Kennice Balmoria
Professor Umphlet
CYSE200T
04 April 2026

According to the SCADA Systems Article, SCADA uses parts like RTUs, PLCs, HMIs, and communication networks to keep everything running smoothly. Supervisory Control and Data Acquisition systems are the computers that help people monitor and control big, important machines in places like water plants, power stations, and factories. They collect data from sensors, show it to operators through screens, and allow people to make adjustments when needed. The article also explains that people often assume these systems are usually safe simply because they're physically secured or "disconnected from the Internet," even though modern SCADA now uses standard networking, which increases exposure to cyberattacks.

According to CISA, the United States has 16 critical infrastructure sectors that are considered "so vital" that their disruption would seriously affect national security, the economy, or public health. Critical infrastructure is attractive to attackers because society depends on it for basic needs, and disruptions can cause major harm. Even with these risks, SCADA applications help reduce the danger by providing real-time monitoring, alarms, and centralized visibility so operators can quickly spot unusual activity. Newer SCADA setups use backup hardware, industrial firewalls, VPNs, and whitelisting to block unauthorized changes. Together, these tools make it easier to detect problems early and keep essential services running safely, even when cyber threats are present.