John Heath

November 11, 2025

SCADA Systems

BLUF: Critical Infrastructure Systems (CIS) are critical for ensuring quality of life for the public. CIS are subject to cybersecurity threats, which would be detrimental for society. Fortunately, SCADA systems can mitigate cybersecurity risks.

Risks of Critical Infrastructure Systems

CIS consists of water treatment plants, power grids, streetlight systems, emergency services, etc. These sectors of critical infrastructure are crucial to ensuring the well being of society. Without them, society would not be able to function at maximum efficiency, with the potential for lives to be lost. Because these systems are vital for societal function, they are targets for cyberwarfare or cyberterrorism. For example, a 2015 attack on Ukraine's power grid affected hundreds of thousands of individuals. According to the CISA, "power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers." (CISA) They were targeted by Russian hacker group called Sandworm who gained remote access to the systems by acquiring authorized credentials. They then used "KillDisk malware which erases selected files on target systems and corrupts the master boot record, rendering systems inoperable". (CISA) While the Sandworm group did not gain anything monetarily, they gained proof that they were capable of remotely shutting down an opponents power grid, while also gaining deterrence to any country considering targeting Russia in a cyber attack.

How SCADA can Mitigate Cyber Risks

SCADA systems provide an array of tool for mitigating cyber risks. For starters, SCADA applications can alert cybersecurity professionals of cybersecurity threats. Functions like intrusion detection and monitoring systems can provide a type of surveillance for security systems that alerts professionals if systems are in an irregular or compromised state. Furthermore, SCADA systems can be used to create a Master Station. “Master stations can have multiple servers, disaster recovery sites, and distributed software applications in larger SCADA systems.” (SCADA Systems) These master stations mitigate cyber threats by utilizing strict access control measures and network segmentation to ensure that an attacker can not move laterally throughout the network if they were to gain access to it. Additionally, SCADA systems can be allocated to allow backup hardware to step in for failing hardware.

Conclusion

SCADA systems are a valuable asset to securing critical infrastructure systems. They make it more difficult for cybersecurity measures to fail, as well as making them harder to operate once they are compromised.

References

SCADA Systems. “SCADA Systems.” *Google Docs*, 2019, docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0.

---. “Cyber-Attack against Ukrainian Critical Infrastructure.” *Cybersecurity and Infrastructure Security Agency*, CISA, 20 July 2021, www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.