**CYSE 200T Journal Entry 2**

**Write Up: SCADA Systems**

**Taylor Reel**

# SCADA Systems and Critical Infrastructure Security

## Introduction

SCADA systems, or Supervisory Control and Data Acquisition systems, are used to monitor critical infrastructure and industrial processes such as water treatment plants, power plants, gas pipelines, and manufacturing plants. The system collects data from the equipment with the assistance of Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) that send data to a central computer system. Operators are then able to view this data and adjust it through a control interface. SCADA systems basically maintain large, complex processes running and secure by allowing people to monitor what is happening in real time and act as needed.

## Critical Infrastructure Vulnerabilities

Critical infrastructure, like power grids, water treatment plants, and transportation, depends on SCADA systems to keep things running, but those systems have real weaknesses. Many field devices (RTUs, PLCs, HMIs) still use default or weak passwords, so anyone who finds those credentials can get in. Poor access controls also make it easy for an insider or a hijacked account to do damage. On top of that, physical security is often overlooked. If someone can open a control cabinet, plug into a network jack, or get to an HMI that is not properly isolated, they can bypass software protections and directly interfere with operations. These are straightforward problems with potentially serious consequences (Singh, 2020).

Another large vulnerability exists on the cybersecurity front of SCADA systems. Most individuals tend to believe such networks are safe simply because they're physically protected or out of network, but that's not the case at all. SCADA systems control fundamental operations like water supply, traffic lights, power, and gas or oil pipelines, so any breaching could be catastrophic. Threats also include unauthorized access to software through tampering, viruses, or other malware, and network vulnerabilities that permit attackers to remotely transmit malicious commands straight to SCADA devices (Singh, 2020). Protection depends on VPN usage by most operators without realizing that an attacker having physical access to network switches or jacks can evade protection and hijack the system.

## Mitigation Strategies

SCADA systems guarantee that important infrastructure is up and moving, though failure may be very dangerous and cause financial strain. Keeping problems from arising, some systems use rugged hardware that can withstand extreme temperature variations, voltage variations, and vibrations. Many important facilities also use redundant hardware and fallback communications so that when one piece of equipment crashes, the other will take over automatically (Tech, 2023). This setup lets operators replace or repair equipment without interrupting operations, but it also shows how much we depend on these systems, if the backup fails, the results could be devastating.

SCADA programs operate to reduce such forms of threats by going beyond basic network security. Firewalls and industrial VPNs are now designed specifically for SCADA systems, giving operators more control over users accessing the system and what data comes in. Application whitelisting also safeguards against software changes from non-approved sources, which would make it harder for attackers to manipulate control systems. When these controls are

in good standing, they defend SCADA networks against remote attacks and physical attacks, which render critical infrastructure more secure.

## Works Cited

Google. (n.d.). *SCADA systems*. Google Docs. https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0

*SCADA - Tech-FAQ*. Tech. (2023, July 31). https://www.tech-faq.com/scada.html

Singh, S. (2020, April 28). *Biggest threats to ICS/SCADA systems*. Infosec. https://www.infosecinstitute.com/resources/scada-ics-security/biggest-threats-to-ics-scada-systems/?utm_source=chatgpt.com