Cyber Threats and Vulnerabilities in Industrial Control System

Ankita Gupta
Symbiosis Institute of Technology,
Pune Campus,
Symbiosis International
(Deemed University),
Pune, Maharashtra,India
ankita.gupta.mtech2023@sitpune.edu.in

Pritesh Shah
Symbiosis Institute of Technology,
Pune Campus,
Symbiosis International
(Deemed University),
Pune, Maharashtra,India
pritesh.shah@sitpune.edu.in

***Abstract*—Industrial Control Systems (ICS) are specialized systems used in critical infrastructure, such as highways, tunnels, railways, electric utilities, water management, and mobile networks, to automate industrial processes. These systems comprise various control systems, including sensors, controllers, and networks, which work together to control and automate processes. ICS is primarily used in transportation, utilities, and communication systems, ensuring efficient and safe operation. However, ICS faces several cyber threats, including a shift in focus toward Operational Technology (OT), which directly manages and controls physical processes. Government and private entities owning critical infrastructure are at high risk of cyberattacks, which can lead to severe consequences, including loss of life and significant economic damage. Misuse of ICS can result in data manipulation and physical damage to infrastructure, causing harm not only in the virtual world but also in the real world, affecting people's lives and well-being. ICS are crucial for the smooth operation of critical infrastructure, ensuring services like electricity, water supply, and transportation function properly. The proper functioning of ICS is vital for public safety and national security, and protecting them against cyber threats is of utmost importance.**

***Index Terms*—Industrial control system, Cyber threats, Vulnerability analysis, ICS Security, Operational Technology,**

I. Introduction

Industrial control systems are primarily used to handle many essential infrastructure activities such as power supply systems, water management, oil, transportation, manufacturing, etc. ICS was initially meant to function with specific protocols and hardware tools without security concerns. ICSs are becoming more integrated with the Internet of Things, and this growth necessitates an increase in the risk of cyber attacks and vulnerabilities in ICSs [1]. Threat actors target several types of ICS to perform cyber attacks, including

- SCADA (Supervisory Control and Data Acquisition) is a system that processes and collects data from control systems that operate at a higher level and across long distances. Pipeline systems and microwave transmissions are examples of SCADA.
- Distributed Control Systems (DCS) are systems of specifically built computers, controllers, and sensors that are distributed across industrial operations. Chemical facilities and nuclear power plants are examples of uses.
- Industrial Automation and Control Systems (IACS) are a collection of electronic, mechanical, and electromechanical devices that perform functions such as controlling, monitoring, and actuating logical equipment. It also provides data in real time. Autotransformers and motor controllers are two examples of uses.
- PLCs are electronic devices that perform a variety of operations such as input/output control, three-mode control, counting and timing mechanisms, sequential control, and an intuitive programming interface. Escalator and lift operations are some examples of uses.
- Safety Instrumented Systems, or SIS, are utilized in industries to provide safety duties. It is a hardware

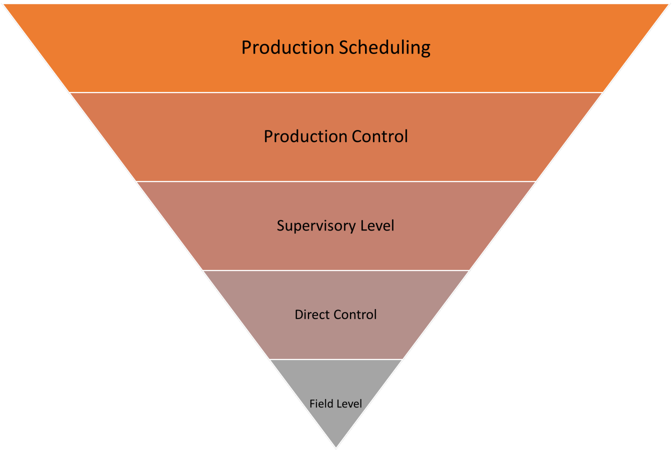

Fig. 1. Functions Of Manufacturing Control Levels

and software-based control system that offers protection whenever a dangerous state is recognised.

- Remote Terminal Units (RTUs) are industrial control systems that use microprocessors. These link diverse devices to control systems electronically. Air traffic equipment is one example of an application.
- Human Machine Interfaces (HMIs) are information exchange devices that use hardware and software to convey data between humans and machines or computerised systems. Centralised control rooms are an example of such application.
- Intelligent Electronic Devices (IEDs) are a grouping of electronic devices containing microprocessors, such as circuit controllers, that perform a variety of duties such as power monitoring, control, and metering. Sewage treatment plants and food processing industries are two examples of uses.

A. *Cyber Threats*

Bot networks, Attackers, Criminal organizations, Foreign intelligence systems, Phishers, Insiders, Spammers, Spyware, Malware, Terrorist groups, and Industrial spies are common cyber threat vectors. These threat sources render the ICS entirely exposed and exploitable. Spoofing, Data tampering, Disclosing Data, Denial of Service, and Privilege Escalation are five types of cyber threat vector assaults on ICS protocols. Spoofing is the act of stealing data by impersonating someone else. Data tampering is manipulating data by accessing unauthorized files. Disclosing Data is the act of hackers breaching data without permission, Denial of Service makes devices unavailable to intended users, and Privilege Escalation allows hackers to gain unauthorized privileged access within the system. Cyberattacks are becoming more complex and are aimed at a variety of industries, including petrochemicals and oil, energy businesses, and industrial control systems. Among the most notable assaults was the 2010 Stuxnet virus, which was created by Israeli and US intelligence and effectively attacked Iran's nuclear plant. Other noteworthy assaults include the Shamoon malware attack in 2012, which targeted major energy businesses including Saudi Aramco and RasGas, and the Night dragon malware campaign in 2010, which targeted international oil and petrochemical industries. The ICS virus Triton/Trisis/Hatman attacked Middle Eastern petrochemical complexes in 2017, while the Russian-based gang Sandworm targeted the electrical system of Ukraine in 2014.

B. *Vulnerabilities*

Industrial control systems (ICS) are complicated systems that communicate and operate industrial processes by utilising numerous instruments, controllers, computers, and software. These systems are vulnerable to cyber attacks both within and outside of the control system network. Buffer overflows, unauthenticated protocols, insufficient user authentication, late software adoption, misconfigurations, third-party outsourcing, weak firewall rules, inadequate hardware, insider threats, and no functional backups are all common problems. Buffer overflows are programming mistakes that occur when programmes exceed the buffer boundary, but unauthenticated protocols confirm device connection. Weak user authentication, such as passwords, biometrics, fingerprints, and iris scans, can also be used to exploit vulnerabilities. Inadequate software adoption might result in exploitation and hostile hacking. Misconfigurations, third-party outsourcing, lax firewall rules, insufficient hardware, insider threats, and a lack of backups can all be security risks.

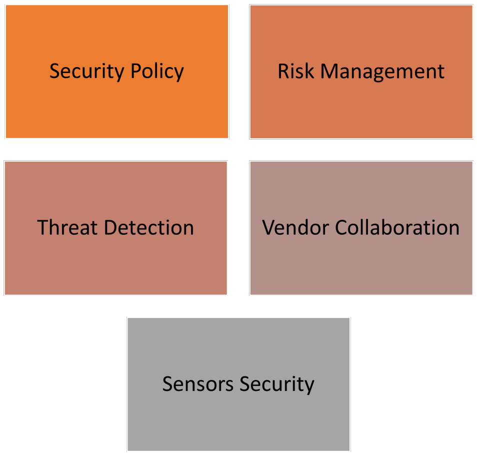

Fig. 2. Solutions For ICS Security

C. *Industrial Control System*

Industrial control Systems (ICS) are vital infrastructure systems that govern and manage physical processes. Cybersecurity is critical for defending against cyber threats and assaults. ICS security, or Operational Technology (OT) security, focuses on securing the technology that directly controls and manages physical processes in critical infrastructure. Asset discovery and management, vulnerability management, network disruption prevention and detection, endpoint detection and response (EDR), patch management, and access control are key components of ICS security. Asset discovery, vulnerability management, and network protection are essential for recognizing and managing possible ICS hazards. Threat detection and response provide rapid identification and reaction to possible threats, reducing the effect of cyber assaults. Patch management inhibits the exploitation of known vulnerabilities, lowering the chance of successful exploitation. Factors for implementing targeted solutions in the ICS environment include Fig 2security policy and procedure audit, threat detection, risk management and mitigation, and resolution of critical security challenges involving intrinsic vendor relationships.

Section II explains the Motivation of this paper, and

Section III explains the Literature Survey. In Section IV, the Methodology is explained. Section V explains the Findings, and Section VI explains the Future Scope. The paper is concluded in section VII.

II. Motivation

The importance of cyber threats and vulnerabilities in Industrial Control Systems (ICS) cannot be overstated. It raises security awareness, informs individuals, organisations, and governments about the dangers of ICS, and has an influence on key infrastructure such as energy, transportation, and water supply. The increasing frequency and sophistication of cyber assaults on ICS have sparked worldwide alarm, and understanding and mitigating these risks is critical for protecting these critical systems. Cyber assaults can have serious real-world implications, such as service interruptions, economic losses, and dangers to human safety. Addressing these risks is crucial for national security because unauthorised access to or manipulation of key infrastructure can have global consequences. As ICS combines new technologies such as the Internet of Things (IoT) and cloud computing, new risks and vulnerabilities develop. Documenting these changes allows stakeholders to remain up to date on the dynamic threat picture. Cyber hazards in ICS present a chance to discuss best practises, effective cybersecurity measures, and technology solutions while ensuring compliance with rules and standards. Addressing vulnerabilities that might jeopardise public safety is likewise critical, as is encouraging continuing research and innovation in the field of cybersecurity.

III. Literature Survey

The research papers on ICS cybersecurity focus on cyber malware attacking behaviors, which significantly affect a nation's national security and economy. [2]They recommend focusing on Industrial Control System (ICS) security and implementing an ICS security framework to protect ICS systems from both internal and external cyber attacks. The ICS security framework consists of procedural security control, operational security control, technological security control, physical security control, regulatory security control, and compliance security control. The Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model is introduced to address uncertainties in managing vulnerabilities in ICS network systems. The model aims to provide a unique way to handle uncertainty in vulnerability management within ICS networks and proposes a methodology for developing security strategies for preventing cyber attacks. The research paper on RowHammer vulnerability, which refers to the failure of Dynamic Random Access Memory (DRAM), surveys the vulnerability and highlights how circuit failures can introduce vulnerabilities in system security. [3] The goal is to enhance the resilience of critical infrastructure against cyber threats, safeguarding national security and economic stability. These research papers contribute valuable insights to the field of ICS cybersecurity, emphasizing the need for comprehensive security frameworks [4], proposing innovative models for vulnerability analysis, and highlighting specific vulnerabilities, such as RowHammer, that can impact the security of industrial systems.

IV. Methodology

Several approaches may be used to highlight cyber dangers and vulnerabilities in Industrial Control Systems (ICS). Penetration testing, vulnerability assessment, security auditing, incident response simulation, threat modelling, Red Team vs. Blue Team exercises, training and awareness programmes, and secure coding workshops are examples of these. Penetration testing is simulating attacks on the ICS to detect vulnerabilities and weaknesses. This includes identifying target components, simulating various cyber-attacks, and documenting weaknesses and probable entry points. Vulnerability assessment include detecting and analysing vulnerabilities in software and network setups, prioritising them based on severity, and suggesting remedial steps. Security auditing assesses the efficiency of security controls and policies by assessing access restrictions, authentication processes, encryption protocols, firewall configurations, intrusion detection systems, and other security measures.Incident response simulation is a way for evaluating an Information Security System's (ICS) capabilities. It entails creating and executing a scenario that simulates a cyber-attack, and then watching how the ICS detects, responds, and mitigates the danger. Threat modelling is used to identify possible risks and attack vectors, which results in the creation of an ICS architectural model. Exercises pitting the Red Team against the Blue Team replicate hostile circumstances, hence improving security mechanisms and educating employees about cyber hazards and best practices through training and awareness programs promoting a security-conscious culture. Secure coding seminars teach developers how to write secure code to avoid vulnerabilities and how to audit existing code for security flaws.

A. Working Model

A primary ICS environment where a cyber threat is introduced at a specific cycle, leading to the manipulation of PLC data and the generation of an alert in the HMI. To demonstrate the basic simulation of the cyber threats and vulnerabilities in the Industrial Control System uses a simulated ICS environment consisting of a Programmable logic controller (PLC), a supervisory control and data acquisition (SCADA) system, and a human-machine interface (HMI) Matlab is used as a working model. The algorithm used for basic simulation describes the PLC that generates random data in normal operation. And at a certain cycle (vulnerability cycle), a cyber threat is simulated by exploiting a vulnerability in the PLC. The

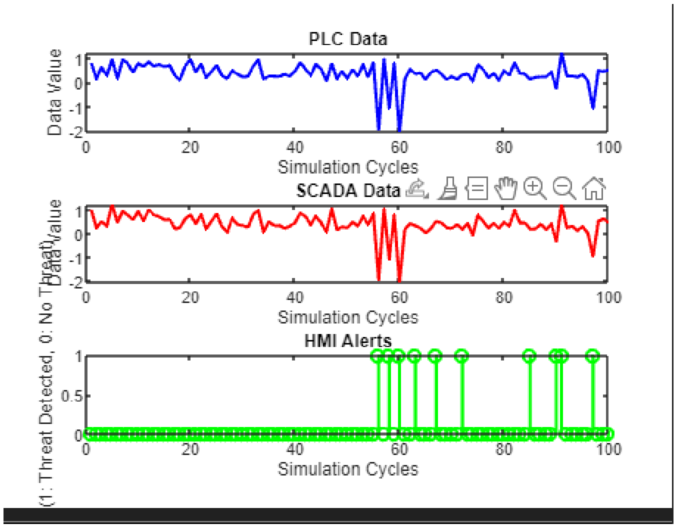

Fig. 3. Basic Cyber Threat Simulation in ICS using MATLAB

exploit's success is determined randomly. If the exploit is successful, the PLC data is manipulated, and an alert is generated in the HMI.

B. Result

The simulation results show that cyber assaults on ICS systems may be successful even when sophisticated defences are in place. Because it directly controls the physical process, Fig 3 the PLC system is the most susceptible, with the greatest number of reported attacks. The SCADA system is less susceptible because it is more insulated from the physical process. The HMI system is the least susceptible since it is primarily used for monitoring and control and does not have direct access to the physical process. To improve ICS security, organisations should implement network segmentation, use strong passwords and multi-factor authentication for all systems and devices, keep ICS software and firmware up to date, monitor systems for suspicious activity, have a response plan in place, and conduct regular security audits.

V. Findings

Since the COVID-19 outbreak, cyberattacks on worldwide Industrial Control Systems (ICS) have expanded considerably, focusing on Critical National Infrastructure (CNI) and utilities. This is most likely owing to adversaries' increasing investment in targeting ICS over the previous five to ten years, which will continue accelerating the ICS threat landscape. ICS devices and protocols may be found in various industries and critical infrastructure, such as manufacturing, transportation, health, energy, and water treatment. Asset owners should invest in network detection-based solutions, secure remote access systems, internet-facing device protection, and other industrial-specific security measures. Supply chain

Government Services
Network Communication
Transport
National Critical Infrastructure
Internet of Things
Trading Services
Healthcare

Fig. 4. National Critical Infrastructure

assaults, such as the Target security breach and the NotPetya ransomware, have also grown in popularity because the COVID-19 pandemic has influenced security threats and cyber-attacks, making it crucial to consider the supply chain of vaccines. Supply chain assaults occur when an attacker obtains access to a system via a third-party supplier or partner, influencing any step of a product's lifetime. Management should focus on reducing adversaries' capacity to disrupt company continuity through supply chain assaults and establishing thorough protocols for rapid and effective incident recovery. Compliance to the PPT Triad (People, Policies, and Technology) can assist in increasing cyber defenses, but the ideal strategy is to add innovation and continual improvement to each aspect in the PPT Triad through process modifications. Malware threats include malware delivered via removable media such as CDs and USBs, insider assaults, and ransomware. Control-system technicians dissatisfied with their jobs can steal credentials, log in to equipment controlling the physical process, and send shut-down instructions to portions of the process, resulting in partial plant shutdowns. Most systems on the industrial control system can be infected with ransomware, producing disturbances in the industrial network. Supply chain assaults pose substantial challenges to enterprises, and management must handle these risks to maintain business continuity and system security. Organizations should proactively establish cyber security governance and risk management to secure a safer future Fig 3. This includes recognizing dangers, keeping track of assets, formulating regulations, and educating employees. Setting up alerting systems, regulating access to regulated places, and deploying firewalls are all examples of physical security measures. Monitoring network traffic, establishing intrusion detection systems, and reviewing audit trails are all examples of security monitoring. Patching and vulnerability management, testing updates, and upgrading old software and hardware are all part of host security. Supply chain management should also prioritize cyber security, invest in safe goods, and maintain the integrity and confidentiality of information.

VI. Future Scope

The fast rise of Internet of Things (IoT) devices has made them vulnerable to cyber-attacks, prompting the establishment of rules and standards to safeguard these devices. These rules must take into account issues such as different devices, communication protocols, resource constraints, Denial-of-Service (DoS) resistance, end-to-end security, unique network designs, bootstrapping a security domain, and operational challenges. [5] Incorporating Artificial Intelligence (AI) and Machine Learning (ML) is critical for improving IoT security. Entities may dramatically increase their capacity to protect sensitive data, prevent cyber-attacks, and minimise business interruption by utilising AI and ML. Quantum security principles in IoT can have a substantial influence on the security of IoT devices and networks. Quantum-resistant cryptographic methods and quantum key distribution can improve the security of data transmission in IoT devices. Access control and privacy can be improved with blockchain technology and contextual information. AI and machine learning can swiftly scan big data sets for abnormalities and suspect activity, alerting network admins. Real-time analysis improves their dependability and makes them less vulnerable to hostile attacks. However, they encounter difficulties in detecting security breaches. Explainable AI and adversarial training can help to solve these concerns by increasing transparency, increasing resistance to cyber-attacks, and boosting performance and user experience.

VII. Conclusion

Cyber threats and vulnerabilities in Industrial Control Systems (ICS) can be identified through various methods such as penetration testing, vulnerability assessment, security auditing, incident response simulation, threat modelling, Red Team vs. Blue Team exercises, training and awareness programs, and secure coding workshops. Penetration testing involves simulating attacks to identify vulnerabilities and weaknesses, while vulnerability assessment involves identifying and analyzing vulnerabilities in software and network setups. Security auditing evaluates the efficiency of security controls and policies. Incident response simulation evaluates ICS capabilities by creating and executing scenarios simulated by cyber-attacks. Threat modelling identifies potential risks and attack vectors, while Red Team vs. Blue Team exercises promote a security-conscious culture. Secure coding seminars teach developers how to write secure code and audit existing code for security flaws. To improve ICS security, organizations should implement network segmentation, use strong passwords and multi-factor authentication, keep software and firmware up to date, monitor systems for suspicious activity, have a response plan, and conduct regular security audits.

References

[1] X. Fan, K. Fan, Y. Wang, and R. Zhou, "Overview of cyber-security of industrial control system," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, pp. 1–7.

[2] U. D. Ani, H. He, and A. Tiwari, "Vulnerability-based impact criticality estimation for industrial control systems," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, pp. 1–8.

[3] M. Wiboonrat, "Cybersecurity in industrial control systems: An integration of information technology and operational technology," in *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, 2022, pp. 1–6.

[4] U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware threat and its impact on scada," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 2019, pp. 205–212.

[5] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review," *Sensors*, vol. 23, no. 8, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/8/4117