Name: Charmi Patel

Date: March 17, 2024

SCADA Systems

BLUF

The SCADA systems was created for industrial control and for other governmental project purposes. With these systems being implemented worldwide they have become important tools to go over certain infrastructures and processes. Even though they have been enhancing from each generation there still is ongoing concerns for security issues that may occur with these systems like cyber threats, etc.

Overview of SCADA

SCADA also known as supervisory control and data acquisition helps control many infrastructure, facility-based, and industrial processes. This includes things like water treatment, airports, or manufacturing. Within SCADA there are many subsystems like the apparatus, supervisory system, remote terminal units, programmable logic controller, and communication infrastructure which helps process, gather, connect data and other signals. The systems of SCADA control and look after the sites and systems through large areas. By acquiring the data, the usage of PLC and RTU levels are needed to measure its status, reports, and readings. From there the control room makes decisions to either override or adjust the normal PLC controls by using the HMI. From inputting the data things like tag databases are used which are sometimes called points. Points help control and monitor the system through soft and hard points. Hard points are known as output and input of the system and soft points require math and logic operations (SCADA Systems).

HMI and SCADA Hardware

HMI also known as Human Machine Interface takes the processed data and sends it to the human operator. HMI and SCADA are both interconnected with one another to retrieve data and any management or trending information. Information can be graphical like diagrams or digital including photographs. HMI includes a drawing program just like how the SCADA system is used by the alarm clocks and include two status points like alarm or normal. This alerts the SCADA operators and managers any text messages or emails when the alarm is activated. With

HMI and SCADA being connected with one another it provides different types of communications with PLC manufacturers or third part packages to configure HMI on its own (SCADA Systems).

SCADA operations, architectures, and methods

At first SCADA used modern connections which initiated the communication requirements which was called telemetry. Those protocols included were IEC 61850, DNP3, etc. which recognized and used by the big SCADA vendors. To retrieve proper communication the usage of PLE allowed better communication from the devices that weren't known to be part of the network. During the early years SCADA was not invented so the usage of mainframe systems was used since networks were not in existence. Then the usage of RTU was developed to help communication to vendors through a wide range of network, but communication through multiple channels and stations was only run through by LAN, but on the other hand there were many security issues due to the protocols being upheld so the usage of WAN protocols was initiated (SCADA Systems).

SCADA issues and trends

Through these systems many security and internet connection concerns has arose. This includes cyberterrorism, cyberwarfare attacks as well. Majority believe that the SCADA networks are meant to be safe since they are not connected through the internet. Since the systems are used to monitor and control multiple processes then if the systems were destructed it would be a negative impact which would leave two threats. The first threat is giving unauthorized access to the software and the second one being allowing packet access to networks that host and are involved within the SCAFA devices. These risks are addressed by developing and creating industrial VPN and firewall solutions (SCADA Systems).

Conclusion

The SCADA system plays an important role in managing and looking after multiple industrial processes, infrastructures, etc. Within these systems are another pair of subsystems like HMIs, RTUs, and PLCss which are all connected within the infrastructure to provide proper communication channels and data retrieval. These systems are meant to process the data and not control them. With the help of RTUs and PLCs proper information is provided through the usage of HMI. These systems have developed through each generation to provide secure protections and enhancements. As always, there are concerns with security issues like being

susceptible to unauthorized access and cyber threats. Even though efforts are being made to bring an awareness to the risks, special VPNs, firewalls, and other important industrial processes and operations are implemented to help enhance communication worldwide (SCADA Systems).

References

SCADA systems. SCADA Systems. (n.d.). https://www.scadasystems.net/