Prescott Kowalski

6APR25

Professor Umphlet

Write up: SCADA Systems

VULNERABILITIES

As many know, older technology and legacy systems are littered with issues. From threats of ransomware due to the high value of critical infrastructure, to security issues due to the lack of modernization of these legacy systems. However, in theory, AI and automation may help with this to enhance cybersecurity by automating threat detection and response, but physical layers will still be needed. Per *Dark Reading,* "One of the biggest challenges in securing critical infrastructure is the reliance on legacy systems. These outdated systems often can lack modern security features, making them attractive targets for cybercriminals." Increased connectivity through IoT devices have also created more entry points for cyber threats, making targets of systems like power grids and water supplies.

SCADA SYSTEMS

Due to the emergence of AI threats and desire for remote access, a zero trust model will be needed for the SCADA systems. Per *SCADA Systems,* SCADA vendors are developing specialized Industrial VPNs to mitigate the risks, as well as firewall solutions that are based on TCP/IP. Per numerous sources, *Agilicus* and *Delina* being examples, SCADA systems are using a

Zero Trust model to mitigate risks. A Zero Trust Model requires complete authorization from the user to even begin the remote access process. Meaning, without facial recognition, voice recognition and other forms of biometric technology, access will not be granted. Industrial firewalls, VPNs, among others, are just a few of the ways SCADA systems are mitigating the risks.

CONCLUSION

In conclusion, Vulnerabilities will continue to be a problem with the rise of AI, but as SCADA systems continue to adapt and be modernized with Zero Trust, firewalls, industrial VPNs and similar technologies, they will be mitigated. This is crucial, as SCADA systems have countless underlying issues that are easily avoidable with modernization. Modernization and adaptation of Legacy Systems will take a while to do, but are vital for the safety of our critical infrastructure.

REFERENCES:

- "Navigating Cyber-Risks and New Defenses in 2025." *Darkreading.com*, 2025, www.darkreading.com/vulnerabilities-threats/navigating-cyber-risks-new-defenses. Accessed 29 Mar. 2025.
- Novak, Chris. "Navigating Cyber-Risks and New Defenses." *Dark Reading*, 28 Mar. 2025, https://doi.org/https://www.darkreading.com/vulnerabilities-threats/navigating-cyber-risks-new-defenses.

- “What Are the 4 Types of SCADA.” *Empowered Automation Solutions LLC*, 17 Jan. 2025, www.empoweredautomation.com/what-are-the-4-types-of-scada.
- “SCADA Systems.” *SCADA Systems*, www.scadasystems.net/. Accessed 29 Mar. 2025.
- Carson, Joseph. “Zero Trust for ICS / SCADA Systems: How Does It Work?” *Delinea*, 2025, delinea.com/blog/zero-trust-for-ics-scada-systems.
- ANON. “Using Zero Trust to Enable Secure Remote Access to SCADA for Water Systems.” *Agilicus*, 1 Aug. 2024, www.agilicus.com/using-zero-trust-to-enable-secure-remote-access-to-scada-for-water-systems/.