Nicholas Robertson

SCADA system write-up summary

SCADA is a multi-level automotive control system that is used in industrial settings to monitor machine activity.

SCADA Overview

Supervisory control and data acquisition or SCADA is a multi-layered control operating system that is used in industry settings to monitor machine activities throughout a company. It contributes in “gathering real-time data from machines like their operating status, recording events to be placed in a log file so that the company can know what happened on what date, and directly interacting with devices like switches, valves, pumps and motors through human-machine interface software.” (inductive automation, 2018). There are many facets that make SCADA a comprehensive and logical evolution in human automation and if tampered it can have dire consequences. In this write-up we will be discussing what makes SCADA what it is, what are the vulnerabilities associated with infrastructure and how does SCADA mitigate these issues.

Field Instrumentation

Field instrumentation is a term used to describe the terminals, monitors, sensors and other hardware that SCADA uses to monitor the main equipment. It is one of the most important aspects of SCADA, because without it the system would be able to alert the workers if something was wrong with the machinery. These instruments not only work as alerts, but they can also be used to “measure physical properties like whether a machine is on or off, or the level

of fuel in a tank." (Paessler, 2022). Think of it as the eyes of the system, as it sees practically every aspect of the machines and how they currently operate.

Field Controllers (RTUs and PLCs)

RTUs and PLCs work very similarly in that they collect data from the machinery to see if any sensors have gone off and monitor the health of the machine through data collected. After this the data is then sent to the main terminal to alert a worker if there are any problems going on with the machine so they can fix it. At this point the differences between RTUs and PLCs become apparent as RTUs will allow the user to check and solve the problem wirelessly, as it uses "microprocessors to convert data collected from sensors into usable data for the central hub." (Stephen Mokey, 2019). PLC on the other hand has to be directly wired into a workers device in order for them to change or resolve any problems that might be going on with the system.

Human-Machine interface (HMI)

HMI or human-machine interface is a term used to describe the way SCADA implements its data in a more human friendly way. Things like color coding the different levels on terminals to indicate the health of a machine and having the system indicate which sensor, valve or pump needs to be looked at or taken care of would be examples of HMIs. This is a pivotal component of this system, as it not only helps worker know that something is going on with the system and it need to be taken care of, but it also helps with logging purposes, in which case they can go in and detail the issue of what happened on what day and how was it taken care of. This leads to far less headaches and issues in the future.

Network Connectivity

This is a simple one to explain, with any and everything that is connected to the internet the use of network connectivity becomes prevalent. It is essential for SCADA to be connected to networks in order for it to monitor every system connected to it and also relay any information back to the terminals. Network Connectivity can be done in two ways, whether wired or wireless. Most industries tend to use their own private networks to prevent outside sources from poking through the systems.

Database

SCADA takes logs and compiles them into databases in order to keep a record of events that might have occurred with some of the machinery. This is important not only for legal reasons but because if there was an issue that needed to be sorted out at a certain point and time, no one can say that the issue never happened or the system never caught the problem and alerted the staff, because there would be evidence to disprove that statement.

Vulnerabilities and mitigations

Just like with anything that is connected to the internet in some form, critical infrastructure can be vulnerable to attacks. Attacks like phishing emails to put malware or spyware onto a computer of an employee and root though and collect as much data as they can before being caught is always a possibility. When it comes to attacks like that, the only thing that companies can even do is better train their staff to not open suspicious emails. And while SCADA can’t attack malware and/or prevent it from entering its system due to human-errors, it

can help detect it before it becomes too much of a problem. As stated before in the database section, logs are taken of pretty much everything that goes on within the system. So if there are multiple logs throughout the database that says there is a problem going on with the machinery, employees and management can see it fairly quickly and resolve it before it becomes uncontrollable by shutting down operations (which can be done through SCADA). As mentioned before, human-error is something that SCADA can't eliminate, but it is an aspect that SCADA can mitigate with the help of its user interface. With it being easy enough to use and understand, workers will have a better time preventing disastrous outcomes. Intentional sabotage is another attack that would affect large industrial companies, like someone tuning a pressure valve too far, which can cause a pipe to burst. SCADA's sensors would go off and alert though HMI that there is too much pressure build up in this pipe and it needs immediate attention. Production would be stopped, log files would go into the database and cameras would be checked to see if there were any employees at the specific place and time to see if they might have been the cause of that incident. On a more life threatening level, if someone dumped a bunch of chemicals into the water, SCADA can detect the amount of toxins in the water and alert the facility about the issue before too much of it is leaked out to the public.

Conclusion

SCADA is a powerful and highly useful detection system that is essential for industrial corporations. It protects not only their assets, but it also protects the lives of millions of people and assures that production on the foods and products we use and consume on a daily basis is available to us on a consistent basis.

Work Cited: https://inductiveautomation.com/resources/article/what-is-scada

https://www.digitroniklabs.com/blog/scada-components-data-collection-management/

https://www.paessler.com/it-explained/scada#:~:text=Field%20devices%20in%20SCADA%20systems,of%20fuel%20in%20a%20tank.