Danielle Caplinger - October 20th, 2024

SCADA Systems & Critical Infrastructure

SCADA systems are integral to running critical infrastructure, but they also play a key role in keeping these critical systems safe.

Overview

SCADA systems, or Supervisory Control and Data Acquisitions, are the systems that coordinate and keep industrial control systems running. Industries including utilities, power, telecommunication, and manufacturing rely on these systems to gather and appropriately react to data going on in their industrial systems. With so many aspects of critical infrastructure relying on these systems, security must be a top priority . This is more of a concern in recent years with the connection SCADA systems have with IoT devices and other IT networks. With all of these new vulnerabilities, SCADA systems must also adapt to stay secure to prevent potentially harmful impacts to communities worldwide (Cybersecurity of Critical Infrastructure, n.d.).

SCADA Systems

SCADA systems are different depending on the industry and specific company that is using them. However, there are a few main components that are in most SCADA systems. These include remote sensors, programmable logic controllers (PLC), remote terminal units (RTU), the supervisory system, a human machine interface (HMI), and the communication network that allows these parts to connect. The remote sensors collect data for a given system which is then collected and processed by the RTU before sending it to the supervisory control system. PLCs

are field devices that help control functions mostly automatically based on either human or data-generated input. Finally, the HMI allows a human operator to see all of this information, usually graphically, and allow them to change controls as necessary (SCADA Systems, n.d.).

Vulnerabilities in Critical Infrastructure

Critical infrastructure is inherently a big target for attackers of all skill levels. They are under attack more than ever in recent years through cyberwarfare techniques around the globe. Industrial control systems and SCADA systems are often the target of the attack in order to disrupt industry operations, potentially limiting critical utilities. These systems were not made with security by design, meaning they often have weak, if any, authentication and encryption protocols. They also tend to use default security settings and passwords that attackers can take advantage of. These systems are also increasingly connected to other IT and OT systems, including those with more IoT devices, meaning there are more opportunities to infiltrate the system (SCADA Systems, n.d.).

SCADA as Mitigation

Although there are many potential threats against SCADA systems, there are also many ways to secure them to protect critical infrastructure as a whole. Network segmentation and firewalls are an important security asset to minimize network traffic and the associated attack vectors. The individual components of any industrial control system should also be kept as secure as possible with MFA and VPNs being used wherever possible. Physical security should also be taken into account with fences, guards, and locks being used to secure the perimeter of industrial environments. Network security monitoring is also essential in SCADA systems; monitors

should be sending alerts for any action taken by a controller or human that is out of the ordinary and logged for later verification (Cybersecurity of Critical Infrastructure, n.d.). There will never be a perfectly impenetrable system, but implementing these controls on SCADA systems will keep them and their industrial systems as a whole as secure as possible.

Conclusion

As industrial systems get more complex and interconnected with other IT systems, security cannot be neglected. SCADA systems play an important role in keeping these systems secure as they are the building blocks to industrial control systems. By implementing some standard cybersecurity practices and using SCADA systems to monitor for unusual activity, industrial systems will be more secure. This means they will be less vulnerable to malicious threats from hackers and state-sponsored cyber attackers.

References

Cybersecurity of Critical Infrastructure with ICS/SCADA Systems. (n.d.) IEEE Public Safety Technology. https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems.

SCADA Systems. (n.d.) SCADASystems. http://www.scadasystems.net.