Seth Sarauw
CYSE 200T
November 9th, 2025
Professor Duvall

SCADA Systems

BLUF

I will be discussing the vulnerabilities associated with critical infrastructure systems, as well as the role the Supervisory Control and Data Acquisition (SCADA) applications play in mitigating these risks.

Vulnerabilities associated with critical infrastructure systems

According to the aforementioned article, two vulnerabilities would be unauthorized access and "packet access to network segments that host SCADA devices". According to EGNYTE, unauthorized access is "when a person gains entry to a computer network, system, application software, data, or other resources without permission" (EGNYTE, 2025). Unauthorized access can be done by a human or a malware, and it could be intentional or unintentional. There are multiple reasons for someone to want unauthorized access, such as: revenge, stealing data, or blackmail. Packet access to network segments that host SCADA devices refers to the weakness in security when an unauthorized individual is able to intercept or manipulate data packets. According to the aforementioned article, this is a vulnerability as there is little to no security in the packets. The article also states that users tend to believe that a virtual private network (VPN) is good enough protection, failing to realize there are physical switches that can easily bypass those "protections".

SCADA Mitigation

According to the aforementioned article, SCADA is addressing these risks by creating and implementing specialized VPNs and firewalls to protect the networks. The article states that these VPNs and firewalls are based on Transmission Control Protocol/Internet Protocol (TCP/IP). According to TechTarget, TCP/IP is "a suite of communication protocols used to interconnect network devices on the internet" (TechTarget, 2024). The article also states it can be used for private computer networks like intranets or extranets. Another thing SCADA is doing as a protection measure is implementing whitelisting protocols, as they are excellent at keeping unauthorized users out as well as unwanted changes.

Conclusion

To conclude, there are multiple vulnerabilities associated with critical infrastructure systems which include unauthorized access and packet access to network segments. SCADA has been creating and implementing VPNs and firewalls based on the TCP/IP to protect the network packets.

Sources

"Unauthorized Access: Meaning & How to Prevent It." Egnyte, 28 Oct. 2025, www.egnyte.com/guides/governance/unauthorized-access .

Yasar, Kinza, et al. "What Is TCP/IP and How Does It Work?: TechTarget." Search Networking, TechTarget, 26 Sept. 2024, www.techtarget.com/searchnetworking/definition/TCP-IP.