Carlos Carey

Professor Kirkpatrick

SCADA Systems Write-Up

03 November 2022

SCADA Systems History, Components, Applications, Problems and Solutions

SCADA Systems may not be secure, there are changes being made in order to fix this problem. “In a nutshell, SCADA systems are industrial control systems (ICS) that specifically provide supervisory-level control over machinery and/or industrial processes that span a wide geographical area (such as energy distribution plants)” (*One Flaw Too Many: Vulnerabilities in SCADA Systems*, n.d.-b). Without SCADA systems society would not be where it is today as we are now dependent on these systems and the tasks they perform without human input, however this doesn’t mean these systems are flawless either. In order to understand why we rely so heavily on SCADA systems, we must look into the reason they were created.

History of SCADA Systems

According to Jones (2019), before SCADA systems existed, the industrial sector of business relied heavily on the use of manpower to relay and monitor a machine's systems with analogs and dials. In the 1960s, early versions of automation were implemented in order to alleviate the amount of downtime, but had the downside of the technology being hard to configure and rather bulky. This also meant that the first generation (Monolithic) implementation of SCADA systems were independent as when it was developed as networks didn’t exist. The

second generation (Distributed) allowed the communication between multiple systems through LAN, and the information was shared in real-time. “The protocols used for the networks were still proprietary, which caused many security issues for SCADA systems” (*SCADA Systems*, 2018). The third-generation (Networked) of SCADA systems is what we currently use, and the communication happens through the internet. Vulnerability is increased, however, implementation of protocols and security techniques can be implemented in SCADA systems to reduce the newly created vulnerabilities.

Components of SCADA System

Even though SCADA systems seem rather complex and intricate, especially with the third generation, they allow the operator to oversee and control multiple systems. The system the operator sees all the information displayed on is called the HMI (Human Machine Interface). The HMI presents all processed information in diagrams and graphs which updates in real-time. The supervisory station is what is responsible for communication between field equipment and other systems. Remote Terminal Units (RTUs) are used primarily in remote and isolated environments, however convert signals from sensors into digital data before being transmitted to display, and store the data in a database. Programmable Logic Controllers (PLCs) are versatile, unlike RTUs, and are used in most applications. They communicate with sensors, machines, and other devices to then relay the information back to the supervisory station to be processed. All of this is basically useless without having Communication Infrastructure, as proper infrastructure allows for the relay of information efficiently to a centralized system. This also links PLCs and RTUs to the supervisory computer.

Applications of SCADA Systems in Society

In 2008-2010, American car companies such as Ford, Chrysler, Dodge, and Chevrolet were at the forefront of backlash for deciding to do massive layoffs of workers to replace them with automated manufacturing of vehicles with machines, and hiring programmers to implement SCADA systems to make the cost of producing automobiles cheaper. Pharmaceutical companies use machines that are automated to precisely manufacture prescribed medications as there's statistically less margin for error with a modern machine than a person. According to Anderson (2022, October) SCADA Systems implemented with water treatment plants have allowed for lower costs, more remote control of processes, and more advanced functionality, allowing for a more quality product. All of these implementations of SCADA Systems are examples of it being implemented into what is considered critical infrastructure, as things such as cars, water, and medicine are used daily by billions of people.

Vulnerabilities of Critical Infrastructure

As we continue to develop SCADA Systems, we continue to ignore the protection of these systems which puts nations and people at risk of becoming victims to attacks that could be prevented. The increased exposure, interconnectivity, complexity, common technology, and increased automation are points of vulnerability according to the recent research conducted by Phillip A. Craig jr (Paganini, 2020). Not only that, there are some locations where there may be SCADA Systems that are unguarded or unmanned, which leaves them vulnerable to physical

vulnerability. “According to a Forrester study, 56% of organizations using SCADA/ICS reported a breach in the second half of 2018 through the first half of 2019. Only 11% indicate they have never been breached” (Paganini, 2020).

The reasons for the breach can be linked to multiple issues. According to new research, SCADA Systems often run on Legacy software, have networking issues, are exposed to DDoS attacks, have not changed from Default Configuration, and are even exposed to Web Application Attacks which leaves them vulnerable to even SQL Injection, which is easily preventable (Paganini, 2021).

Mitigation of Vulnerability in Critical Infrastructure

Even though it seems SCADA Systems are the issue, that is not the case. The issue is how we have implemented SCADA Systems and how loosely security was originally tied to these systems. Now that the vulnerabilities are visible and have been exposed, there is now a push for the security of these SCADA Systems as most critical infrastructure is using some form of SCADA System. There would be an incalculable cost if there was a cyber attack against all critical infrastructure across the globe, there are some steps we can begin with to help begin mitigating the vulnerabilities of critical infrastructure.

In order to prevent physical access, you must restrict access to the site. Requiring clearance for the site, and document access will mitigate the physical vulnerabilities. On the digital side, you could implement firewalls, allow virtual patching, prevent unauthorized device

access, employ authorization and authentication (2FA/Biometric), implement endpoint protection, and even something as simple as changing default system settings and passwords can mitigate the vulnerability of some of the systems. Third-party vendors are a security risk too, you must keep track of administrative accounts they have to your systems as well.

You must be able to recover if they manage to get into your system, therefore you should have some form of backup system. Having redundant hardware, fallback mechanisms, and backup procedures in case the other two implemented systems fail. A recovery plan also helps as having offsite data storage could save your company from losing almost everything. Simply keeping systems up to date and having consistently updated records on backup can help tremendously.

Conclusion

As time has gone on, people have begun to realize the importance of protecting SCADA Systems, and their relation with critical infrastructure. “According to a report published by Fortinet, many organizations using SCADA/ICS plan to increase spending on security technologies this year”(Paganini, 2021). Millions, maybe even Billions, of people rely on critical infrastructure every single day for simple necessities such as water, food and medicine. We must be able to protect it or society may simply be brought to its knees. The possible future of war will be on the internet, and they will target water treatment plants, nuclear power plants, and agriculture. Industry as a whole needs to embrace cybersecurity as it is now a problem across the board in every field.

Works Cited

SCADA Systems. “SCADA Systems - SCADA Systems.” *SCADA Systems*, 2018, www.scadasystems.net/.

One Flaw too Many: Vulnerabilities in SCADA Systems. (n.d.). Security News. November 6, 2022, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems

Jones, C. (2019, May 14). *A Brief History of the SCADA System*. The Earth Awards. https://www.theearthawards.org/a-brief-history-of-the-scada-system/

MaintainX. (2022, January 11). *What Is SCADA? | MaintainX*. https://www.getmaintainx.com/learning-center/scada-definition/?utm_campaign=bing-search-non-branded-global

Anderson, M. (2022, October 28). *SCADA Applications in Water Treatment*. PLC Programming Courses for Beginners | RealPars. https://realpars.com/scada-applications/

StackPath. (n.d.). Retrieved November 6, 2022, from https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions

Paganini, P. (2020, October 13). *Improving SCADA System Security*. Infosec Resources. https://resources.infosecinstitute.com/topic/improving-scada-system-security/

Paganini, P. (2021, August 7). *SCADA & security of critical infrastructures [updated 2020]*. Infosec Resources. https://resources.infosecinstitute.com/topic/scada-security-of-critical-infrastructures/