Mark Migdal 11/9/2025
CYSE200T

Scada System and Their Vulnerabilities

In this document, I will cover the basics of SCADA systems and what can go wrong with them.

What are SCADA systems?

SCADA systems, or Supervisory Control and Data Acquisition, are the most typical way of control and data acquisition within critical infrastructure. SCADA systems include RTUs (Remote Terminal Units), sensors, actuators, PLCs (Programmable Logic Controllers), etc. These are used to either collect data about what's happening with critical infrastructure or to control certain aspects of it.

What makes SCADA systems so vulnerable?

All of the small pieces that make up SCADA systems are very simple and made to do basically one job. They typically aren't made with any security in mind because it would significantly alter the part. Also critical infrastructure typically takes many years or even decades to build, so once the build is complete, the tech is usually pretty out dated. Another factor is that all of these small, important, parts are in very difficult places to reach and aren't really made to ever be replaced or serviced.

Why is Cyber Security So Important For SCADA Systems?

If SCADA systems were compromised in any of the United States critical infrastructure it would be catastrophic to say the least. For example, let's say a nation state actor were to get access to some of the SCADA systems for a water company. They could do two major things, either stop water entirely or they could poison water by tampering with the Data Acquisition. Both of these results could cause so much damage, to the likes never seen in the US before.

How To Mitigate The Risks

There are a few options when it comes to mitigating cyber security risks. The first one is making all of the small, simple, parts have more security measures. Now obviously that would completely change everything about critical infrastructure but it's a necessary thing to ensure the safety of the people. Another solution would be making the parts of the SCADA systems more accessible to work on to allow parts to be replaced with more up to date technology.

Conclusion

This paper and many other examples show why it's important to update the security in SCADA systems. They are far too important to be so vulnerable to cyber attacks. I believe that companies are capable of fixing these issues but it will cost a lot of money. Even though it will cost a lot it will be very worth it to ensure that critical infrastructure stays online.