SCADA Systems: Examining Critical Infrastructure Systems & SCADA Mitigations

Written By: Ryan Stephens

Executive Summary:

SCADA Systems are integral to the functionality of Critical Infrastructure; they monitor and report data back to experienced administrators and engineers, who then analyze the data to ensure smooth and effective operations. SCADA Systems are being increasingly targeted by malicious actors of all kinds, who seek to cause harm to innocent civilians by shutting down Critical infrastructure or aiming to cripple military infrastructure. There are numerous threats facing SCADA Systems, but major ones include insider threats, unauthorized access, and privilege escalation. However, manufacturers are aware and actively seeking to mitigate these risks through the implementation of Firewalls, VPNs, and Whitelisting.

What Is A SCADA System?

SCADA stands for Supervisory Control and Data Acquisition, which is essentially an Industrial Control System (ICS). In simple terms, SCADA is a system that gathers information, analyzes it, and displays the information in a user-friendly Graphical User Interface (GUI) for engineers or system administrators to monitor. (DPS Telecom, 2022)

Why Are SCADA Systems Important?

SCADA Systems are commonplace within critical infrastructure environments and everyday facility-based environments. Regarding critical infrastructure, SCADA Systems control everything from water treatment facilities to gas pipelines, wastewater treatment facilities, and even nuclear power plants. While in more everyday applications, they control facilities such as airports, Train stations, railroads, and the Power Grid. This means that SCADA Systems are vital, and billions of people rely on them to do their job effectively day in and day out.

Who's Behind Attacks on Critical Infrastructure?

As mentioned above, SCADA Systems are integral to the functionality of Critical Infrastructure, which is why attackers often target these systems. In the modern age, there are countless examples of attacks on critical infrastructure, such as the Stuxnet attack on Iran's Nuclear Program, where the American National Security Agency teamed up with Israeli Intelligence Agencies to target Programmable Logic Controllers controlling Iran's Nuclear centrifuges.

(which can be regarded as critical infrastructure in their case, as it allows Iran to project power and influence throughout the Middle East and on the world stage), or the numerous attacks on water treatment facilities across the United States and Europe from adversarial nations like North Korea, Iran, China, and Russia. Attacks on critical infrastructure can occur from anyone, anywhere, at any time, whether from state-sponsored cyber organizations or nation-states themselves. Attacks on critical infrastructure level the playing field for everybody.

Specific Vulnerabilities Regarding SCADA Systems:

Most people believe that SCADA Systems are more likely to be secure because they are disconnected from the internet or located in remote, hard-to-reach areas; however, this is not always the case, due to multiple reasons, including insider threats, unauthorized access, or privilege escalation. (Kirkpatrick, 2025) In the case of insider threats, malicious actors could install malware or intentionally change settings on devices within the SCADA System to cause harm to physical devices or manipulate the information displayed to authorized users. Unauthorized access to SCADA devices is the most significant vulnerability to the integrity of data and the availability of the system, as most, if not all, unauthorized users would manipulate data or disrupt the device, thus eliminating its availability. Regarding privilege escalation, most SCADA Devices assume that whoever is connected to the device is the authorized user and therefore automatically grant them “admin” privileges, which means the user can do whatever they want with the SCADA Device.

How Are SCADA Systems Mitigating Vulnerabilities?

The manufacturers behind industry-standard SCADA Systems are aware of the risk of cyberattack. They are actively working on developing solutions to mitigate the risk of these vulnerabilities being exploited through various means. Some of the mitigations are as follows: implementing industrial VPNs and firewalls for networks using TCP/IP, and whitelisting SCADA devices. (Kirkpatrick, 2025)

Diving Deeper into Specific Mitigations:

Virtual Private Networks: Virtual Private Networks, or VPNs for short, are essentially tunnels that encrypt data while it is being transmitted between devices. Therefore, implementing VPNs in SCADA Systems makes it more difficult for attackers to intercept and modify the data being transmitted.

Firewalls: Firewalls enable network segmentation, preventing attackers from moving into different parts of a network after breaching a single point of entry. Firewalls can also filter unauthorized traffic and restrict those unauthorized IP addresses from continuing to send packets

to the network, while implementing access control to allow only certain users access to the SCADA devices.

Conclusion:

SCADA Systems in today's world are exposed to numerous risks, but with the correct implementation of mitigations, these risks can be reduced to manageable levels. Researching new ways to mitigate threats on SCADA Systems for future use is also vital, as Artificial General Intelligence and Quantum Computing are on the horizon; older methods of security will not suffice for keeping Critical Infrastructure safe.

References

Knowledge base: What does scada mean?. Knowledge Base: What is SCADA? How Does it Work? (n.d.). https://www.dpstele.com/scada/knowledge-base.php

Kirkpatrick, C. (2025). SCADA Systems Article. Norfolk; Old Dominion University.