Radoslav Yanev

Oct 12th, 2025

SCADA systems and vulnerabilities associated with Critical infrastructure systems

Critical infrastructure systems are vulnerable to many types of cyberattacks – ransomware, DDoS, insider threats and physical attacks. SCADA system and application help mitigate that risk. Supervisory Control and Data Acquisitions are used in power systems and to monitor, operate and control infrastructure processes, facility-based processes and industrial processes. Failure in the SCADA system can have severe consequences and it is very important to always follow a protocol.

SCADA Systems Overview

SCADA (Supervisory Control and Data Acquisition) systems are used in power systems to monitor, operate and control generation; transformer, switching and load stations. Such control can be automatic or manually initiated by operator commands.

(Hamoud 2003). Most of the actions are now automatic. SCADA systems consist of set of field sites, located in different places and each one of those fields also has at least one RTU, PLC and IED. The system, especially the small ones, have one main data center. The HMI is also an important part of SCADA, an apparatus that gives the processed data to the human operator. It provides the diagnostic data, management information, trending information, detailed schematics, maintenance procedures and troubleshooting guides.

SCADA Security Issues and Vulnerabilities

The popular belief is that those systems should be safe, because they are not connected to the internet. Unfortunately, this is not the reality. First, many systems rely on outdated technology – old protocols and software and insufficient security features. Remote access also has its weak points, as it gives additional entry points for hackers. The main computer holds all the control, and any unauthorized access can cause a lot of trouble. From unintentionally induced changes to viruses, host machines are usually the main target for the criminals. Another big threat is related to the packet access to network segments that host SCADA devices. Very little security is usually implemented to those and using VPN is not nearly sufficient.

Mitigating Risks

"There is a shortage of accurate historical data on SCADA incidents that can be used in the risk management process because of the confidential nature of this field." (Elhady, 2019). Real time monitoring is one of the main advantages of the system. SCADA always monitors the processes and if the system detects an alert, it will notify the appropriate personnel. The newer version of the system also provides enhanced access control – Multifactor authentication (MFA) and Role-based access control (RBAC) can ensure that only the people that are authorized to use specific machines are the ones with the access to it. Most of the Scada applications use encryption to protect data between the main computer and the remote units. Protocols, such as HTTPS/SSL are used to protect that vital data when it is transmitting. As mentioned earlier, web-based software is used with a VPN for extra security.

Conclusion

Since its implementation back in the 1950s, SCADA has been crucial in many aspects. The system is responsible for crucial infrastructure software and a single breach or cyberattack can cause a huge amount of damage to not only the system but to people too. With the advancement of technology, the risks are going to become greater and greater. I cannot emphasize more that following protocol always is the key to minimizing the risk as us humans always try to do things in a easier and shorter way as possible and thus we create room for errors.

References

SCADA Systems. (2019). *SCADA Systems*. Google Docs. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0

Hamoud, G., Chen, R.-L., & Bradley, I. (2004). Risk assessment of power systems SCADA. *2003 IEEE Power Engineering Society General Meeting (IEEE Cat. No.03CH37491)*. https://doi.org/10.1109/pes.2003.1270402

Elhady, A. M., El-bakry, H. M., & Abou Elfetouh, A. (2019). Comprehensive Risk Identification Model for SCADA Systems. *Security and Communication Networks*, *2019*, 1–24. https://doi.org/10.1155/2019/3914283