Bryan Gregg
CYSE-200
Cybersecurity Technology and Society

Strengthening Our Defenses: SCADA and Modern Cybersecurity

Introduction

Critical infrastructure systems are too important and too vulnerable to operate without strong oversight. These systems run our power grids, water plants, pipelines, and transportation networks, yet many of them rely on outdated technology that leaves gaps for attackers to exploit (CISA, 2024). SCADA applications are necessary. SCADA provides real-time visibility, warnings, and control needed to catch problems early. If we want to protect our communities and keep essential services running safely, we must demand that SCADA and similar applications be used across all our systems.

Function and Purpose of SCADA

Supervisory Control and Data Acquisition (SCADA) is the system that oversees major operations like water plants, power grids, pipelines, factories, and transportation networks. It monitors equipment that runs machinery and alerts operators when something needs attention (U.S. Department of Homeland Security, 2023). Through the Human–Machine Interface, operators can see real-time data and make changes when problems occur. Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) gather data, carry out commands, and make quick decisions. All this information moves across wired, wireless, or internet-based networks. SCADA also stores key data points, like temperature and pressure, with timestamps so operators can review previous activity. Over time, SCADA has evolved from isolated systems to modern, internet-connected networks (CISA, 2024).

Why SCADA Security Matters

Because SCADA controls essential services, it is a major target for hackers. Many essential services and systems rely on old technology that was never designed with cybersecurity in mind. Connecting these systems to the internet or corporate networks creates openings for attackers to slip in, steal data, and disrupt operations (CISA, 2024). Even small issues like weak passwords or outdated software can lead to serious consequences such as power outages, contaminated water, or damaged equipment.

SCADA helps reduce these risks by acting as the system's supervisor. It gives operators real-time visibility, alerts them when something looks wrong so prompt action can be taken before problems escalate. Modern SCADA adds stronger protections including encryption, authentication, and alarms that detect unusual activity (U.S. Department of Homeland Security, 2023). It provides monitoring and early warnings needed to keep essential services stable and protect our communities.

The Future of Infrastructure Security

Project Glasswing is a new cybersecurity effort designed to find and fix software weaknesses before attackers can exploit them. Named for the transparent-winged glasswing butterfly, the project aims to increase software visibility and reveal the weaknesses that attackers exploit. Aaron Larson's article, *Project Glasswing: What Power Companies and Grid Operators Need to Know*, explains how this new tool functions to protect power companies and grid operators (Larson, 2026). The project was announced by Anthropic on April 7th of this year. The American AI company and several other tech partners are using advanced AI to uncover hidden vulnerabilities across operating systems, open-source tools, and even critical-infrastructure

software. Its speed and its ability to identify thousands of flaws at once makes it especially important in keeping systems safe.

Project Glasswing also highlights how exposed our infrastructure really is, especially systems built on older technology. AI can now find weaknesses faster than we can fix them, which is a serious concern for power grids, water plants, and pipelines already struggling with outdated equipment (Larson, 2026). When AI-driven attacks can move in minutes, we need SCADA more than ever. SCADA provides real-time visibility, early warnings, and the ability to act quickly. Modern SCADA tools have added encryption and authentication. They can also divide networks into smaller subnets. AI can identify vulnerabilities at lightning speed, and we need supervisory systems that can respond just as quickly to keep essential services stable, safe, and protected.

Conclusion

We cannot afford to ignore the weaknesses in our infrastructure, and we cannot rely on outdated systems to protect the services our communities depend on. SCADA and other applications are essential for keeping these systems secure and responsive. Project Glasswing shows us just how quickly AI can uncover vulnerabilities, and that should push us to strengthen our defenses (Larson, 2026). If we want reliable power, clean water, safe transportation, and resilient public services, then we must commit to fully implementing, maintaining, and securing SCADA and any other tool that helps safeguard our critical systems.

References

CISA. (2024). *Advisory on vulnerabilities in critical infrastructure systems*. Cybersecurity and Infrastructure Security Agency.

Larson, A. (2026, April 11). *Project Glasswing: What power companies and grid operators need to know*. POWER Magazine.

Scada Systems. (n.d.). *Supervisory Control and Data Acquisition*. http://www.scadasystems.net

U.S. Department of Homeland Security. (2023). *Industrial control systems security overview*.