Bianca Perez

3/26/2023

SCADA Systems

SCADA (Supervisory Control and Data Acquisition) system is a collection of both software and hardware components that allow supervision and control of plants, both locally and remotely. The stance I have taken, provided by the article called "SCADA Systems", is that this system has major security issues, yet that can be remedied if handled correctly.

What is a SCADA?

SCADA systems can be found in the hearts of multiple industries. They are called Industrial Control Systems (ICS), which collect information from equipment and industrial processes and provide supervisory-level control over them *(Where Can Vulnerabilities Be Found in SCADA Systems?, 2022)*. Usually located over a wide geographical area. Information is performed from hardware such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). An example of a PLC provided by the article *(SCADA Systems - SCADA Systems, 2018b)* states in an industrial process, "Controls the flow of cooling water, the SCADA system allows any changes related to the alarm conditions and setpoints for the flow (such as high temperature, loss of flow, etc) to be recorded and displayed." Both RTU and PLC are stationed at the sites where the processes are located. Doing so, both will receive commands from and send information to the master station. This benefits network technicians to make important decisions based on real-time data. The master station or called the Human Machine Interfaces (HMIs), will display

the processed data to the human operator. SCADA systems can be found in major functions of the industries as follows: manufacturing, oil, gas, transportation networks, energy, water, and waste treatment.

The vulnerabilities and the remedies

SCADA systems can bring multiple benefits yet its vulnerabilities and potential threats are a problem for network technicians. This also can affect the users in the end. As mentioned before, SCADA systems are used to control and monitor major systems in modern society. Provided by the article *"SCADA Systems"*, the first problem can be anything malicious that can affect the control host machine like a virus or a human access. The second issue can be found through the packet access or in other words data broken up to network segments that host SCADA devices. Both pose a threat to the system, with the most well-known attack being the Stuxnet malware in 2010. It was the wake-up call that such a danger exists. The impacts done by such attacks can include damage to equipment, theft of sensitive information, critical human safety hazards, and snowball effects down the supply chain *(Where Can Vulnerabilities Be Found in SCADA Systems?, 2022*). Mainly it's best to stay updated and to ensure all applications are implemented. An example can be identifying all connections to your SCADA system like the network, this helps solve the second issue mentioned before. Better yet, it's best to have a recovery plan if a disaster arises. System backups are essential to the SCADA system to solve any destruction of the system. In addition, SCADA vendors are also an excellent option to protect SCADA systems as follows: Honeywell, Schneider Electric, GE Grid Solutions, ABB, and Siemens Energy (Best SCADA Vendors, n.d.). These manufacturers provide perfect-fit solutions to any problem.

Conclusion

In conclusion, SCADA systems can be harmful if fallen to the wrong hands or virus. Though by the advance of technology, the SCADA system's security will continue to grow. For now, it's best that applications that are used are updated. For it's essential to ensure the safety of the system and the public.

References

Where Can Vulnerabilities Be Found in SCADA Systems? (2022b, January 14). DPS Telecom. https://www.dpstele.com/blog/where-can-vulnerabilities-be-found-in-scada-systems.php

SCADA Systems - SCADA Systems. (2018b, July 25). SCADA Systems. http://www.scadasystems.net/

Best SCADA Vendors. (n.d.). https://www.dpstele.com/blog/top-5-best-scada-vendors.php