Sergio Hunter

Professor Kirkpatrick

CYSE200T_14936

20 September 2026

Write-Up: SCADA Systems

Supervisory Control and Data Acquisition, also known as SCADA, "is a system of software and hardware elements that allows organizations to control and monitor industrial processes by directly interfacing with plant-floor machinery and viewing real-time data (Inductive Automation, 2026)." This includes processes involving water treatment, gas pipelines, airports, ships, manufacturing, and power generation. SCADA systems are very important in managing industrial operations because they help process data from machinery and connecting infrastructure which will help maintain efficiency, mitigate any potential operations downtime, and allow professionals to make informed decisions when it comes to facility operations.

There are a few subsystems that are usually present within SCADA systems: a supervisory system that gathers data about a process, a human machine interface that professionals use to read processed data, remote terminal units that are used to convert electrical signals from equipment into readable digital values, programmable logic controllers that are used to automatically control and carry out machine functions, and communication infrastructure that connects remote terminal units to the supervisory system. Each subsystem works continuously with each other to provide accurate machine operation data and infrastructure process data to professionals. SCADA systems are utilized in a multitude of industries these days like healthcare, water management, and transportation. For example, in healthcare you can find SCADA systems working to monitor air quality across different hospital rooms, automatically

switch to emergency power in the event of a loss of grid power, monitor medical gas lines for any inconsistencies or issues, and so on.

SCADA systems are not immune to security issues. It is possible for SCADA systems to be tampered with by unauthorized parties. Two of the more common risks associated with SCADA systems are outdated operating systems and insufficient network segmentation. An outdated operating system can be very problematic because they could have unpatched vulnerabilities that an individual can exploit to introduce malware into these critical systems. Insufficient network segmentation can be problematic as well because "A flat network architecture allows attackers to move laterally across systems once they gain access, increasing the potential impact of a breach (Amos, 2025)."

A well-known example of an attack on a SCADA system is Stuxnet. Stuxnet was introduced to Iran's Natanz nuclear facility via an infected USB flash drive being plugged into one of the facility machines. Once plugged in, it was able to spread across the Windows devices in the facility and searched for a software that managed PLCs connected to uranium enrichment centrifuges. Stuxnet then modified the code on the PCLs causing the centrifuges to rapidly speed up and slow down, causing extreme mechanical wear on the rotors and causing them to fail. Stuxnet caused almost 20% of Iran's nuclear centrifuges to be destroyed, setting Iran back in its pursuit of nuclear power.

While this attack didn't take down infrastructure meant for civilian use, one can imagine how bad it would've been if Stuxnet was used to cripple something like Iran's power grid. If there was a malware that could completely cut off a country's power grid, it would leave citizens and organizations of that country in disarray. Hospitals may not be able to provide aid to those who rely on powered equipment, water systems may not be able to provide sanitary water for

people to use, and things like food and medicine could spoil due to not being stored properly. It would be very detrimental even if the outage was only for a short period of time.

There are some ways organizations can improve security regarding SCADA systems. Making sure operating systems are updated when necessary is important for addressing any vulnerabilities associated with outdated software. Each organization should have a procedure in place to ensure that systems are updated regularly and don't interfere much with daily operations. Designing and implementing network segmentation is important for mitigating risks and breaches within an organization. Things like properly configured firewalls, intrusion detection systems, and demilitarized zones will help contain any potential threats that are trying to access critical systems. Continuous monitoring practices should be a priority for any organization to prevent any unsuspected threats that may not be well known yet. Establish an incident response plan and make sure to review and update accordingly.

References

C. Kirkpatrick (n.d.). *SCADA Systems*. Google Docs. Retrieved on September 20, 2026. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0#heading=h.7piv6i8samcb

Inductive Automation (2026, June 30). *What is SCADA, Who Uses it and How SCADA Has Evolved*. Retrieved on September 20, 2026. https://inductiveautomation.com/resources/article/what-is-scada#supervisory-control-and-data-acquisition-scada-explained

Z. Amos (2025, March 21). *9 SCADA System Vulnerabilities and How to Secure Them*. Automation.com. Retrieved on September 20, 2026. https://www.automation.com/article/9-scada-system-vulnerabilities-and-how-to-secure-them

D. Kushner (2025, June 20). *The Real Story of Stuxnet*. IEEE Spectrum. Retrieved on September 20, 2026. https://spectrum.ieee.org/the-real-story-of-stuxnet