SCADA Systems Vulnerabilities

Jordan Morris

Power plants, water treatment facilities, dams, and transportation networks are all examples of critical infrastructure that society heavily relies on every day. In recent years, technology has made it possible to use computer software to increase the efficiency of these systems. Systems like Supervisory Control and Data Acquisition, or SCADA, allow operators to monitor and manage critical infrastructure. While systems like SCADA allow for easier management of necessary processes, they can also be vulnerable if security measures are not in place.

The SCADA Systems article describes SCADA as centralized systems designed to monitor and control industrial and other types of processes. Components of SCADA systems, like Remote Terminal Units and Programmable Logic Controllers, receive data from sensors and equipment on site. The data is sent back to a central location through an HMI or Human Machine Interface. Operators can monitor how the system is running from here and make any necessary changes. By using this system, businesses and industries can monitor their operations in real time.

SCADA systems create opportunities for vulnerabilities. Because many SCADA systems use modern networking technology, like TCP/IP, they are able to be connected to and controlled remotely. However, the article points out that this leaves SCADA systems vulnerable to cyber threats like hacking. If someone were to gain access to a system, they can cause physical components of the infrastructure to be controlled by someone who does not work for that infrastructure. For example, someone could make the water run backward or cut energy

distribution to parts of the city. Infrastructure is an especially important target because it affects so many people.

In addition to the information in the article, the National Institute of Standards and Technology provides information that many industrial control systems were not designed with cybersecurity in mind. This means that these systems lack many defenses that modern computers have. Threats like ransomware, data breaches, and denial-of-service attacks can and have happened on critical infrastructure.

While SCADA systems leave vulnerabilities, they also allow for risk to be mitigated. If abnormalities in the system are spotted early, action can be taken to prevent it from further damaging the system. Alarm capabilities notify operators of dangerous conditions. Systems can also be put in place to backup other systems if they were to fail. Firewalls, virtual private networks, and application whitelisting can also prevent outsiders from accessing private systems. By taking these precautions, critical infrastructure can operate safely.

References:

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