S.C.A.D.A

SCADA systems are very important for critical infrastructure and are integrated with a lot of systems such as power grids, water treatment facilities, and transportation networks. Critical infrastructure does come with some vulnerabilities but SCADA applications do play a part in mitigating these risks.

Vulnerabilities…

Critical infrastructure has several vulnerabilities and threats that could affect it in minor and major ways. The threats are put into three categories: "natural threats, human based and accidental/technical". Natural threats could be earthquakes, tornados, floods, or tsunamis. Human based could be cyber attacks, rioting or bombing, ect. Accidental/technical are infrastructure failure or equipment breakdown and hazardous material accidents. "Vulnerabilities are characteristics of critical infrastructure that lead to reduction in performance or function as a result of being subjected to categorized threats mentioned above". Overall some common vulnerabilities of critical infrastructure are old systems, lack of security updates, insider threats, weak authentication and third party software or hardware. critical infrastructure systems can be very expensive to replace so a lot of the current systems are older and rely on systems that aren't supported anymore. Which would make them very susceptible to an attack. Along with older systems there might be a lack of security updates which would cause vulnerabilities. People that work in the industry and on these systems can act maliciously and pose a significant threat by using their own credentials to cause damage or steal data. Weak authentication is very possible because some systems can have weak password policies in place which would make it easier for an attacker to steal or manipulate data. Some critical infrastructure systems rely on third party hardware or software which introduces vulnerabilities because the hardware and software could have weak security and be used in exfiltration of the system.

SCADA mitigation…

Even with critical infrastructure systems having vulnerabilities, there are other systems to help mitigate these problems. One of which is SCADA, supervisory control and data acquisition. SCADA is a system that provides control over industrial processes over certain areas like an energy distribution plant. SCADA systems also mitigate risk in critical infrastructure. It provides real time monitoring which allows for quick analysis and identification of potential threats. The system also collects and analyzes the data over time to provide operators a data analysis of trends or patterns that indicate threats or issues. SCADA systems are configured to send alerts and notifications for certain events such as system failures or abnormal readings so that operators take action and prevention measures. In the event operators can perform corrective action SCADA can use automated responses. The system can be programmed to trigger certain actions based on the event or incident. An example would be if an unusually high temperature is detected in a pump in a power plant, it would automatically shut down the equipment to prevent any damage. This is very efficient because even if malware or other harmful software happens to affect the equipment, SCADA has the ability to automatically detect, access and take action.

conclusion

Just like in any system, Critical infrastructure has vulnerabilities. Even with this knowledge, SCADA provides an effective solution for monitoring and controlling critical infrastructure systems which mitigate overall risk involved.

BY: ADRIAN GALVAN

S.C.A.D.A

REFERENCES:

http://article.nadiapub.com/IJCA/vol1_no1/3.pdf

https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems

https://docs.google.com/document/d/1Z2GVYSkvHUTJ37wXJmTlmPQmPnsSTUrV/edit

BY: ADRIAN GALVAN