Derek D. Hillman SCADA Systems
04/06/2025 Vulnerabilities

Modernized SCADA systems are used in a plethora of industries today. They are used in our local energy companies, water plants, subway stations and more. SCADA systems are a system of systems utilized as an administration tool for critical infrastructure administration systems. Just like any other web connected device SCADA systems are vulnerable to cyber-attacks as well. I will explain some of the following vulnerabilities that these systems may have.

It is increasingly becoming more common for IoT devices to be utilized within SCADA systems and the issue with that is IoT devices a very vulnerable to intrusion. IoT devices are generally small items with a small footprint of printed circuit boards which do not have the capacity for high levels of encryption and other security features that other Information technology systems have. This leads to having a weak point in a systems infrastructure. These devices are usually connected to more secure systems, so it creates an easy and logical way threat vector for a novice threat actor to invade one’s network. Another issue is the complexity of these systems in large data centers. It can be easy to forget to misplace one of these small devices on an inventory list. “48% of security leaders pointed to the complexity of their IoT ecosystem as the biggest challenge “(Ożarowska, I. 2024, April 6)

As time progressed so did the SCADA systems landscape. When these systems were introduced to industry most of these systems were stand-alone air gapped systems. This stature provided a good level of security since these systems weren’t all interconnected. The blast radius of an attack could be contained just to a small subset of systems. Today’s SCADA systems are now available through the open internet which increases the risk of an intrusion immensely. When systems are internet facing the TCP/IP communication protocols are vulnerable to the plethora of network attacks etc.

In conclusion SCADA systems are just as vulnerable as most other Information Technology systems in today’s Cyberspace. It is another layer of technology that the world's researchers and cyber analysts should be mindful of since a lot of our infrastructure utilizes these systems today.

References:

Ożarowska, I. (2024, November 27). *Most common IoT security issues and how to prevent them*. Spyrosoft. https://spyro-soft.com/blog/industry-4-0/most-common-iot-security-issues-and-how-to-prevent-them?utm_source=google&utm_medium=cpc&utm_campaign=Industry_DS&utm_term=c_&utm_content=Financial_blog&utm_creative_format=search_dsa&utm_marketing_tactic=tofu&gad_source=1&gclid=EAIaIQobChMI5bilxYrEjAMVjCZECB27IAS4EAAYASAAEgICQfD_BwE

SCADA systems. (n.d.). http://www.scadasystems.net. Retrieved April 6, 2025, from https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit?tab=t.0