International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Cyber Security Framework for Manufacturing Industry with Robotic Process Automation integration

**Murugappan K[1] and T. Sree Kala[2]**

**Submitted**: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

**Abstract.** Cyber Security is becoming one of the business enablers in the current Industry. It is a necessity rather than added item as there were various security breaches that occurred in the past that brought many businesses to their knees. Especially it is a challenge in the Manufacturing industry because of the lack of security consideration in Operational Technology (OT) equipment and its surrounding processes. OT is a hardware and software-integrated platform that shall be used to monitor and control the physical device's operation. A major portion of it is mechanical, and those that use digital controls have closed, proprietary protocols. However now the trend is moving towards smart technology, and convergence of Information Technology and OT is unavoidable. This paves the way for typical cyber-attacks in OT. It shall lead to critical infrastructure damages or malfunctioning, and those results in key services failure, and put human life at risk. Hence in this paper, we explored cyber security requirements in the manufacturing industry, robotic process automation integration and recommend a proposal to build an end-to-end Cyber Security framework.

***Keywords:*** *Cyber Security Framework, Operational Technology Security, Manufacturing Industry IT Security, Robotic Process Automation*

## 1. Introduction

Manufacturing process converts raw materials or components into finished products. This shall involve petroleum, chemicals, textiles, plastics, electronics, transportation, and food processing etc. These are prone to cyber security attacks and impact can be devastating as society is depended on these industries for its various needs. This paper explores the cyber security framework establishment in the manufacturing industry and automation of critical tasks so that cybersecurity attacks avenues shall be mitigated effectively.

## 2. Problem Identification

[3] Past and current cyber events reveal that cyber security attacks on manufacturing organizations are in an uptrend due to the availability of powerful compact computers, easily available free exploits, and internet connections. The intention behind these attacks varies according to the nature of the business these manufacturing organizations are in. For example, one of the household appliance manufacturing companies in New York got hacked, and customer information was stolen. The attackers exploited the loophole in the company website. To quote another event, a state-sponsored attack group compromised another country's nuclear enrichment program, imagine if the same can be used to change the calibration of the controlling mechanism of some hazardous material storage or even change some critical parameters of life-saving saving medical equipment that would cause huge impacts to the society. Hence in this paper, we are proposing a cyber security framework that shall provide a reasonable governance mechanism to protect the critical assets of the manufacturing industry and its processes.

## 3. Proposed Solution

It must consider various elements such as People, Process and Technology. It shall follow the approach as mentioned in the Fig.1. below.

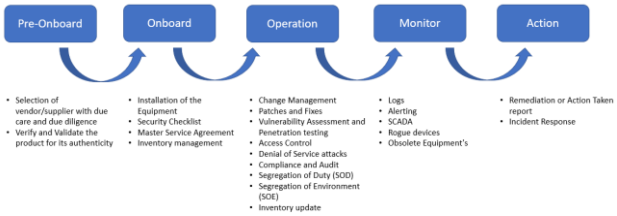


**Fig.1.** Cyber Security Framework Focusing on Operational Technology

### 3.1 Pre-Onboard

**Selection of Vendor:** This is a very important step to ensure that a reliable vendor is selected, and only selected raw materials are used in the manufacturing process. A manufacturing company must perform this with proper due care and due diligence. The diligence shall be done with the help of software bots or also called as robots by exploring various factors involved in the selection process.

**Verify and Validate:** verify that only genuine raw material/ component is received. This shall be done manually or using an automated method. Either way, it must be further validated against the original raw material quality that is agreed upon. This is to ensure that no

forged, duplicated, or malware-implanted materials are allowed in the production environment.

### 3.2 Onboard

**Installation of the Equipment:** Equipment Installation must be done carefully and placed in the respective layer as stated in the ISA-95 standard. This standard supports professionals to streamline processes and improve industry safety, stability, profitability, and efficiency. [2] It classifies production systems into 5 levels as depicted in below Figure 2.

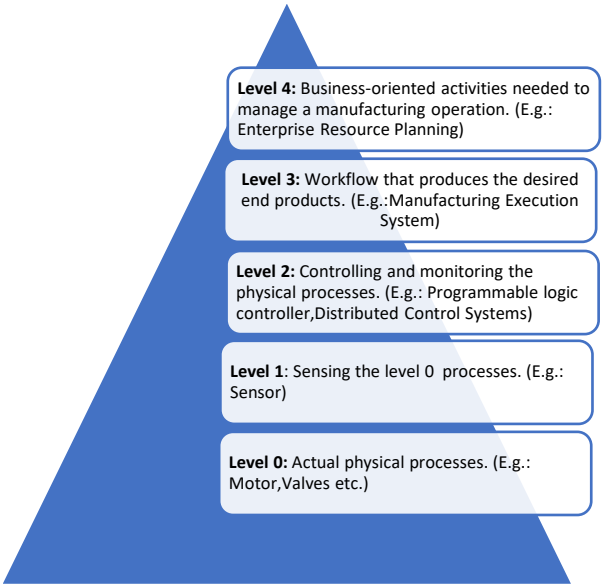


**Fig.2.** ISA-95 Level Diagram

**Security Checklist:** Installation and configuration checklist must be in place while deploying the product to production. This shall include Air-Gap arrangement wherein devices are not connected to network due to its critical nature and operated in standalone mode to avoid remote attacks. Also, communication between ISA-95 standard layers need to be secured with strong protocols.

**Attack Surfaces and Vectors:** There are various avenues available for an attacker to land into the manufacturing environment**.** Since most of the systems are now connected to network, either with internet or intranet the potential avenues are more. Some of them are listed below for reference perspective. These must be addressed appropriately during the onboard stage itself. The Robotic Process Automation shall help in gathering the intelligence from various sources and hunt down the vulnerabilities in the below areas. There are various players in the market to provide an RPA solution and some of them are open-source software's as well.

- Corporate network
- Customer network
- Unsecured virtual private networks (VPNs)
- Uncontrolled internet connection and not known to the Organization IT team
- Unsecured wireless connections
- Malicious IP packets
- IP fragmentation attacks
- Simple Network Management Protocol (SNMP) enumeration
- Open network ports (Vulnerable / Unnecessary ports)
- Weak authentication in protocols and SCADA elements
- Maintenance hooks not removed in production environment
- E-mail transactions on control network
- Buffer overflow / Memory overflow attacks
- Unsecured Telephone lines

**Master Service Agreement (MSA):** A legal binding contract must be signed between Vendor and Manufacturer to ensure a smooth operation of manufacturing and timely support from the vendor for raw materials or components or services. This shall include clauses as stated in below Table 1.

| Clause | Comments |
|---|---|
| Warranty and Guarantee | To ensure timely replacement and technical support |
| Security | To ensure security is considered and agreed by both parties |
| Vendor Lock-in | To avoid single point of failure at the time switching over to different vendor. The previous vendor may not be supportive, and some data or equipment's may not be suitable with the new vendor environment. |

**Table.1.** MSA Clauses (Critical Points to be Covered)

**Inventory management:** Any OT brought into the premises need to be accounted with ownership identified. For example, OT used at the production floor is mapped to the Production manager. If shift operation method in place, then Production head would be liable for the equipment's**.**

### 3.3 Operations

Various activities come under the operations to safeguard the manufacturing environment. Some of them are listed below for easy reference.

**Change Management:** Any changes in the OT environment shall follow through the change management process. This is to ensure that no unauthorised changes in the production line and thus by stability and security of the environment is kept intact. The change request should minimum answer the following questions, why, when, who, where, and how? Once these questions are answered final sign-off is required from the respective business and change approval board.

**Patch and Antivirus Management:** [4] OT equipment may come with a mini operating system. Many OT systems are embedded in nature and already hardened however it is better to keep a watch on any security breaches reported in the similar platform. [7] If any breach occurred somewhere else, then organization must proactively fix it with right patches in collaboration with the respective vendor. Vulnerability management for OT is complex in nature compared to traditional IT Systems because often-times use legacy or outdated equipment and software that no longer receive security updates. Moreover, downtime is very crucial in production OT equipment's as this may impact business revenue and reputation.

**Vulnerability Assessment and Penetration Testing (VAPT):** Periodic vulnerability assessment and pen test has to be performed to ensure that Production floors are running with minimum or negligible risk. This vulnerability management is mandated in NERC CIP-007. The points be considered while performing Vulnerability assessment shall be as follows

- Identify the assets and Manually / Automatically. E-discovery or scanning shall be performed to identify the live assets within the network.
- Once Assets identified scan the assets for vulnerabilities with the in-house developed/ vendor provided/ commercially off the Shelf Product.
- Once vulnerabilities identified it must be categorised and enumerated for effective assessment

Once vulnerabilities are identified it must be validated whether these are exists in the production or shop floor systems. This is where penetration testing will come in. Usually in IT systems the penetration testing would be performed in a production like system, for example, staging environment or pre-production environment. However, this approach can be very difficult in the manufacturing environment. In manufacturing environment, you may need to perform the pen test in the real production environment and even a small mistake can result in devastating impact on production or human life. In the manufacturing industry trigger for penetration testing shall be coming from customer requirement, compliance requirement or Red-team exercise by the organization. The Red-Team exercise is nothing, but organization is engaging Third-party to perform a pen test which is like how real hacker will try to perform the attack on actual production system. The only difference is that no Denial of Service or Distributed Denial of Service is entertained here. Some of the Supervisory Control and Data Acquisition (SCADA) system related attack methods are listed below:

- SCADA system Access
- Remote Terminal Unit (RTU) or local Programmable Logic Controller (PLCs) Compromise
- SCADA master control station Compromise
- Attack on Weak password
- RTUs or local PLCs Access
- Spoof master control station and send incorrect data to RTU
- Master control station shutdown
- local control RTUs shutdown
- Communications disruption between SCADA master control station and RTUs
- RTU control program Modification

**Data Diodes and Unidirectional Gateways**: To avoid any significant security breach in the mission critical network the devices are placed in air-gap arrangements, i.e., these devices will be not be connected to network and any access to these devices require a physical presence of the person involved. This demands a lot of manual work when upload or download of data is required in this isolated air-gap environment. To avoid this kind of situation the data diode is used. This is the physical one-way channel where the traffic is allowed from insecure network to secure network and no reverse traffic is allowed.

**Access Control:** Access to OT Equipment's shall be provided based on need-to-know basis and least privilege principles. This shall include both physical and logical access to the systems.

**Denial of Service (DOS):** Any DOS or Distributed DOS must be prevented from happening to avoid devastating effect on the Manufacturing Industry.

**Compliance and Audit:** Compliance is a second line of Defence process in Traditional IT and the same applies to Industrial control systems (ICS) as well. Audit shall plan with various needs in focus, and its frequency must be aligned based on the industry need. At least once in a year audit can be performed or whenever there is a significant change in the environment. This shall be aligned with respective local/international law and regulations focusing on the specific industry type. RPA can be used to gather evidence from authentic sources and parse through them to identify any deviation in the compliance or audit processes.

**Segregation of Duty (SOD):** This process shall be established across the OT environment so that there is no conflicting access is provided and thus by avoiding fraudulent activities.

**Segregation of Environment (SOE):** As stated in the ISA-95 layered approach different environments/layers need to be isolated based on the criticality level. This is to avoid any malpractices that is possible in a Flat network

**Inventory Update:** Any modification in the existing OT or Industrial controls systems to be updated in the centralized inventory management system. If that is not available there should be a manual process to update it in shared file and access to that must be restricted based on need basis. This shall help to maintain the up-to-date inventory and instrumental to an effective recovery process. Moreover, all Assets need to be identified, classified according to business criticality.

**Risk Management:** Anything that affects a business objective is considered as a Business Risk. For example, Unavailability of skilled resources for SCADA is a business Risk. For understanding the risk pertaining to Manufacturing the corresponding Threats to be identified. Threat might be a source and has a potential to attack the vulnerabilities exist in the system or services. Any weakness or loophole is considered as a Vulnerability. The phase of the Risk management life cycle is given below

- Risk Identification
- Risk Analysis and Evaluation
- Risk Mitigation or Treatment
- Monitoring
- Lessons learned and communication

**Risk Identification:** To identify the risk, we need to identify the threat sources with respect to the line of business or operation. For manufacturing business, the threat sources shall be as mentioned in the below table 2.

| Act of God | Man-Made | Failures |
|---|---|---|
| Flood | Malwares: Virus, Worms, Trojan Horse, Logic Bomb | Power Supply Failure |
| Earthquake | Sabotage | Component Failure |
| Tsunami | Espionage | Equipment Failure |
| Landslide | Vandalism | System Failure |
| Tornado | Strike | Logistics Failure |
| Volcano Eruption | Lack of Skill / Co-ordination/ Collaboration etc. | Supply chain Failure |

**Table.2.** Threat-Profiling

Once we identify the threat sources and categorise them it would be called as Threat profiling. Risk Identification and Threat profiling shall be performed in multiple ways. Few of them are listed below

- Interview the concerned business or operation owner
- Walkthrough with the concerned business or operation owner
- Checklist
- Questionnaire
- Observation
- Previous Reports

**Risk Analysis and Evaluation:** Once the threat source is identified the related vulnerability that it can exploit to be considered for the calculation of the risk. Usually the risk calculation involves the following

- Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF)
- Annualized rate of occurrence (ARO) = Number of times disaster event can occur in a 12-month rolling period.
- Annualized Loss Expectancy = (ALE) = SLE * ARO

Here the Asset value is calculated not only based on procurement cost, rather it includes many other costs such as maintenance cost, replacement cost, transactional impact cost etc. Exposure factor is nothing but how much impact the organization will face if the risk event is materialized on that asset. For example, assume that if there is a warehouse and its current asset value stored in it is 10000 USD, and if one-time fire explosion causes 50% Asset exposure then the loss, Single Loss Expectancy, would be AV* EF, which comes around 5000 USD. Then organization must reserve the money to withstand this impact. Risk Analysis calculation can be Quantitative as mentioned above, or it could be measured in qualitative perspective as well. When risk is measured and represented in some percentage estimation or can be mapped to some monetary value then it would be considered as Quantitative Risk Analysis. If risk cannot be measured in some percentage estimation and measured based on some intangible parameters such as brand reputation, good will etc., then it would be considered as Qualitative Risk Analysis. Once Risk is analyzed it must be prioritized based on business impact. The impact shall be based on Confidentiality, Integrity, Availability, Customer loss, Reputational loss, Regulatory loss and Financial loss.

**Risk Mitigation:** The risk mitigation or treatment plan is to ensure that risks are addressed based on risk priority so that the impact to the business or operation is reduced. Not that every identified risk needs to be addressed immediately, but rather they must be prioritized and addressed accordingly. There are various methods possible to provide risk mitigation. The methods are

- Risk Avoidance (E.g., No hazardous material storage inside the work location)

- Risk Acceptance (Can be done when identified risk is within the organization risk appetite or live with that condition only. E.g., Factory location is near to Volcano eruption Area in Japan)
- Risk Reduction (Put a control to reduce the risk, E.g. Business Continuity Plan)
- Risk Transfer (Transfer the risk to third-party. E.g., Cyber Insurance / IT outsourcing)

**Risk Monitoring:** Risk need to be monitored periodically because today the asset may not be critical as it is not storing any customer confidential data however it may become critical soon when customer confidential information is stored in it.

**Lessons learned and Communication:** In every phase of the risk management life cycle the communication to the concerned stakeholder is very important. This communication shall be over an email or over any approved medium by the business.

**Standards to be followed:**

Below are the standards that shall be considered for the manufacturing industry. Please note that before applying any policy or standard, perform risk assessment and that helps to identify the applicable policy and standards pertaining to that industry.

- ISO 27001:2013 Standard for establishing information security management systems
- ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems
- ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment
- GAO-04-140T, Critical Infrastructure Protection, Challenges in Securing Control Systems
- NIST, System Protection Profile for Industrial Control Systems (SPP ICS
- Federal Information Processing Standards Publication (FIPS Pub) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- The NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- API Standard 1164
- AGA Report Number 12

**3.4 Monitor**

**Logs:** All critical logs must be maintained either in the local equipment or centralized management system. Its access is protected and regularly monitored for any deviations. In the below table 3, IPS/IDS log monitoring function is explained.

| Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) | Function |
|---|---|
| Network-based IDS connected to the SCADA | Monitor SACADA and its environment |
| DMZ monitoring | Monitor the De-Militarized-Zone for any attacks |
| Firewall | Detection of attack in the firewall |
| Attacker Detection | Block the attacker at the earliest by monitoring the attacker movement |
| Server Monitoring | Detect Buffer-overflow or Denial of Service Attack |
| Host based IDS | Detect the actual compromise by parsing through the local system's log. |

**Table.3.** IDS/IPS Log Monitoring

The other logs that can be monitored from security perspective are given in below table 4.

| Log Type | Comments |
|---|---|
| Resource Utilization | Provides information on the level of utilization for all system resources |
| Central Processing Unit | Provides information on the usage and capacity of the unit (CPU) CPU. Unusual changes in CPU utilization might indicate an attack or unauthorized access |
| Storage Capacity | Provides an accounting of total disk capacity, disk capacity being used, and disk capacity available. Analysis can show possible unallocated disk sectors that might contain malicious code. |
| File Access Attempt | Indicates denial of attempted access to files. |
| Memory Usage | Provides an accounting of total memory capacity and memory capacity being used. Analysis can reveal possible malicious processes |
| Shutdown of Systems | Indicates when system operation was terminated, how it was terminated, and by whom it was terminated. This shutdown might allow an attacker to access files |

| | |
|---|---|
| | upon startup and bypass security mechanisms. |
| Process Utilization | Provides information on the time a specific program was started and the associated user. This data is useful in analyzing programs launched by unauthorized individuals or processes. |

**Table.4.** General System Logs Monitoring

**Alert:** Alert can be in the form of a Dashboard display in the plant floor or email or short message services. In all these modes there should be a service level mechanism must be inbuilt so that they can be resolved within the stipulated timeframe in a consistent manner.

**Supervisory Control and Data Acquisition (SCADA):** It is a software and hardware combination system that gather real-time data from ICS. It controls industrial processes, record events, and interfaces with devices like valves, motors, pumps, and sensors. [1] The general layout of the SCADA is provided in the below figure 3.

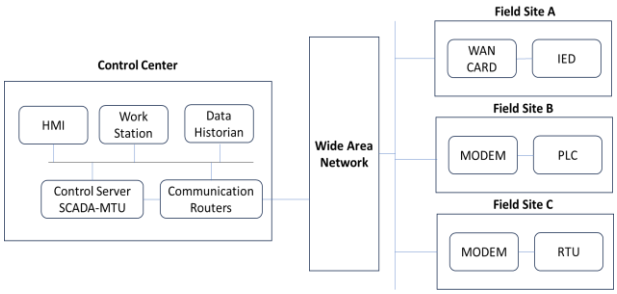


**Fig.3.** SCADA General Layout

Field devices involve physical devices attached to measuring devices and controlled by PLC. The communication to the control center shall be through a leased line, Radio or Satellite.

**Critical Infrastructure and Potential impact of security breaches:**

**1 Petroleum Industry:**

Monitoring is important in this petroleum industry as this is a critical infrastructure for nations growth as most of the country's transportation is depended on Petroleum or its related products. To support the country's growth the critical equipment's in this industry need to be monitored in real time or near real time. Most of the infrastructure is built near to seashore or coastal area to reduce any unnecessary transportation delay because of the dependency factors.

**Petroleum Industry - Security breach consequences:**

If crude oil processing port is attacked it will have a big impact on the country's economy. Some ports or all ports can be shut down as part of an emergency procedure in anticipation of similar attacks. SCADA attack may affect communications, water, bridges, dams, and pipelines. It may destroy the complete city if there is an explosion because of improper monitoring and controlling of the critical infrastructure. The Hydrocarbon processing all stages must be controlled and strict discipline to be followed from security point of view.

**2 Nuclear Power Plants:**

Reactors generate heat that results in high-pressure steam. This steam is useful to power the turbine and converts the rotational energy to electrical energy. Basically, the fission is one of the methods to produce lot of heat in Nuclear. Whereas in Fossil fuel plants the source of heat is from Fossil Fluids. There are two types of reactors normally used in Nuclear power plants, one is Boiling Water Reactor and another one is Pressurized water reactor. Usually, Boiling water reactor that generates high megawatts of electrical power must have proportionate neutron-absorbing control rods that have to be operated. Emergency core cooling system is one of the requirements to prevent the core overheating. Pressurized water reactor is vastly used in Submarines to power them. In this the coolant is kept under pressure to prevent boiling.

**Nuclear Power Plants - Security breach consequences:**

In both reactor systems there is a possibility for radioactive materials can escape to the environment because of a core meltdown. SCADA-type systems are responsible for controlling heat removal and handling other normal and emergency situations in the nuclear power plant. Therefore, any interference with the operation of the SCADA system can have dramatic and dangerous consequences.

Another issue is spent nuclear fuel, which also contains the radioactive products of the fission process. This spent fuel can be reprocessed to produce new fuel rods or it can be stored in pools in nuclear power plants.

**3 Electric Power Generation**

In a coal based Electric power generation the coal is crushed and pushed into a furnace. The coal burning generates heat that has an impact on a boiler and generates steam that is used to drive steam turbines. The turbines drive electricity generators that provide power to the distribution grid. The steam is condensed and recirculated into the boiler to repeat the process. A local control room of a SCADA system operates the plant and its processes. Many parameters and devices to be controlled for proper operation of the plant, including emergency response. The remote terminal units (RTUs) are located across the plant at the needed control points. The control components include the following:

- Emergency Response computers
- Supervisory PLC

- Master PLC hot backup
- PLC controlling the Turbine
- PLC controlling the Burner
- PLC controlling the Air quality
- PLC controlling the Water treatment
- PLC controlling the Boiler
- PLC controlling the Conveyor system
- Power substation local control PLCs

**Electric Power Generation - Security breach consequences:**

It is estimated that potential economic impact of a hypothetical attack on the U.S power Interconnection, which serves millions of people, could reach several billion. This shall also lead to rise in death rates due to failures in health and safety systems.

**4 Water Purification System:**

In a water purification process, water is pumped from a reservoir or other water sources to a water purification plant. Once purification done, the water is pumped through a transmission system to the consumers. In this process, the following activities are considered:

- Scalability
- Water pipelines pathways management
- System Controls and performance
- Water quality maintenance

In the above context SCADA system shall be used to control and monitor the water purification process, pumping and pipeline pressures. For long distances radio modems are used to communicate between the central supervisory station and the remote locations.

**Water Purification System - Security breach consequences:**

Water purification process is disabled or disrupted. Intruders shall modify the parameters pertaining to water pressure and pump data pressure. This shall lead to disruption in transmission operations and certain time may case damage to the workers.

**5 Crane Control:**

Cranes in various sizes are used in many factories and plants across many countries. It is useful to examine their associated control mechanisms to ensure the security and safety of the people who are operating that. PLC shall be used to control the crane movement and control signals can be transmitted over a radio modem from a supervisory control station. Certain Radio modems used in specific frequency may not require a license.

**Crane Control - Potential Impact:**

Control system compromise or local PLC compromise at the crane shall result in its crashing, drop the extremely sensitive loads, and harming humans and equipment.

**SCADA protocols Evolution and its Security:**

A protocol defines the format of the messages and the rules for the exchange of the messages. SCADA uses various protocols starting from proprietary to standard TCP/IP suite. The evolution is provided for the reference in the below table.

| Manufacturer | Protocol |
|---|---|
| Allen Bradley | Devicenet, ControNet, DF1, Data Highway plus, Data highway 485 |
| Modicon | MODBUS, MODBUS Plus, MODBUS TCP/IP |
| Siemens | Profibus |

**Table.5.** SCADA Protocol

There are layers being referred and considered during the development of the system and it must be followed by most of the Original Equipment Manufacturer (OEM). This is to ensure the standard and effective communication among the participants. There are two models generally being referred by the industry. One is Defence based TCP/IIP model and another one is OSI, the Open System Interconnection Model. Here we talk about OSI Model to understand how layers helps in building the standard communication. The OSI model layers are explained below table 6.

| Layer # | Name | Function | Protocols Used (not an exhaustive list) |
|---|---|---|---|
| Layer 7 | Application Layer | Layer 7, the top layer in OSI model, helps to ensure the Application control. | FTP/ HTTP |
| Layer 6 | Presentation Layer | Controls the formatting. E.g. Compression /Encryption of the packets | TIFF/PIFF/ JPEG/MPEG/ ASCII /DES/AES |
| Layer 5 | Session Layer | Establish the desired communication among the communicati | SOCKS |

| | | | |
|---|---|---|---|
| | | on participants | |
| Layer 4 | Transport Layer | It ensures the integrity of the communication. It means if any error or packet loss between the sender and receiver this would ensure the retransmission of those missing packets. | TCP (Transmission Control Protocol) / User Datagram Protocol (UDP) |
| Layer 3 | Network Layer | Responsible to route the packets to identified destination. Various routing protocols exist in this layer. | IP and IPX |
| Layer 2 | Data Link Layer | It bridges the communication between Physical and Network Layer. Once routing and individual target is identified in the network level it must be reached out eventually with the help of Physical address assigned in the respective system. This physical address is called Media Access Control (MAC) and embedded in the physical network card itself. | MAC and Logical Link Connection (LLC) |
| Layer 1 | Physical Layer | This is the layer which carries the data bits (0 and 1). All wired and wireless physical devices come under this. Example CAT5 network cable and Hub devices. | RJ45 (Used for Local Area Network) RJ11 (Used for Telephone communication) |

**Table.6.** OSI Layers

Now we will talk about the SCADA protocols in a brief level to understand the security requirements.

**MODBUS:**

In the year 1970 MODICON introduced the MODBUS protocol, it is fitting in OSI layer 7, Application layer. This works on Client Server based communication. Programmable Logic Controller (PLC) uses

this method for communication. Now this protocol is aligned to accommodate the modern TCP/ IP based communication. In MODBUS no security against unauthorized commands or interception of data.

**DNP3:**

It is an open SCADA protocol, can be useful for serial or IP communication between control devices. It is used by utility industry such as water and electrical suppliers for the exchange of data and control instructions between master control stations and remote computers or controllers called outstations. It is a complex protocol and initially planned for low bandwidth network, hence migrating to ethernet will be difficult.

**Utility Communication Architecture (UCA):**

Utility Communication Architecture (UCA) is introduced especially in Electrical industry to ensure the reliable communication which is better than DNP3. UCA 2.0 migrated to IEC Standard IEC61850 for substation automation. IEC61850 is part of a Common Information Model (CIM).

**Controller Area Network (CAN):**

Based on ISO Standard 11898-1 were developed for the automotive industry in the mid-1980s

for use in serial communications up to 1 Mbps. It can support up to 110 nodes on a two-wire, half-duplex network. The protocols operate at layer 1 and layer 2 of the OSI model. Communication is based on the Ethernet carrier sense multiple access with collision detection (CSMA/CD) method. Cost of software development is high in CAN.

**Control and Information Protocol (CIP):**

It is an open family of protocols that is implemented in the application, presentation, and session layers of the OSI model. Thus, CIP forms a common upper layer of protocols that can be used above different lower layers, such as those employing EtherNet/IP, DeviceNet, and ControlNet. The below figure 4 depicts the relationship among CIP and other protocols.

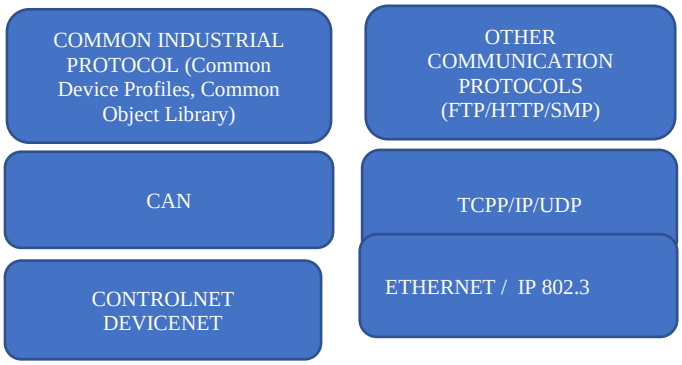


**Fig.4.** Relationship among CIP and other protocols

**DeviceNet:**

Motor, valve controls, starters, sensors, displays, operator interfaces, control computers and PLCs shall be connected through DeviceNet. It is an open standard based on the CAN protocols.

**ControlNet**:

It is a real-time and open network protocol. It utilizes the CIP protocol object capabilities and shall support up to 99 nodes. The Data rate could be of 5 Mbps. It has multiple controllers and operator interfaces. It operates at the application layer providing the application object library, at the presentation layer providing messaging services, and at the session layer supporting message routing and connection management. The cost of ControlNet based hardware can be higher, and troubleshooting can be more difficult than other protocols.

**The flexible function block (FFB):**

It is based on half-duplex bus network. It was developed by the Fieldbus Foundation, which is a consortium of 130 automation organizations. It can reduce and/or eliminate the need for expensive and difficult to maintain custom control software and special I/O gateways for PLC applications.

**Process Fieldbus (Profibus):**

It is fieldbus serial network open standard for use in time-critical control and data acquisition applications. It comes under European international fieldbus standard, EN 50 170. It provides transmission rates of 31.25 Kbps, 1Mbps, and 2.5 Mbps in the physical layer. Maximum speed is only up to MBPs. The cable and distance extender are more expensive. It works in master slave configuration, so if master fails all the slave connected to the slave will not respond.

**Firewall Services Restriction:**

Ports or Services to be allowed/ not allowed in Firewall for SCADA environment is provided in the below table 8.

| | |
|---|---|
| Telnet / FTP / HTPP | Restricted, these are clear text communication. |
| SSH/ TLS | Allowed, only to the intended people |
| SCADA ports and Services | Allowed, only to the network that has a business or operational requirement. |
| Simple Mail Transfer Protocol (SMTP) | Outbound email allowed.<br>Inbound email restricted. |

**Table.8.** Firewall Services Allowed

**Supervisory Control and Data Acquisition (SCADA) baseline:** SCADA systems are slowly moving away from isolated stand-alone proprietary systems to computer-controlled systems that uses standard traditional software, protocols and Internet. This puts the SCDA network to common cyber related attacks. Few of them are listed below.

- Man-made malwares such as Virus, Worms, Trojan horse, and Logic Bombs
- Confidentiality breaches
- Integrity breaches
- Service interruption
- Clearing the attack tracks or audit logs tampering

Usually, field PLC must operate in real time and any delay due to software bugs can result in critical infrastructure malfunctioning that affects workers safety, product quality and functional costs. Another

Drawback is SCADA plant equipment's may not have high memory capacity to run a large program. In a nutshell, IT Systems are focusing on protecting the security Triad which is Confidentiality, Integrity and Availability. But SCADA systems are focusing on reliability, quick response, emergency handling that affect

human safety, quality of services and plant safety. Hence there is a need to establish a baseline for SCADA Security and the same is proposed here below. There are minimum security requirements as part of the Baseline. The same shall be followed for any devices that gets deployed to the production or shop floors.

- All interfaces to SCADA are identified and Data or Workflow is established.
- Purpose of each interfaces is identified, and risk assessed with the help of respective operation/ business owner
- Unnecessary connection to the SCADA network is removed.
- If possible, isolate the SCADA network to ensure the security of SCADA systems
- Evaluate the security of any third-party connection to the SCADA network with the help of penetration testing or vulnerability analysis.
- Harden SCADA networks by removing or disabling unnecessary services.
- If possible, try to avoid any open source library in the SCADA control servers to reduce the avenue for attack surfaces.
- Try to strengthen the security of SCADA by not only relying on proprietary protocols to secure the system.
- Apply the recommended patches by the respective vendor. Ensure vendor is kept in loop if there is a requirement of security patches.
- If any maintenance backdoor is required ensure strong authentication is implemented to provide secure communications
- Implement Intrusion prevention and Intrusion Detection systems at appropriate location to ensure ingress and egress traffic is monitored and establish continuous incident monitoring to be able to effectively respond to cyberattacks.
- Identify any commercial and open-source security tools to perform the technical audit of manufacturing environment. Ensure that open source is vulnerability assessed before deploying it into the production environment.
- Conduct physical security surveys of the location that has a connection to the SCADA network, especially unmanned or unguarded remote sites.
- Establish Red Team to perform the attack and Blue Team to secure the environment. This is to identify the weakness in the security and patch them before it is too late.
- Establish the organization structure and RACI matrix, to identify and define cybersecurity Responsibilities, Accountability, Consultation and Informed Roles. This ensures that clear segregation of duty is established.
- Establish an effective Risk management program
- Establish a network protection strategy based on multilayer security or Defence-in-depth. It must be considered early in the design phase of the development process and in all technical decision making associated with the network.
- Establish policies and procedures to protect the network and confirming the consistent approach in protecting the operational environment.
- Establish an effective configuration management process. It must cover both hardware configurations and software configurations.
- Establish security self-assessments program. This helps organization to identify its own issues, conduct root-cause analyses, and implement effective corrective actions that address individual and systemic problems.
- Establish business continuity and disaster recovery plans. This is to ensure that operation is recovered quickly when there is a disaster. This reduces the impact to the business. If not properly managed it would lead to heavy loss to the operation and business.
- Cybersecurity performance measurement is established and hold individuals accountable for their performance. Effective cybersecurity performance requires commitment from leadership and set the tone at the top level. So that it shall be adhered by the employee or workers of the organization.
- Conduct Security training to the employees. Usually human being is the weakest chain in the security environment, hence adequate training is required to ensure that everyone understand the security requirement and follow the industry security requirements without fail. This would avoid or reduce the social engineering related attacks on the industry as well. If there is a deviation or exception in the policy, then it must be approved by the concerned business or operational unit with the proper variance form.
- Access to the assets must be provided based on need-to-know basis (Role based / Job Description based) and least privilege (Always start with the minimum access provisioning and if required elevate the privilege)
- User credential must not be written down or pasted on any machine in the production or shop floor systems, if it is done this would dilute the Industry security requirements.

**Rogue Devices:** If any devices connected to the ICS environment without any authorization that must be identified with the help of periodic wired and wireless scanning. Wherever not possible physical walkthrough is required to see any devices hooked into the ICS environment.

**Obsolete Equipment's:** [9] This is a problem in most of the manufacturing industries and must be tackled with long term and short-term strategy. If any legacy ICS device that is already outdated shall be running without proper vendor support and patches. Hence close monitoring is required in those systems to ensure no breaches because of those devices. This may warrant for engaging with a third-party provider to lend a support to the industry in case of an issue.

### 3.5 Action

**Remediation or Action taken report:** Any action taken for operational and security incidents can be recorded and monitored to avoid similar incidents and loss in future. This shall be done electronically or non-electronical methods such as maintaining logbook, registers etc.

**Incident Response:** [5] Every manufacturing industry shall have an incident response plan. The incident category, classification, setting up a team, identifying the recovery strategy, allocating resources, establishing escalation matrix must be done in a proactive approach and not at the time incidents. This is recommended because human brain may not think effectively in the emergency time and moreover this may lead to inconsistency in the recovery process, delayed recovery etc.

## 4 Common Pitfalls and Protection in ICS Security:

In section 3 Cyber security framework is explained and can be used for each ICS control environment. In the below table 9 explained various pitfalls in the ICS.

| Area | Pitfall | Protection Mechanism |
|---|---|---|
| Network Protection | [6] ICS environment connected to internet. This increases the chances of remote attack in the ICS environment. | No Direct connection to Internet. If required for operational reason, then restrict the connectivity with firewall filtering and monitoring mechanisms. Use Secure ICS protocols. If not possible in the existing network, then have a close monitoring until legacy devices are migrated to the newer environment. Example for legacy protocols; RS-232, RS-485, modbus, BACnet, dnp3, hart, etc. |
| Default Parameters/ Settings | Lot of devices comes with default features, services etc. For example, SCADA comes with many features, most of them may not be required for your environment. This increases the chances of hacker's success in exploiting the network. | Set up a Security Hardening practice for Plant and Enterprise Equipment's. |
| Identification, Authentication, Authorization and Accounting (IAAA) | Logical controls are not inbuilt as part of the ICS equipment's. This is because of devices built for operations and did not consider security by default. In few scenarios though these are inbuilt, administrators are not skilled/ interested enough in setting up these features. | Default username/ password to be modified in the purchased/ developed system. If IAAA is not inbuilt find out an alternate method for access management. Security Awareness training to all workers. |
| Physical Access | Most of the critical systems /equipment's left in an open environment without any physical barrier or protection. | Enable the physical security access provisioning and de-provisioning process. |

| | | |
|---|---|---|
| Review and Analysis | Accesses to ICS environment was not removed on time. May lead to possible security compromise. | Periodic Physical and Logical access reconciliation of ICS environment. |

**Table.9.** Common pitfalls and protection mechanism in ICS

## 5 Comparative Analysis

Comparative analysis study outcome is provided here. Many companies in the Manufacturing Industry claims that their process is very strong and that mitigates cyber-OT related risk however in practical, organizations are yet to mature in security framework establishment. This leads to instability and inconsistency in the operation. [3] Author Uchenna P. Daniel Ani, explored the cyber security risk trend that impacts the industrial environment and entities that depend on it. [1] NIST Special Publication 800-82 Rev2 explains how ICS can be secured, whilst maintaining quality and safety requirements. [2] Authors Shuang Huang, Chun-Jie Zhou, Shuang-Hua Yang, and Yuan-Qing Qin explored the resilient intelligence for industrial cyber-physical systems (CPS). They talked about an integration of many processes and technology in manufacturing industry especially the layered integration approach in OT environment. [7] Author Maurice Dawson suggest maintaining a baseline secure configuration for manufacturing plants. This need to be defined and communicated across the industry before obtaining an Approval to Operate (ATO). [5] Authors Eric Byres, P. Eng and Justin Lowe explains about the movement of OT to open standards from closed knitted protocol standards such as Ethernet, TCP/IP and web technologies without considering adequate security. This provides an increasing opportunity for hackers to take advantage of the control industry's ignorance. This proposed framework is already incorporated in one of the manufacturing companies and progressing its journey towards operational maturity. This shall be further explored in other industries as well.

## 6 Conclusion

Manufacturing industry is struggling to cope up with the increase in cyber security related attacks that results in operational downtime, financial loss, Intellectual property loss and confidential data leakage. It is natural that we can't provide 100 percent security against the cyber-attacks however establishing a proper cyber security governance framework and ensuring its compliance by the users of an industry will provide reasonable protection against these types of attacks. Hence in this paper we explored and proposed a cyber security framework for manufacturing industry with automation. [10] This shall be further explored and enhanced using Intelligent Process Automation (IPA) that combines Artificial Intelligence, Machine learning and Robotic Process Automation.

## References


[1] Stouffer, Pillitteri, et al., Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2, 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[2] Huang, S., Zhou, C. J., Yang, S. H., & Qin, Y. Q. (2015). Cyber physical system security for networked industrial processes. International Journal of Automation and Computing, 12(6), pp. 567-578.

[3] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), pp.32-74.

[4] Graham, J., Hieb, J., & Naber, J. (2016,June). Improving cybersecurity for industrial control systems. In 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE) (pp. 618-623). IEEE.

[5] Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Kongress (Vol. 116, pp. 213-218).

[6] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, pp.52-80.

[7] Dawson, M. (2018). Cyber security in industry 4.0: The pitfalls of having hyperconnected systems. Journal of Strategic Management Studies, 10(1), pp.19-28.

[8] Wegner, A., Graham, J., & Ribble, E. (2017). A new approach to cyberphysical security in industry 4.0. In Cybersecurity for Industry 4.0 (pp. 59-72). Springer, Cham.

[9] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, pp.103, 97-110.

[10] Murugappan K, Sreekala T. "An Enhanced Security Framework for Robotic Process Automation". In: Cyber Security and Digital Forensics pp 231-23.Springer, October 2021.