Blaine Gernandizo

Professor Bowman

CYSE 200T

30 October 2025

SCADA Systems

Although it may not seem like it, critical infrastructure systems, such as those in water, energy, and transportation, are highly susceptible to significant cybersecurity vulnerabilities. This risk is often heightened by a false sense of security, stemming from the mistaken belief that these systems are isolated from the internet. Many of these facilities rely on legacy Industrial Control Systems (ICS) and SCADA systems that were originally designed decades ago with proprietary protocols, offering minimal protection against modern threats leaving them exposed through unpatched software. The ongoing convergence of propriety control to standard TCP/IP has dramatically expanded the attack surface, exposing critical processes to sophisticated cyber-attacks. Such breaches could lead to devastating disruptions, including unauthorized access to control software and the network packets that directly command industrial hardware.

They provide comprehensive, real-time monitoring and supervisory control, enabling operators to rapidly detect anomalies and intervene in industrial processes. A key mitigation feature is the automated alarm system, which triggers immediate alerts via text or email to facilitate a swift incident response. To counter cyber threats, these systems are increasingly supported by specialized industrial firewalls and VPNs, which segment and protect the network to isolate critical control assets from unauthorized access. Furthermore, SCADA systems meticulously log all operational data as historical timestamp-value pairs, creating a forensic record for post-incident analysis to determine the root cause of failures and prevent future occurrences. Emerging technologies like artificial intelligence for behavioral baselining and deception technology, such as honeypots, further enhance threat detection and response. By adhering to Security frameworks like the NIST Cybersecurity Framework and leveraging a strategy that combines these controls, SCADA systems are instrumental in securing critical infrastructure, ensuring the continuous safe operation of vital services against evolving cyber threats.

References:

SCADA Systems

Cybersecurity of Critical Infrastructure with ICS/SCADA Systems – IEEE Public Safety Technology. (n.d.). https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems/