20collateral%20damage.

Lamba, A., Singh, S., Singh, B., Dutta, N., Muni, S., (2017). MITIGATING CYBER SECURITY THREATS OF INDUSTRIAL CONTROL SYSTEMS (SCADA & DCS). *International Journal For Technological Research In Engineering*, 2347 - 4718, 31-34. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3492685

Loshin, P. (2021, December). *SCADA (supervisory control and data acquisition)*. TechTarget. https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition#:~:text=SCADA%20(supervisory%20control%20and%20data%20acquisition)%20is%20a%20category%20of,to%20control%20equipment%20and%20conditions.

Naedele, M. (2007). Addressing IT Security for Critical Control Systems. *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 115-115, doi: 10.1109/HICSS.2007.48.

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

Sectrio. (2019, September 25). Complete Guide to SCADA Security. Security Boulevard. https://securityboulevard.com/2022/09/complete-guide-to-scada-security/

What is SCADA? (2018, September 12). Inductive Automation. https://inductiveautomation.com/resources/article/what-is-scada#:~:text=The%20term%20%E2%80%9CSCADA%E2%80%9D%20was%20coined,processes%20more%20than%20ever%20before.