Frederick Gervacio

Christopher Bowman

CYSE 200T

12 April 2026

SCADA Systems

Critical infrastructure systems (CIS) can be victims of serious vulnerabilities, including outdated systems, insufficient maintenance, outdated security protocols, and unpatched software. The principal cause for these issues to be exploited is due to unauthorized software access due to viruses or malicious packets that are used to attack the network. By implementing supervisory control and data acquisition system provides some relief in improving the protection against these risks, as it uses modern security controls like advanced monitoring, network segmentation, and adaptation of regulatory cybersecurity frameworks. With Network segmentation, this means that by dividing the network and isolating certain areas to be accessed only directly at the location it increases security. With the implementation of advanced monitoring and regulatory cybersecurity frameworks it increases the reaction time against attacks and reduces the threat levels and the impact of the damage.

Critical infrastructure systems (CIS) are implemented in sectors such as energy plants, water treatment facilities, healthcare, and transportation. These sectors are heavily dependent on industrial control systems (ICS), which are known for prioritizing the

continued operation of the systems. This basically means making sure that the systems are operational 24/7, places a heavier burden to make sure that the necessary updates and security patches can be performed on time. This can lead to causing vulnerabilities over time that can be exploited by hackers or enemy countries.

SCADAs tend to run on outdated systems and/or unpatched software which can create significant vulnerabilities due to the necessity of having the critical sectors running and not causing disruption. To implement updates on older equipment can be challenging, as the updates might no longer be supported. If the system can be updated this creates gaps in the security that leaves the network open to threats and impossible to protect. By simply shutting down the network and implementing new and more advanced equipment that can keep up with the security demands and all the ever-changing threats, it is the only way to protect these critical infrastructures.

Network segmentation can be implemented using Demilitarized Zones (DMZs) and internal micro-segmentation that creates a division of network for Internet of Things (IoT) devices and the Industrial Internet of Things (IIoT). By establishing this division of network between the different devices that has proven to be vulnerable to attacks it will increase the security of the systems. The Industrial Internet of Things that are managed by SCADA need to communicate on a separate network to regular IoT devices like security cameras, badge system, and many others.

By combining continuous monitoring, anomaly detection and machine learning tools can create a better understanding of the traffic that goes on the network and adapt better to

identified traffic anomalies. With machine learning tools the systems adapt faster to response to threats and identify zero-day attacks.

The new SCADA systems enable the adaptation of regulatory cybersecurity frameworks, the division of the network to avoid access from external attackers, the ease of implementation for updates to critical systems with minimal downtime and interruption of the CIS. These changes can take time and can be costly to implement, but in the long run it will pay off as it will reduce the threat that leaving old and outdated system in place can cause.

Links used for data:

https://eiscouncil.org/how-critical-infrastructure-vulnerabilities-stall-businesses/

https://www.micromindercs.com/blog/critical-infrastructure-threats