Krystiana lee
Professor Duvall
CYSE 200T
April 8, 2026

Vulnerability and the role of SCADA Systems

BLUF

Critical infrastructure systems are targeted easily by cyber attacks because of weak internet connections and security. SCADA (Supervisory Control and Data Acquisition) systems play a huge role in helping protect these systems by making sure they are monitored, actively sending alerts, as well as controlling processes automatically.

Introduction

Critical systems are things we use everyday like transportation, water systems, and electricity. These systems use SCADA to monitor and control operations. SCADA systems use computers, networks, and sensors to help run theses processes. They may seem helpful they can be a risk of cyberattacks.

What SCADA Systems Do

SCADA systems gather data from machines and sensors by using devices such as RTUs and PLCs. The data is then sent to a main system and shown on screen called an HMI, where operator can see what us going on. SCADA systems usually run on their own. For instance, they can change the temperature or flow of water without help from people. If something goes wrong, operators can still step in. Many fields, including water treatment, energy, and manufacturing, use SCADA systems.

Vulnerabilities in Critical Infrastructure

These systems are weak for a variety of reasons. First, a lot of SCADA systems are outdated and did not come with good security. This makes it easier for hackers to gain access in.
Second, modern systems can connect to the internet. This makes them easier to handle, but it also gives hackers more ways to get in. Another issue is getting in without permission. Weak passwords, viruses, and unsecured networks make it easy for hackers to get in. Some SCADA communication systems don't have strong security either, so attackers can send commands straight to devices. A lot of people think SCADA systems are secure because they don't operate online or are physically protected, but this is actually not always the case. If these systems are attacked, it may lead to big problems like electrical outages or water system malfunctions.

How SCADA Helps Reduce Risks

SCADA systems have some downsides but they also make things safer. One way is to watch it in real time. This means that the system is always looking for problems.
SCADA systems can also act on their own. For instance, the system can fix it right away if the pressure gets too high, without having to wait for a person.

Krystiana lee
Professor Duvall
CYSE 200T
April 8, 2026
They also send alerts when something occurs wrong so that operators can act quickly. Which helps keep things from getting worse.
Firewalls and VPNs are two examples of security tools that SCADA systems can use to keep out people who shouldn't be there. They also keep track of data. Which helps businesses find problems and make security more effective over time.

Conclusion

In conclusion, critical infrastructure systems are essential but can be hacked. SCADA systems are a big part of both making these risks and lowering them. Hackers can attack them, however they also help keep an eye on systems, send alerts, and fix problems. To keep important services safe, it is very important to make SCADA security better.

References

https://www.fortinet.com/resources/cyberglossary/scada-and-scada-systems
https://docs.google.com/document/d/1VnMlL2YmcW5Jg4MdDa1dt5fJpmQM0KVH/edit