

Tracey Bernasco

9/20/2026

CYSE200

Chris Bowman

SCADA Systems and Cybersecurity in Critical infrastructure

Critical infrastructure systems are used to provide essential services for businesses and organizations. Many of these systems are reliant on computer technology to collect information, manage processes and monitor equipment either close by or far away. One such device is Supervisory control and Data Acquisition (SCADA). SCADA systems allow organizations to monitor and supervise industrial processes while providing operators with information about the condition of equipment and infrastructure. The concern is how a successful attack against a SCADA system could have massive consequences in not only the organization computer network but also its physical operations and the people who depend on those services. In this document we will be discussing cybersecurity vulnerabilities and the risk associated with SCADA systems.

SCADA systems are used to monitor and supervise physical process and industrial operations. Unlike a tradition computer system that mainly handles information, SCADA systems are connected to physical equipment. This allows organizations to collect conformation about the equipment, monitor operating conditions and make sure that it's running well. SCADA systems use several components to collect and manage physical equipment. Remote Terminal Units (RTUs) connect to sensors and physical equipment, convert signals into digital information and send that to supervisory system. The person that operates the system through Human

Machine Interface (HMI) presents information in a way that helps operators understand what is happening to the system. Because SCADA systems connect computer networks with physical equipment they are used in many types of critical infrastructure. One example of SCADA being used is the energy industry. Power generation and other energy operations require continuous monitoring of equipment and operating conditions. SCADA can help operates with information about equipment and allow them to identify any problems that seem abnormal.

Water and wastewater management is another important application. Water treatment facilities contain various types of equipment such as valves and pipes that need to be monitored and controlled. The benefit of SCADA systems is that that information can be collected and presented to the operators at any time without being there physically. This means that if there was a problem to occur, the operator can quickly identify the problem and dispatch service and maintenance which is integral to the operation process. These of one of many examples of how SCADA can help meld the physical equipment and their operators to make the processes run smoother but there are some problems that need to be addressed.

While SCADA systems provide extreme benefits to critical infrastructure, they also create a cybersecurity risk because they connect computer networks to physical equipment. One vulnerability that could happen is an attack gaining unauthorized access. According to the article, unauthored users may gain access to software and make changes to the system or introduce malicious software. If an unauthorized person gains control they could potentially change how equipment operates or interferes with critical processes. The SCADA systems have improper access control which occurs when the software does not properly restrict access to critical resources. (Ahmed et al., 2022) Another vulnerability focuses on the communication networks used by SCADA devices. Attackers may gain access to network segments where SCADA

devices are located. Some SCADA communication protocols were not originally designed with strong security features, which can make the network traffic vulnerable to malicious threats.

The impact of a SCADA cyberattack could have major consequences for the organization, its infrastructure and the people who depend on these services. Because SCADA systems can monitor physical equipment the attack would take away the availability or damage the equipment. For water treatment system it could disrupt the use of water and systems involving electricity and gas it could have devastating impacts on the people who need them. This adverse reaction could have financial consequences for the organization itself. Because so many people rely on critical infrastructure it's important that organizations maintain their availability and security.

Some of the ways organizations can improve the security and resilience of SCADA systems is controlling who can access SCADA software and networks. Limiting access to authorized personnel can reduce the possibility of unauthorized person making changes to the systems. The assigned reading also shows virtual private networks (VPNS) firewalls and whitelisting as security approaches that vendors used to help protect SCADA environments. Having multi-factor authentication can provide an added layer of security. Strong passwords requirements also make it more difficult for unauthorized users to gain access. (Ahmed et al., 2022) These technologies can help control network communication and restrict control. Another important strategy is preparing for system failures and security incidents. Having organizations.

Overall, SCADA plays an important role in monitoring and managing critical infrastructure and operations. We have identified possible vulnerabilities that could allow unauthorized users to access the system and interfere with operations. Identifying these issues

also shows that organizations can reduce this risk using some cybersecurity tactics and by taking these measures organizations can improve the protecting and resilience of SCADA systems that support critical infrastructure.

References

https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 125, Article 103028.

<https://doi.org/10.1016/j.cose.2022.103028>