SCADA Write Up

Jadyn Richardson

11/5/2023

Jadyn Richardson

11/5/2023

BLUF/ What is SCADA?

SCADA stands for Supervisory Control and Data Acquisition and is used to help run our critical infrastructure. Although it has its flaws, it still has its own protections from vulnerabilities such as redundancy, ease of use, and updating software.

Redundancy

In short, redundancy is a way for a system to keep on operating if a part of it fails. It is important for systems to have back up options should a vital part of it fails so that the machine can maintain a baseline level of effectiveness while it is being restored to its intended state. One example of redundancy in the SCADA system is that some processes can function without the use of the master computer. This means that if the master computer goes down, there will be other functions that still operate. A quote from an article by SCADA systems says: “Execution of easy logic processes without involving the master computer is possible because of ‘smart’ PLCs or RTUs…”.

Ease of Use

Another way for SCADA to combat security vulnerabilities is through its ease of use. When systems are easy for people to use, it reduces the risk of human error. SCADA makes its systems to use by accommodating for the user. One of the programming languages that it uses is very easy to use and requires minimal training to carry out basic functions with it. The SCADA system article says: “EC 61131-3 has very few training requirements…”. Another way that

SCADA makes systems easy to use is with the way that it collects and presents data. At the end of any process, the way that data is used is up to humans. This means that if the data is presented in an easily digestible way, then less errors will be made, and decisions will be easier to make. An example of SCADA presenting data in an easy way is with the interactive diagrams it shows its users.

Updating Software

SCADA systems, like all other systems, need to be updated regularly to ensure security. As software and hardware get older and older, malicious parties will find ways to exploit those older systems. SCADA combats this by updating their hardware and software regularly in order to keep their security up to date. Adam Stone says that “Most of this equipment has embedded software built into it, and it's the software that runs all of these activities on the hardware and controls the hardware,” Iyer says. “If this software is not updated, you have the risk of cyberattacks (2022).”

Conclusion

In conclusion, SCADA systems are vulnerable to cyberattacks like all other machines in our world today. But SCADA takes as many precautions as it reasonably can which include redundancy, ease of use, and updating software.

Sources

https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit

https://fedtechmagazine.com/article/2022/06/federally-operated-scada-systems-work-block-cyberattacks