Nicholas Rossler

Critical Infrastructure Vulnerabilities and SCADA

Critical Infrastructures are vulnerable and attacks on them can be very damaging to those who rely on the infrastructures with even loss of life at risk.

Many think that cyberattacks would revolve around computers and sensitive data that many may have posted online in online transactions. Not many would think about the possibilities of a critical infrastructure being hit by a cyber attack and the events that may come from it. In this paper, the vulnerabilities of critical infrastructure and how SCADA can help mitigate these risks will be explored.

Critical Infrastructures have many vulnerabilities that if exploited can severely impact many individuals. Some of the vulnerabilities include outdated technology, where outdated systems are used in critical infrastructures because they simply work. The problem is that these systems "can be difficult to maintain and keep secure" and these systems are "lacking the latest security software and features" to keep the system secure (Critical Infrastructure). Another vulnerability in Critical Infrastructures is default passwords, because many are focused on ease of use instead of securing technologies, many will use default passwords. This can lead to severe consequences as a default password being cracked can lead to unauthorized access to systems in critical infrastructures.

Some examples of critical infrastructure being hit with cyber attacks are the Colonial Pipeline ransomware, or the Ukraine Power Grid, but another is a water treatment facility in Florida. In this attack in Florida, a hacker was able to get into the systems at a water system in Florida and "increased the amount of sodium hydroxide (lye) in Oldsmar's water treatment system" (Hacker Tries). The bad actor in this attack "increased the sodium hydroxide content

from 100 parts per million to 11,100 ppm" which could have severely impacted those may have drank this water (Hacker Tries). This attack was stopped because a worker was able to see that the levels were increased and reduced back it normal levels without it being a threat to anyone.

Supervisory Control and Data Acquisition (SCADA) are used in infrastructures to control the processes within the infrastructure. SCADA is used in systems to help "control and monitor the entire site, or they are the complex systems spread out over large areas" (SCADA Systems). Because SCADA systems can provide human operators with the statistics of the infrastructure, such as the sodium hydroxide levels from the Florida water treatment incident, it can help operators know when things are going bad at the site. This has increased the security at these infrastructures since operators on site can respond when numbers in the operation are changed by an outside source. However, while it can help provide security, the third generation of SCADA systems today on the internet have also increased the vulnerability of the systems. The use of "security techniques and standard protocols means that security improvements can be applied in SCADA systems" (SCADA Systems).

Critical Infrastructures have vulnerabilities that if exploited can lead to disastrous consequences, such as attempts at poisoning water from the water treatment facility in Florida. While systems like SCADA can help human operators monitor the operations and make sure everything is in line and increase security, SCADA itself still has vulnerabilities along with outdated technology in the critical infrastructures.

Sources:

"Cyber Attacks on Critical Infrastructure: Guide & Risks." *Pelco*, 15 Oct. 2025, www.pelco.com/blog/critical-infrastructure-cyber-attacks#key-vulnerabilities-in-critical-infrastructure-systems. Accessed 12 April, 2025.

"Hacker Tries to Poison Water Supply of Florida City." *BBC News*, BBC, 8 Feb. 2021, www.bbc.com/news/world-us-canada-55989843. Accessed 12 April, 2025.

"SCADA Systems" https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0. Accessed 9 April, 2025.