SCADA Systems

Trey Smith

The vulnerabilities within critical infrastructure can be vast when looking at the maintenance required to put it to use. In (Cyber attacks 2024) it says “cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable.” These vulnerabilities can have severe impacts on day-to-day life. In the same source, there was a map that showed where these threat actors tried to attack, and they were things like water systems in Texas, healthcare systems in New Mexico, and wastewater treatment statements in New Jersey. SCADA devices collect and survey data that is transmitted from sensors and other types of devices. These devices can make sure that all things are running safely and efficiently. These devices also mitigate risk by being a way to double-check and diagnose the system when things start to go wrong. For example, supervisory stations are “responsible for communication with the field equipment." They can also “have multiple servers, disaster recovery sites, and distributed software applications in larger SCADA systems." This way, if anything goes down due to an attack, they can reconfigure and reboot their systems with a hotfix so that the whole facility doesn’t have to go down when they get attacked (SCADA Systems, 2018).

References:

SCADA Systems. (2018). *SCADA Systems - SCADA Systems*. SCADA Systems. https://www.scadasystems.net/

(SCADA Systems, 2018)

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems. (n.d.). https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

(*Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems*, n.d.)