Name: Kris Vargas

Date: 3/22/23

SCADA Systems

BLUF

The acronym known as "SCADA" stands for supervisory control and data acquisition. SCADA encompasses all of the industrial control systems that are utilized to control important infrastructure processes, industrial processes, and facility-based processes. Using computers and analysis of real-time data, SCADA allows for a way to monitor and control these complex processes effectively, whether it be using centralized systems that control entire sites, or complex systems spread out over large areas with more automated control.

Vulnerabilities (Critical Infrastructure Systems)

Critical Infrastructure can be broken down into 14 particular areas, according to the US government(2). These areas include Agriculture and Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Banking and Finance, Energy, Transportation, Chemical Industry and Hazardous Materials, Postal and Shipping, National Monuments and Icons, and Critical Manufacturing(2). Now what do all of these wide-ranging sectors have in common? In one way or another, they all provide either goods, services, and/or assets that are considered essential for society and the economy to function. But because of how important each sector is, that also means that if any of them were to be damaged or messed with, the entire flow of society and the economy would be in deep

trouble. Critical infrastructure systems are no stranger to vulnerabilities such as data breaches and often require careful monitoring by professionals in order to ensure that the processes are being carried out without any problems, and such attacks or problems can result in their entire foundations being put in jeopardy. So given their obvious importance, we need ways to secure and protect these infrastructures in order to prevent any type of catastrophic consequences from occurring. This is where SCADA comes to fill in a very important role.

SCADA's Role in Mitigation

The way that SCADA is set up is extremely helpful for the individuals that are in charge of protecting critical infrastructure systems. SCADA runs real-time data analysis in order to detect stark changes in normalcy or any other type of activity within the systems that should be alarming or worth noting([1]). For example, in a typical water-cooling system, while the Programmable Logic Controller (PLC) would be in charge of the flow of the cooling water, the SCADA system would allow for any significant changes or alarm conditions such as abnormally high temperatures or change in flow to be properly recorded and then displayed([1]). This not only allows for easier monitoring of the processes and data, but it also translates to much higher system efficiency and reliability([3]), as the system's processes are carefully and meticulously planned out and the automation eliminates much of the threat of human error.

Weaknesses of SCADA

For all of the positives that SCADA has to offer, it would be short-sighted to say that it is without its flaws. Because of how SCADA systems are connected to networks through the usage of computers, cyberattacks are always a very present and dangerous threat([2]). A potential hacker could seek to interrupt or slow down the SCADA-controlled processes by delaying the circuit of

information that the systems use to relay real-time data, thus disrupting the flow and comprising the entire system. Attackers could also seek to mess with the complex programming instructions that go into the system's controllers, which can lead to misfiring's and/or complete malfunction(2). However, with proper training and in-depth informing of the individuals running the SCADA systems (as well as the leaps and bounds that cybersecurity makes in terms of technological advancements everyday), these vulnerabilities can be mitigated effectively, allowing SCADA to flourish under the right conditions.

Conclusion

In conclusion, SCADA systems, despite their current issues regarding vulnerability to potential cyberattacks, are still extremely important and are vital to how we protect and maximize the potential of critical infrastructure systems. With the increasing technological advancements in the field of cybersecurity, more of SCADA's weaknesses will begin to shrink in danger, allowing for them to become even more viable. SCADA systems not only allow for critical infrastructure systems to function as efficiently and as smoothly as possible, but in the unfortunate occurrence that a problem does arise, it will have the real-time data analyzed and displayed for the appropriate professionals to be made aware of the issues and address them accordingly.

References

Google. (n.d.). *SCADA systems*. Google Docs. Retrieved March 26, 2023, from https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?usp=sharing (1)

IJCA. NADIA. (n.d.). Retrieved March 26, 2023, from https://nadiapub.com/journals/ijca/ (2)

Role of SCADA in securing critical infrastructure | waterworld. (n.d.). Retrieved March 27, 2023, from https://www.waterworld.com/home/article/16190328/role-of-scada-in-securing-critical-infrastructure (3)