Daija Brown
Mr. Kirkpatrick
Cybersecurity, Technology & Society-200T
08 March 2026

The Impact of SCADA Systems on Critical Infrastructures

Critical infrastructures are subject to technological and human based vulnerabilities. SCADA systems can provide mitigations to keep critical infrastructures operational.

Technology Based Vulnerabilities

The advancement of critical infrastructures introduces newer vulnerabilities. Internet connections help make critical infrastructures more easily assessable for the people who maintain them and threat actors as well. Remote access to systems makes it easier to maintain the system without physically being in the same location, but an insecure connection could let the wrong people in. Additionally, critical infrastructures are vulnerable to supply chain software based attacks. In September of 2019, SolarWinds suffered a breach that was not discovered until November 2020. By then, the hackers weaponized the code in software updates by adding a trojan virus that created a back door that allowed the threat actors to have remote access to compromised systems. This attack impacted approximately 18k customers, including the United States federal government. “Of those, the threat actor targeted a smaller subset of high-value customers, including the federal government, to exploit for the primary purpose of espionage” (U.S. Government Accountability Office).

Human Based Vulnerabilities

Humans are consistently the weakest link when it comes to cybersecurity. With critical infrastructures, the impact could potentially risk human lives. Without proper education, phishing and social engineering attacks are likely to succeed. While unintentional exposure is common, this does not rule out the potential for insider threats. “Insider threats often take two forms: calculated acts of harm and unintentional mistakes. Malicious insiders may exploit access for personal gain or revenge, causing severe damage to systems and trust, At the same time, negligence or simple human errors can open the door to vulnerabilities that adversaries can exploit” (Cybersecurity & Infrastructure Security Agency). The motivations behind an insider threat may not be known, but there are mitigations that could be put in place to stop or log data exposure. A critical infrastructure may also be impacted by improper change management configuration. This would allow a user to intentionally, or unintentionally, to execute a change that may impact the operations of a critical organization.

SCADA Mitigations

Segmenting a network with SCADA devices prevents an attacker from accessing critical systems via lateral movement. SCADA systems can provide further mitigations by implementing VPNs or firewalls to mitigate unauthorized application changes, and prevent a threat actor from sending packets to a network segment that hosts a SCADA device. Modern versions of these devices can be configured to provide access control, and implement the principle of least privilege. This mitigates unauthorized changes to critical systems by unauthorized users. They can also utilize monitoring to detect changes, which helps capture unauthorized changes from individuals who have access, but are not authorized to make specific changes.

Conclusion

In Conclusion, critical infrastructures are subject to vulnerabilities from a technology, and human standpoint. These vulnerabilities can be mitigated by implementing access controls, network segmentation, and monitoring to mitigate the impact to a critical infrastructure. These controls help detect anomalies, and prevent unauthorized changes, and mitigate lateral movement to critical systems.

Works Cited

U.S. Government Accountability Office. “SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic).” *GAO.gov*, 22 April 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic. Accessed 8 March 2026.

Cybersecurity & Infrastructure Security Agency. “CISA Urges Critical Infrastructure Organizations to Take Action Against Insider Threats.” *CISA*, 28 January 2026, https://www.cisa.gov/news-events/news/cisa-urges-critical-infrastructure-organizations-take-action-against-insider-threats. Accessed 8 March 2026.