

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control important parts of infrastructure such as water systems, power grids, and industrial processes. According to the SCADA article, these systems depend on components like programmable logic controllers (PLCs), remote terminal units (RTUs), and human-machine (HMI) to collect data and allow operators to make decisions. These systems are made to control processes over large areas and keep an eye on things in real time to help keep things running smoothly and avoid any problems (SCADA Systems, n.d.).

The article talks about one major liability: modern SCADA systems are now linked to networks and even the internet. While this does make communication and productivity better, it also paves the way for cyberattacks to take place to inflict harm. The article claims that there are two main threats: people accessing systems without permission and attacks over the network that lets attackers send harmful data to SCADA devices. Sometimes, communication protocols do not have much or any security, which makes it even simpler for attackers to take control (SCADA Systems, n.d.). These weaknesses display how vital it is to protect critical infrastructure so that it does not become a target.

Social science plays a vital role in cybersecurity because it is not just about technology; it is also about how people act and what they know. According to Ghaleb and Pardaev (2024), halting cybercrime depends on what employees do, how much they trust management, and the culture of the organization. If employees are not properly trained, they could unknowingly make systems less secure. This is an example of how people can directly affect system security (Ghaleb and Pardaev, 2024).

SCADA systems also help alleviate risks by letting operators see what is going on and receive alerts in real-time, so they can attend to any problems in a quick manner. However, these weaknesses can damage communities that are already at a disadvantage. For instance, if a cyberattack knocks out the power grid or water systems, communities with low-incomes may have a harder time getting back on their feet than people with medium or high incomes because they have fewer resources. This shows that cybersecurity is both a technical and social issue, especially when you think about how some people do not share the same access to support systems.

Hence, SCADA systems are needed to keep infrastructure running, but they do come with some major security issues. To better protect all communities, it is essential to equally make systems safer and raise people's awareness on the matter such as increasing training among individuals and improving the overall work environment. (Ghaleb and Pardaev, 2024).

Reference:

- Ghaleb, F. A., & Pardaev, A. (2024). *Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management.*

- *SCADA Systems. (n.d.). Retrieved from <http://www.scadasystems.net>*