Name: John Ryan

Date: March 21, 2023

Critical Infrastructure and SCADA

Protecting critical infrastructure is essential to avoid potentially catastrophic effects on society. SCADA systems and other controls can protect against many of the threats, yet SCADA systems themselves may introduce additional vulnerabilities and must be deployed with cybersecurity in mind. Mandatory cybersecurity standards are being implemented, especially in the energy sector.

Critical Infrastructure Sectors

Critical infrastructure is defined as “assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (CISA, n.d.). CISA provides a list of 16 sectors meeting this criteria: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors / materials and waste, transportation, water and wastewater (n.d.).

The energy sector is one of the sectors where more structured attempts at improving security have been made. This effort can serve as an example for other sectors as the industry hurries to improve its security posture.

Emerging Threats to Energy Infrastructure

Threats to the energy sector include natural hazards, technical/accidental hazards, and adversarial/human-caused threats (ICF International, 2016, p. 21). Natural hazards may be increasing somewhat due to climate change, and accidents will always occur, but the most salient threats today are those from people: state actors, non-state actors, other groups, home-grown violent extremists, and insider threats (p. 23). The Stuxnet worm, the attack on the Ukrainian grid, and other documented attacks demonstrate evolving vectors of attack. These threats, coupled with novel kinetic options like drones (p. 23), require vigilance in the application of countermeasures, both physical and cyber.

Vulnerabilities in ICS

Industrial control systems are historically insecure by design. Patching of always-on, critical assets is difficult. The large geographical distribution of systems requires remote access that can be exploited (like Ukraine in 2015) and exist in remote areas where providing physical security is challenging. Smart grids are extending networks into homes and businesses, greatly expanding attack surfaces. Many of these systems have foreign supply chains susceptible to quality control issues or malicious backdoors (ICF, 2016, pp. 39-43). Additionally, current supply chains would struggle at quickly sourcing large power transformers (LPTs), the backbones of the grid, should they be destroyed (p. 14).

SCADA Systems

SCADA, or Supervisory Control and Data Acquisition, systems are industrial control systems used to control infrastructure, facility-based, or industrial processes (*SCADA Systems*, n.d.).

“Nearly all the control actions are automatically performed by the remote terminal units (RTUs) or by the programmable logic controllers (PLCs),” while the SCADA systems translate data from these into information that people can understand and use in decision-making. This information is fed through human machine interfaces (HMIs) where it can be viewed and sometimes acted upon through control elements (*SCADA, n.d.*).

These systems serve two critical functions as they relate to risk: 1) providing near real-time information that can be used to detect incidents, and 2) offering a means of responding to incidents. For example, if a weather event downs a power line, the resulting changes to telemetry will make it known immediately. Circuits may then be diverted to maintain services.

SCADA is a powerful tool for monitoring vulnerable assets and responding to incidents. However, these systems come with vulnerabilities of their own. Historically, they have used proprietary or niche communication protocols and operating systems. There has been a trend lately to move toward TCP/IP and consumer-off-the-shelf (COTS) operating systems like Linux (ICF International, 2016, p. 44). The benefits of having more technical professionals to operate and harden these better-known systems is offset by the ubiquity of the technology and its greater familiarity among hackers.

NERC Standards

The North American Reliability Corporation, or NERC, now enforces a set of standards to protect critical assets. There is, for example, an entire series of cybersecurity prescriptions known as CIP (Critical Infrastructure Protection). Some examples are CIP-007 System Security Management, CIP-010 Configuration Change Management, and CIP-013 Supply Chain Risk Management (NERC, 2023). Each of these details the expected requirements, measures, and

compliance auditing of a cybersecurity domain, not unlike the NIST SP 800 series (NERC, 2023).

Conclusion

Critical infrastructure management is changing as technology evolves. This will both mitigate some vulnerabilities and introduce new ones. The energy sector is working toward navigating this risk with the use of SCADA and mandatory standards. An increased reliance on uninterrupted access to power elevates the impact of any incident, an increased number of active threat actors its likelihood. Continued development and deployment of secure SCADA systems and evolving standards is as important as it has ever been.

References

Cybersecurity and Infrastructure Security Agency CISA (n.d.). *Critical Infrastructure Sectors*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

ICF International (2016, June). *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* U.S. Department of Energy. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

North American Electric Reliability Corporation NERC (2023). *US Reliability Standards*. https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx

SCADA Systems (n.d.). Retrieved March 15, 2023, from http://www.scadasystems.net