Myrna E. Santiago

11/05/2023

CYSE 200T_ 17570

SCADA Systems

SCADA (Supervisory Control and Data Acquisition) is a system that coordinates processes in real time. This Industrial Control System (ICS) is used to control processes in infrastructure, facility-based, and industrial areas. This write-up explained the vulnerabilities associated with critical infrastructure, what SCADA is, and how it helps mitigate the risks of said vulnerabilities. (SCADA, n.d.)

What is SCADA?

SCADA is a category of software applications and hardware that gathers data in real-time from remote locations. This data is used to control equipment and conditions in industrial processes. These processes include:

- **Infrastructure –** water treatment, wastewater treatment, gas pipelines, wind farms, etc.
- **Facility-Based –** airports, space stations, ships, etc.
- **Industrial –** production, manufacturing, refining, power generation, etc.

SCADA is a centralized system that relies on remote terminal units (RTUs) or programmable logic controllers (PLCs) that automatically control all actions. Data acquisition starts at this level. (SCADASystems, n.d.)

The data is sent to Human Machine Interfaces (HMIs) or Graphical User Interfaces (GUIs) in the form of points that are either "hard" or "soft". A hard point is the actual output or input of the system. While a soft point is the result of different math and logic operations applied to other points. Once the data is processed, it is displayed to the human operator. The human operator studies the data and can react to alarms or events by sending instructions to the controllers.

Critical Infrastructure Vulnerabilities

Eighty percent of the critical structures in the United States are privately owned. While large companies can cover cyber and physical security, small companies cannot, which creates a disparity of resources. Many companies also rely on outsourcing their needs, which creates a complex system that creates more vulnerabilities because of the extra personnel involved and diverse resources used.

Other vulnerabilities come from natural sources, like hurricanes, earthquakes, volcanic eruptions, droughts, floods, etc. Human caused vulnerabilities, like theft, terrorism, economic espionage, etc. There are also accidental or technical ones, like water-main ruptures, power-grid rid failures, etc.

A growing vulnerability is in cyber security. Adding modern technology can

create a new set of vulnerabilities if done incorrectly and can be the target of malicious agents. (Tal, 2018)

Why is the SCADA system important?

SCADA system allows scalability, which provides better availability of supported hardware and software and the use of cloud computing to meet workload demands. Interoperability which avoids vendor lock-in. Communication allows for widely supported communication protocols. Support that allows third parties to provide support to the systems.

Conclusion

SCADA systems correctly use provide extra security and work efficiency. One operator can pinpoint a problem and solve it, if possible, remotely. This technology can help with large workloads, especially in times when there is a shortage of specialized workers. If applied properly, it reduces the risk of physical security problems by adding layers of security. It also provides digital security through sensors and alarm systems. Like any other system, it can be a target of cybercriminals or criminals with an interest in affecting the country or geographical area in question. Like any other system mitigating these vulnerabilities relies on best practices, education, and keeping up to date with news and patches that can make our control system more secure.

References

SCADA. (n.d.). *What is SCADA?* SCADA. https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for,data%20from%20the%20industrial%20equipment.

SCADASystems (n.d.). *SCADA Systems. S*CADASystems.net. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?pli=1.

Tal, J. (2018, September 20). *America's Critical Infrastructure: Threats, Vulnerabilities and Solutions.* Securitron. https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions.