Mark O'Neal

Professor Umphlett

Cybersecurity Society Technologies

08 April 2026

SCADA Systems

"A SCADA (Supervisory Control and Data Acquisition) system is a software and hardware-based industrial control system used to monitor, control, and analyze industrial processes in real time" (Inductive Automation.) These SCADA systems are honestly magnificent due to their ability to manage complex processes. Although, they are now becoming just as vulnerable, from a cybersecurity aspect, as they are helpful due to the closing of the "air gap." The gap between isolated mainframes and networked architecture is narrowing in as technology continues to evolve, and this makes SCADA systems a double edged sword.

As somewhat stated above, SCADA systems were once physically disconnected from public networks but now it seems like they rely on IP/ethernet (internet.) This new standard connection opens up SCADA systems to the everyday basic cyber threats. Additionally, the average communication protocols lack built-in encryption. This is a blatant issue for remote or programmable controls because if a hacker gains access to the network they may be able to send direct malicious commands.

On the other hand, SCADA applications help mitigate these risks/vulnerabilities. For example, Human Machine Interface (HMI) allows for real time mimic diagrams which help

detect rapid anomalies for physical cyber attacks. Furthermore, the use of dual redundant servers and recovery sites make sure that functions run fairly normal like during partial system failure.

Lastly, companies are now incorporating specialized VPNs and firewalls. Such tools help aid in stopping unauthorized changes/attacks to control software. So, by combining these security layers SCADA systems act as both a target and primary defense against the disruption of important services.