Cyber Threat and Vulnerabilities in Industrial Control Systems

ANKITA GUPTA

Industrial Automation

MTech Embedded System Department of Electronics and Telecommunication

Symbiosis Institute of Technology

October 11, 2023

॥वसुधैव कुटुम्बकम्॥

Abstract

- Industrial control systems consist of various types of control systems, instrumentation devices, networks, and controllers used to operate and automate industrial processes.
- In industries, ICS plays a major role by providing industrial automation, networked automation, process optimisation, and process monitoring.
- Due to increasing cyber attacks and vulnerabilities, critical industrial infrastructure owned by the government and private entities is at higher risk, which can cause loss of life and severe economic damages.

Introduction

- Industrial control system mainly used to control large number of operations of critical infrastructures such as power supply systems, water management, oil industries, transportation, manufacturing industries and so on.
- There are various types of ICS that targeted by threat actors to carry out cyber attacks such as: Supervisory Control and Data Acquisition- SCADA, Distributed Control Systems- DCS, Industrial Automation and Control Systems- IACS, Programmable Logic Controllers- PLCs, Safety Instrumented Systems- SIS, Human Machine Interfaces- HMIs and Intelligent Electronic Devices- IEDs etc.

Material and Methods

- ICS security is also defined as Operational Technology security or OT security. Operation Technology security includes wide range of practices to reduce ICS vulnerabilities, these are following;
- Detection of organization list and details of assets its own.
- Vulnerability management of system.
- Network disturbance protection and detection.
- Terminus detection and response.
- Patch management to protect against vulnerabilities.
- Management to access services and resources.

Diagram

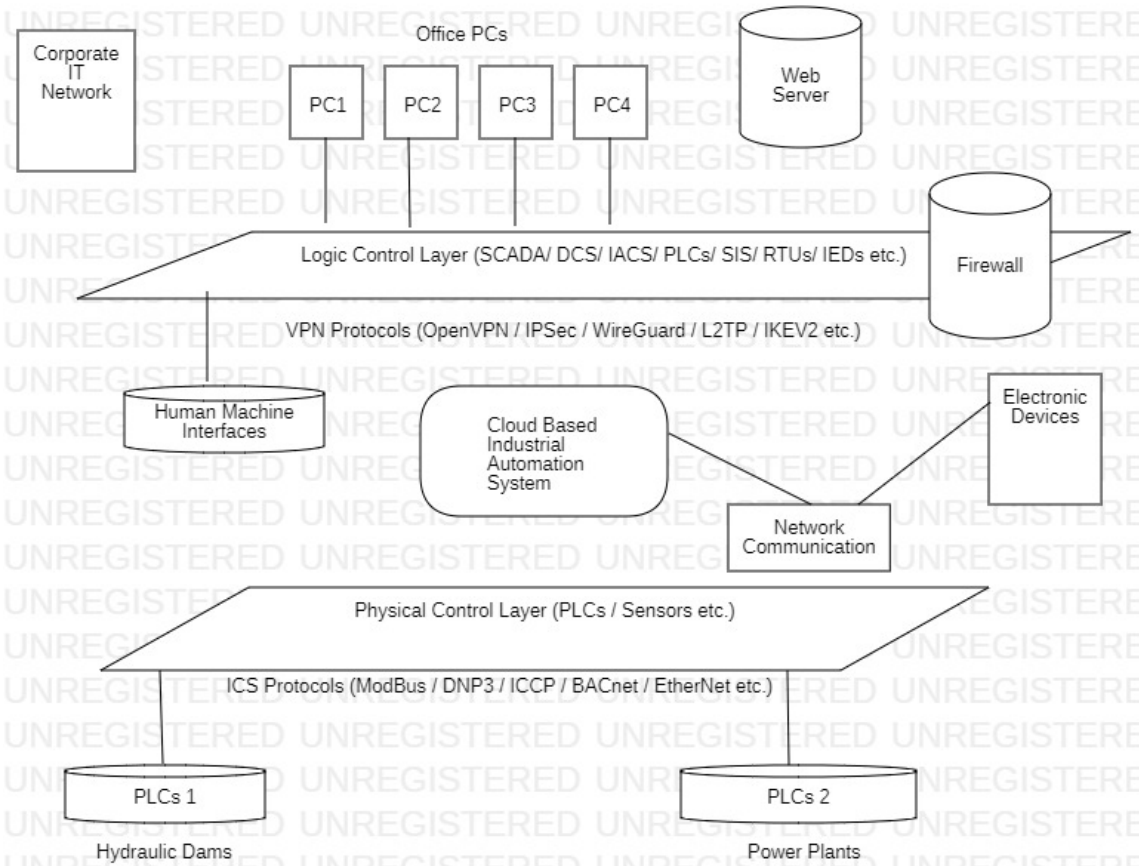

Figure 1: Block Diagram of ICS System

Literature Review

- Mohammad Jbair et al., in their journal "Threat modelling for industrial cyber-physical systems in the era of smart manufacturing," have proposed a structured threat modelling approach for industrial cyber-physical systems that enables the forecasting of cyber risks to protect industrial entities from cyber-attacks.
- Robin Doss et al., in their journal "A Hybrid Cyber Defence Framework for Reconnaissance Attack in Industrial Control Systems," have proposed a bio-inspired adaptive defence mechanism to evaluate the performance of the proposed defence framework in a typical industrial manufacturing network using a software-defined network-based platform and test the defence mechanism in various scenarios.

Analysis of Literature Review

- Developing countries like India alone witness approximately 1700 cyber attack each week on average.
- Most of the countries still not a part of global forums which make other components vulnerable to major cyber threats.
- Creating a global framework by organizations and spreading awareness can prevent system from any hazardous attack.

Stuxnet Attack

- In 2010, a malware Stuxnet developed by US and Israeli Intelligence to target Iran's nuclear facility. Stuxnet successfully targeted Iranian centrifuges.
- Stuxnet also known as first cyber digital weapon. It is basically 500 kilobyte computer worm that designed to attacked programmable logic controller.
- Stuxnet basically attack in three steps: firstly it target windows then asked for software and lastly attacked PLCs.

Solutions

- Before advancement of further industrial revolution some strict security policies are required for any country to protect the critical infrastructure of information as well as operational technology.
- For security of data and systems cyber laws should be provided.
- Automatically encryption and decryption of data whenever it is required by system.
- Securing sensitive systems from any damage.
- Must have a backup solution.

Conclusion

- Some popular ICS attack incidents, like Colonial pipeline ransomware attack, Triton malware attack, Ukraine power grid trojan attack show that the impacts of major cyber-attacks can cause considerable negative effects on other connected components of entire system.
- To represent the concern of advanced cyber attacks before any crucial damage is done to physical system a multi-layer, data-driven cyberattack systems are required to improvise ICS cybersecurity by providing wider attack detection.

References

[1] Mohammad Jbair and Bilal Ahmad and Carsten Maple and Robert Harrison, "Threat modelling for industrial cyber physical systems in the era of smart manufacturing" Journal, 2022.

[2] Xingsheng Qin and Frank Jiang and Chengzu Dong and Robin Doss, "A Hybrid Cyber Defense Framework for Reconnaissance Attack in Industrial Control Systems" Journal, 2023.

[3] Scott Ainslie and Dean Thompson and Sean Maynard and Atif Ahmad, "Cyber threat intelligence, Organizational practice, Research agenda, Intelligence process, Stakeholder management" Journal, 2023.

Question and Answers