Devlin Jett

CYSE 200T

March 19, 2025

Professor Duvall

SCADA systems write-up

BLUF: These are some of the vulnerabilities in critical Infrastructure systems and the role of SCADA.

Key Vulnerabilities

Critical infrastructure systems such as energy, water, industry, and transportation increase cyber and physical threats. SCADA systems monitor and control these networks that are especially vulnerable. A big concern inside of cybersecurity are the vulnerabilities. As SCADA systems grow with more networks using TCP/IP, they become targets for hackers using viruses, and illegal access, potentially causing service disruptions and data breaches. Physical security flaws pose a risk because SCADA components such as Remote Terminal Units also known as RTUs and Programmable Logic Controllers (PLCs) are used making them open to manipulation.

Many SCADA networks continue to rely on old systems and protocols with no active security measures, making updates difficult. The lack of authentication and other methods to prevent data breachers in earlier SCADA systems made them vulnerable to data interception and manipulation. Weak network segmentation lets attackers move laterally within unsegmented SCADA networks without getting caught, raising security concerns and the potential effect of cyber threats.

SCADA's Impact on Risk Mitigation

SCADA systems serve a critical role in infrastructure monitoring their control, and security. They decreased the risk by acquiring and processing data from field devices in real time, allowing for quick identification and automated threat responses. In addition, warning and notifying the systems alerts operators immediately when security breaches or equipment problems occur. To ensure that the protections are fully operational and well protected, backup systems are in place to put in place failover mechanisms in the event of a cyberattack or technical breakdown. Encryption, authentication, VPNs, and firewalls all contribute to increasing security protections by preventing unauthorized access into the systems.

Best Practices for Improving SCADA Security

According to CDW, SCADA security discusses ways for mitigating hazards. Vulnerability management, which includes frequent monitoring and patching of SCADA setups, helps to prevent exploits inside of the system. Password and access control measures, such as strong password restrictions forcing people to make stronger and more unique passwords, and privileged access management, prevent unauthorized access to the system.

Additionally, application control confirms that only approved software is allowed to operate within the system, preventing dangerous malware from infecting it. Another method is network segmentation, which limits access between SCADA and IT networks, reducing attack surfaces and lowering the chances of a cyber-attack on the system.

Conclusion

SCADA systems are a crucial key to protecting important infrastructure, however vulnerabilities because of outdated technology, raises the chance of cyber-attacks, and physical concerns exist. Encryption, segmentation, authentication, and redundancy are critical security measures. Implementing the best practices such as vulnerability management, application control, and network limits improves the security measures, guaranteeing that SCADA programs provide effective protection against developing cyber threats.

References

https://www.cdw.com/content/cdw/en/industries/it-solutions-oil-gas-industry/scada-security.html?cm_ven=acquirgy&cm_cat=bing&cm_pla=SGMT+Energy+Utilities&cm_ite=Oil+Gas+SCADA+Security+B&s_kwcid=AL!4223!10!73942298712697!!!!73942264038136!!52849111!1183075128129754&ef_id=99e844b909e71d3a09382358d5152a48:G:s&msclkid=99e844b909e71d3a09382358d5152a48 (CDW link)

https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0 (SCADA systems doc)