Nigel Adkins
April 8, 2026
CYSE 200T
Professor Duvall

Vulnerabilities associated with SCADA

BLUF: SCADA which stands for Supervisory Control & Data Acquisition is a software system that uses computers and network data for the high level supervision of machines and processes. Due to the openness of SCADA systems they often have vulnerabilities that are easy to exploit.

Lack of active network System

Most SCADA systems don't have an active networks system. This negatively affects the systems ability to detect suspicious activities and combat cyber attacks when they happen.

Slow updates to SCADA systems

New vulnerabilities emerge as systems get more advanced and new technologies are introduced. A lot of SCADA systems lack consistent updates to both hardware and software systems due to inconvenience, with some components of SCADA systems being over 10 years old. This can cause gaps that lead to unreliable systems that attackers can exploit.

Authentication hole

SCADA systems were created to be open and easily operated. This "openness" and easy access leads to Authentication holes where attackers can gain unauthorized access to SCADA systems. The lack of confidentiality of passwords leads to this vulnerability.

Poor Physical security

Poor Physical security like the lack of security guards, security cameras, locks control centers, and biometric access controls could be detrimental to SCADA systems as it would allow easier access to critical systems like power grids or transportation systems (SCADA Security Issues).

Conclusion

Conclusion; SCADA systems have many vulnerabilities due to poor physical security, authentication holes, slow updates, and lack of active network systems. Some mitigation tactics

for these risks include consistent updates to systems, advanced data analyses, limited access, and stricter authentication.

SCADA Systems and Their Vulnerabilities, www.secpoint.com/scada-systems-their-vulnerabilities.html.