Alissia Metcalfe

Course: CYSE 200T #28058

Professor: Al Kinoon

April 12, 2026

SCADA Systems Key Vulnerabilities

SCADA (supervisory control and data acquisition) systems are used to control infrastructure processes. They are critical components of industrial control units. It controls the entire site linked to human machine interfaces (HMI) that are controlled by human operators. Although SCADA systems improve operational efficiency, their connectivity to networks have made them exposed to cyber threats such as computer worms (Stuxnet) and DoS denial of service attacks.

One of the major components to the SCADA systems that make them vulnerable to cyber threats is the outdated software they run on. One being Legacy systems, many SCADA systems rely on Legacy hardware and software that are not updated to mitigate cybersecurity risks or protocols. Hardware includes PLC (programmable logic controllers) and RTU's (remote terminal units) both lack in modern updates. Software includes Windows XP/7 or Factory/Link, Wizcon and early Genesis/TheFix. They are mainly unsupported in not secure due to their lack of compatibility with modern cybersecurity tools.

Another problem found in SCADA systems is their delayed detection of intrusions. An example of this is the U.S attack on Iran's uranium enrichment facility. The U.S targeted Iran's SCADA systems launching a Stuxnet worm that infiltrated their systems. The virus once in the system went undetected for several months. This virus caused SCADA systems within the facility to physically break while sending false (normal) readings to operators. Therefore, it was able to stay undetected.

Improving SCADA systems in ways such as disconnecting them from networks, implementing multi-factor identification, user role-based access, securing communication and most of all updating hardware and software to be compatible with cybersecurity tools used to mitigate the vast growing threats of today. By addressing and updating these vulnerabilities would not only help companies mitigate cyber threats but make the recovery process quicker and more efficient. Helping ensure the resilience and security of these critical infrastructures.

References

- NIST SP 800-82: Guide to Industrial Control Systems Security
- Http://www.scadasystems.net SCADA Systems