Name: Hans Peterson

Date: 3/17/2024

SCADA Systems

Critical infrastructure systems are vulnerable to cyber attacks and malfunctions. SCADA applications mitigate some of these risks through security, redundancy, and HMI.

Cyber attacks

According to the Department of Homeland Security, “Cybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States.” Hackers can target facilities that handle power stations, water treatment, hospitals, and manufacturing centers. If hackers are able to control and shut down critical infrastructure systems, it can cost lives and money. Even ransomware attacks have been brought out. According to Iwuozor, “For example, May 2021 recorded a popular ransomware attack by the Dark Side gang who attacked and shut down the U.S. East Coast’s fuel supply for days after which they extorted a whopping $4.4 million ransom.”

Potential Mitigation for Cyber Attacks

Currently, SCADA applications are also vulnerable to these cyberattacks. To combat this, SCADA vendors are developing specialized firewalls and industrial VPNs. If the processes within a critical infrastructure system are being compromised or controlled by a hacker, an operator could use an HMI to manually override controls.

Malfunctions

Whether a malfunction is caused by natural disasters, power outages, or broken equipment, critical infrastructure systems are vulnerable to malfunctions. Especially in critical infrastructure like water treatment, healthcare, and power plants, malfunctions can bring down sectors within a nation. Like cyberattacks, there are costly consequences. For example, according to Chang, “Hurricane Sandy in 2012 caused electric power outages to over 8.6 million customers in a broad region of the eastern United States; power outage was a key factor in fuel shortages following the storm (U.S. Department of Energy [USDOE], 2013).”

Potential Mitigation for Malfunctions

SCADA systems have redundancy systems to withstand the effects of natural disasters (Ex. temperature, vibration from earthquakes) and continue operation. Back-up hardware automatically takes over hardware that has failed, which allows systems to continue smoothly. Supervisory stations may also be used in the event of system failure; a disaster recovery site allows operation to continue with little hindrance. Dual servers are used in case a server fails. HMIs allow operators to supervise systems and override them if necessary.

Conclusion

Cyberattacks and malfunctions are two of the many vulnerabilities that critical infrastructure systems face. Cyberattacks are the primary threat that critical infrastructure systems now face due to their prevalence and effectiveness. Specialized firewalls and VPNs are being developed for SCADA systems to defend against cyber attacks. Malfunctions are as costly as cyber attacks. SCADA systems use redundancy and HMIs to combat malfunctions.

References

Chang, S. E. (2016, October 26). *Socioeconomic impacts of infrastructure disruptions*. Oxford Research Encyclopedia of Natural Hazard Science. https://oxfordre.com/naturalhazardscience/display/10.1093/acrefore/9780199389407.001.0001/acrefore-9780199389407-e-66

Department of Homeland Security. (2022, February 23). *Secure Cyberspace and Critical Infrastructure*. Department of Homeland Security. https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

Iwuozor, J. (2022, May 18). *The Biggest Threats to the US Critical National Infrastructure*. ITEGRITI. https://itegriti.com/2022/managed-services/the-biggest-threats-to-the-us-critical-national-infrastructure/