SCADA Systems

# Name: Connor Williams

# Date: 11/7/2020

# Details

Supervisory control and data acquisition (SCADA) systems are used for industrial control systems (ICS) that control different types of infrastructures like power plants, transportation, water systems, etc. The SCADA systems are usually composed of Human Machine Interfaces (HMI), Remote Terminal Units, and Programmable Logic Controllers (PLC). The HMI is what human operators use to control and interact with the system processes. The RTUs help to convert the signals from various sensors into digital data. The PLCs and a devices that communicate to the various RTUs, and can be automated to take certain action to keep a SCADA system working. Critical infrastructures are systems that are “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” (Critical Infrastructure Sectors, 2020).

If a SCADA system fails, it could have serious repercussions ranging from simple financial costs, to loss of life or even large-scale disaster. Failures could be a hardware or software issues and could be mitigated through robust software and rugged or redundant hardware. Rugged hardware can be made to withstand extreme temperatures and high voltages or vibrations. Redundant hardware could by a secondary valve or flow controller automatically is switch over to in the event of a primary failure. Software failures are rare as system software is usually thoroughly tested before being released.

Security of SCADA systems is important as they are potential targets of cyber-attacks. While the threat of a physical attack is low, many critical infrastructures have physical security in place to prevent tampering or attack. Most SCADA systems are not directly connected to the internet, so many people believe they are safe. This is a common misconception. The software of SCADA systems appears to be the most vulnerable part of these systems. Systems connected to the internet are exposed to remote cyber-attacks, however even closed network SCADA systems are vulnerable. They could be attacked internally by someone who is allowed access to the software of a SCADA system. The infamous Stuxnet worm is an example of a successful cyberattack on an Iranian uranium enrichment facility’s SCADA system that caused not only system failures, but physical damages (Kroft, 2012). The facility was on an internal network, yet somehow a malware worm was introduced into the system and attacked the vulnerable software. Not only do SCADA systems need physical protections, but they need strong cyber protections.

# References

Critical Infrastructure Sectors. (n.d.). Retrieved November 07, 2020, from <https://www.cisa.gov/critical-infrastructure-sectors>

Kroft, S. (2012, June 4). Stuxnet: Computer worm opens new era of warfare. Retrieved November 07, 2020, from <https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/>

SCADA Systems. (n.d.). Retrieved November 07, 2020, from <http://www.scadasystems.net/>