IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Adopting Cyber Security In Modern I4.0 Based Industrial Automation Systems

[1]Jayakumar GM, [2]Nataraj JV

[1]Senior R & D engineer, [2]Senior R & D engineer
[1]ABB PCP R and D,
[1]ABB Ability Innovation Center, Bangalore, India

Abstract:
The emergence of Industry 4.0 technologies such as Cloud Computing, Data Analytics, IIoT, Machine Learning, Artificial Intelligence is bringing a significant Digital transformation in manufacturing and industrial sectors. Industry 4.0 helps to bring out innovative solutions to industrial problems which help with high production efficiency and productivity. The manufacturing and industrial sector consists of valuable assets that help in production of various goods, it is of very high importance to protect those assets and continuously produce goods without interruption. Usage of modern Industry 4.0 solutions in manufacturing and industrial plants without proper understanding of possible cyber security vulnerabilities, preventive methods could lead to cyber security attacks on industrial plants and could damage equipment and assets. The paper is prepared to explore cyber security vulnerabilities, threats and identify important mechanisms to protect the industry 4.0 based industrial automation systems. The paper explores the areas of Cloud Computing, IIoT, Machine Learning and Artificial intelligence that are utilized to work in co-ordination with Industrial systems.

Keywords: - Cyber Security, Industrial plant security, SCADA, I4.0, Industry 4.0, Kubernetes, Docker, Containerization, Cloud Computing, Artificial Intelligence, Machine Learning, IIoT, Digital.

I. INTRODUCTION:

Industry 4.0:

Manufacturing and industrial sectors have been evolving over decades; the evolution brought many innovative solutions to industrial problems. Many industrial sectors such as power generation, transmission and distribution, oil and gas, paper and pulp, foundries, manufacturing, healthcare, food processing have successfully implemented industrial automation solutions to improve productivity, efficiency, improve downtime. The requirement for innovative solutions to solve industrial problems are high with key focus on productivity, reduce downtime, asset maintenance, scalability, efficiency. With evolution of Industry 4.0, industrial automation solutions are changing from reactive solutions to proactive solutions. The modern industrial automation solutions aim to predict failures in advance and help manufacturing and industrial production sectors to identify problems in advance and protect their most valuable assets and sustain business in most competitive markets. The modern Industry 4.0 solution combines advanced technologies such as Cloud, Artificial Intelligence, Machine Learning, IIOT, Data Analytics. IIoT can establish interconnection between industrial devices for efficient management. Cloud computing technology facilitates seamless hosting, usage and operation of industrial and manufacturing infrastructure. A vast amount of data can be stored in Cloud Computing environments which are later used for Data analytics using Machine Learning and Artificial Intelligence. The Data Analytics is capable to derive meaningful insights of operating plant. The introduction of I4.0 new technologies started providing innovative solutions to various industrial problems, on the other side the emergence of cyber security vulnerabilities are also increasing. In the year 2010, it was observed that virus such as Stuxnet specifically targeted PLC systems that took control the industrial system and intended to cause major damage and loss to industrial plants. So, it is very important for industrial automation plants to prevent cyber security problems by understanding vulnerable areas, securing them with best practices and best policies.

2.0 Industrial SCADA System:

SCADA: Supervisory Control and Data Acquisition (SCADA) systems are industrial control systems that utilize computers, communication networks, and embedded devices to gather and analyze real-time industrial data. Typically, SCADA systems are used in utility companies such as water and waste management and power transmission and distribution.

Key components of SCADA systems include:

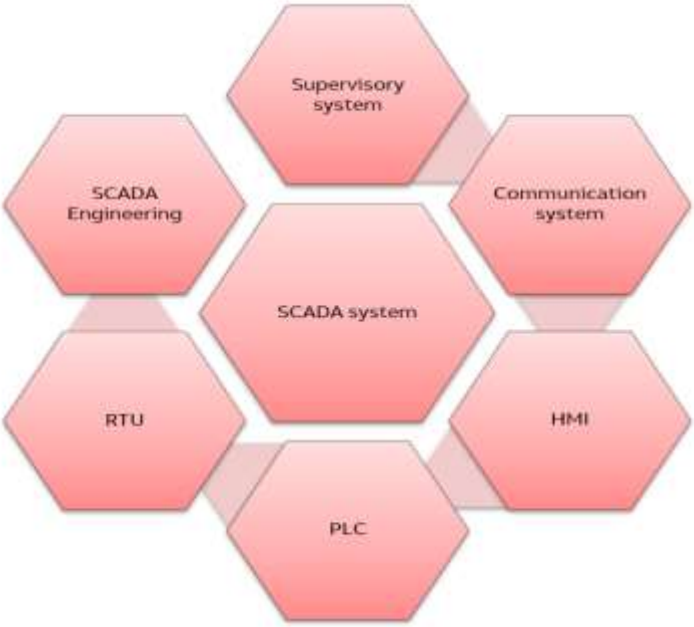


Figure 1.1: Important parts of SCADA system

The above diagram in Figure 1.1 shows the important parts of SCADA system in general. The SCADA system is designed to connect with industrial control systems such as PLCs (programmable logic controllers). PLCs are connected to sensors and actuators via input and output modules that are connected to PLC via hardwiring.

Human-Machine Interface (HMI): An electronic input-output device with a graphic display that provides process data to human operators for monitoring and control.

Supervisory System: A connectivity server that communicates between core control systems such as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs).

Remote Terminal Units (RTUs): Intelligent processor-based devices that collect and transmit telemetry data. RTUs are distributed across plants.

Programmable Logic Controllers (PLCs): Processor-based devices that logically control the SCADA system and its equipment.

Communication Infrastructure: Various communication techniques (e.g., Cellular, Radio, Ethernet) connect process devices, workstations, and servers.

3. Traditional SCADA system in industrial automation:

Below is the diagram of traditional SCADA system

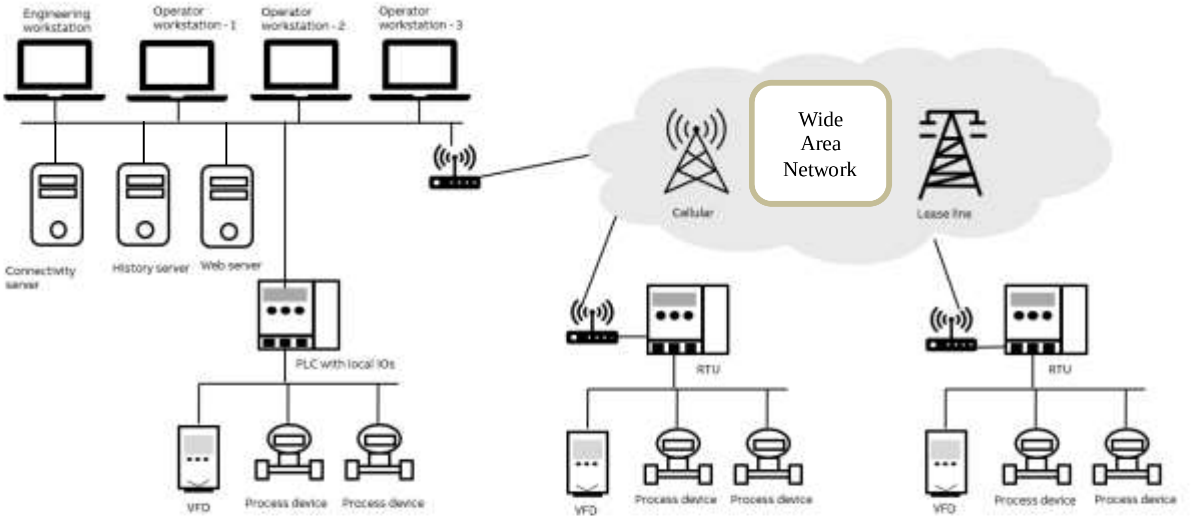
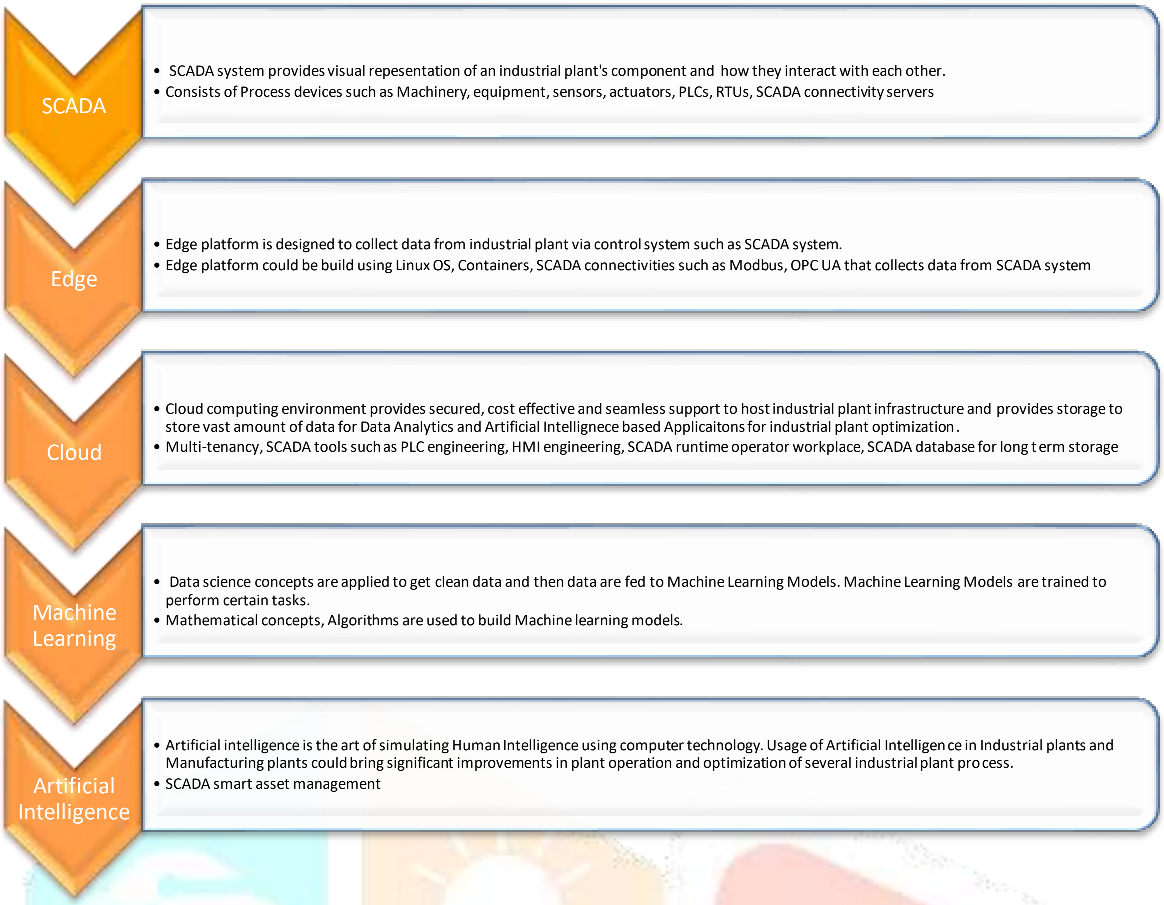


Figure 1.2: Traditional SCADA system

3.1. `Data origin, Data transfer, data storage and data analytics:

The below diagram shows the high-level data flow of process from process devices located inside manufacturing plant in SCADA based industrial control system to Modern digital eco system such as Edge and Cloud Computing. The data is moved from manufacturing plant to Edge platform. The Edge platform receives incoming data and sends the data to cloud computing environments through the internet. To manage internet bandwidth efficiently, Edge provides capability to filter unwanted data and send only most useful data to Cloud Computing environment. The data available in the cloud computing environment could be utilized for analytics applications to derive meaningful insights from manufacturing plant data. Data science techniques are applied to obtain clean data by refining null values and non-mathematical data and then provided to Machine Learning models. Artificial Intelligence applications could be developed that use various Machine Learning models and Deep Learning algorithms to simulate human like behavior to solve various industrial problems with less human interference. With the support of Data Science and Machine Learning models it is now possible to solve industrial problems with less human intervention in efficient and economical ways.



- SCADA system provides visual repesentation of an industrial plant's component and how they interact with each other.
- Consists of Process devices such as Machinery, equipment, sensors, actuators, PLCs, RTUs, SCADA connectivity servers

- Edge platform is designed to collect data from industrial plant via control system such as SCADA system.
- Edge platform could be build using Linux OS, Containers, SCADA connectivities such as Modbus, OPC UA that collects data from SCADA system

- Cloud computing environment provides secured, cost effective and seamless support to host industrial plant infrastructure and provides storage to store vast amount of data for Data Analytics and Artificial Intellignece based Applicaitons for industrial plant optimization.
- Multi-tenancy, SCADA tools such as PLC engineering, HMI engineering, SCADA runtime operator workplace, SCADA database for long term storage

- Data science concepts are applied to get clean data and then data are fed to Machine Learning Models. Machine Learning Models are trained to perform certain tasks.
- Mathematical concepts, Algorithms are used to build Machine learning models.

- Artificial intelligence is the art of simulating Human Intelligence using computer technology. Usage of Artificial Intelligence in Industrial plants and Manufacturing plants could bring significant improvements in plant operation and optimization of several industrial plant process.
- SCADA smart asset management

3.2. IIoT Architecture:

IIoT is an acronym for Industrial Internet of Things which refers to the application of IoT (Internet of things) technology in industrial applications to solve problems using advanced concepts very efficiently with less human intervention. IIoT is a network of intelligent industrial devices such as industrial machines, sensors, and devices that are connected to cloud via the internet. The data generated by IIoT devices could be sent to cloud environment and then analyzed with the help of Artificial intelligence and Machine Learning models to improve efficiency, productivity, and asset health management.

The Industrial Internet of Things (IIoT) architecture comprises four stages as shown below:

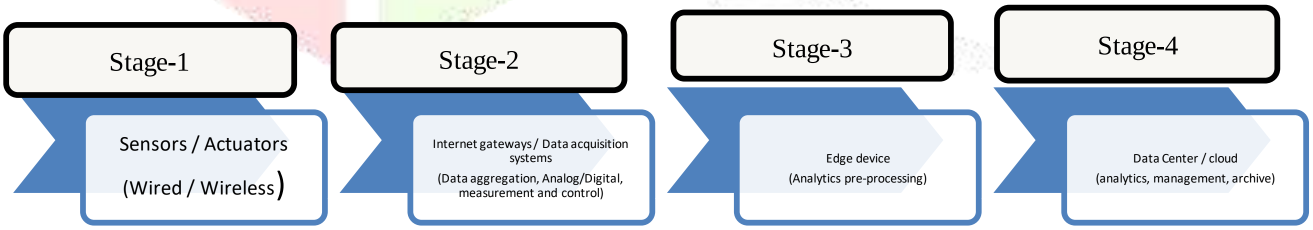

Stage-1
Sensors / Actuators
(Wired / Wireless)
Stage-2
Internet gateways / Data acquisition systems
(Data aggregation, Analog/Digital, measurement and control)
Stage-3
Edge device
(Analytics pre-processing)
Stage-4
Data Center / cloud
(analytics, management, archive)

Figure 1.3: IIoT architecture

Sensors/Actuators:

Sensors convert non-electrical inputs to electrical signals. Sensors collect data from manufacturing plants. The actuators perform actions based on the collected data from sensors. Sensors are classified into active sensors, which emit their own energy to collect real-time data such as X-rays and passive sensors, which use energy from external sources such as cameras. Sensors can measure various parameters such as position, occupancy, motion, Chemicals, Biological elements, velocity, acceleration, force, pressure, flow, humidity, light, radiation, proximity and temperature. Actuators can perform actions such as closing and opening valves, convert electrical energy into rotational motion, use pressurized air or fluid to create linear motion, act as electronic switches to control electrical power flow and isolate electrical devices. Examples of actuators include motors, heaters, relays and switches, pneumatic and hydraulic cylinders.

Internet Gateways/Data Acquisition Systems:

Internet Gateways / Data Acquisition Systems bridge sensor nodes with the external Internet or World Wide Web. They aggregate data, perform analog-to-digital conversion, and control measurements.

Edge Infrastructure:

Edge infrastructure consists of Edge computing devices. Edge devices are designed to have computing capabilities like computer, it ahas CPU, RAM, Disk storage and have communication capabilities with external environment. Edge devices could be designed using containerization technology to provide robust facilities for data processing and excellent connectivity to Cloud Computing Environment. Edge device processes data at the point of collection, reducing latency and network traffic. It performs basic pre-processing tasks like filtering and aggregation before transferring key pre-processed data to cloud services for further analysis. Edge infrastructure is capable of hosting various applications to perform intensive data processing activities and excellent connectivity with data source. The application could support various industrial protocols to collect data from manufacturing plants such as Modbus, OPC and other industrial protocols.

Cloud:

Cloud computing environment provides capabilities to connect with Edge infrastructure and collect data and store them. The cloud layer processes, stores, and analyzes data. Cloud applications provide visualization and analytics tools, presentation of data to end-users through dashboards and visualizations. These applications also offer high-level management and monitoring of the entire system Cloud computing environment could be designed to host many industrial control engineering and runtime applications and improve economics of industrial investments or expenditures.

Machine Learning:

Machine learning (ML) is a branch of Artificial intelligence (AI) that deals with empowering computers and machines to imitate the learning and perform tasks autonomously similar to humans who learn and perform their tasks, thereby improve performance and accuracy of computers and machines through experience and exposure to vast amount of collected data.

Artificial Intelligence (AI):

Artificial intelligence is a technology which provides abilities and empowers computers, robots and smart electronic systems to simulate human capabilities such as learning, decision-making, creative thinking, problem solving, speech recognition, image recognition and autonomy. Computers and machines should be capable of simulating human capabilities and performing tasks. AI combines technologies such machine learning, deep learning, and natural language processing (NLP) to simulate human-like capabilities.

AI systems are carefully designed and developed to simulate human-like intelligence and perform tasks autonomously. AI has four important parts such as learning, reasoning, perception and natural language processing (also called NLP).

Learning characteristics of AI ensures with vast amount of collected data, AI systems can learn and improve their performance over time. AI comprises important techniques such as machine learning, where algorithms are trained on very large datasets to identify important patterns from those datasets and make predictions. After learning using large data sets, reasoning characteristics of AI systems aims to make better decisions based on logical rules, and algorithms, draw conclusions and solve simple to complex problems. The Perception characteristic of AI systems have capability to interpret and understand sensory data collected in its database such as texts, images, and sounds from real world. Computer vision is used for image recognition and speech recognition is used to identify sounds. The fourth characteristic of AI ie Natural Language Processing (NLP), which is a subset of artificial intelligence that uses machine learning models to interpret and communicate with the language that humans understand. Language translation, sentiment analysis, and text generation are some of the core concepts for NLP.

3.3 Modern containerized SCADA system:

Overview diagram of modernized industry 4.0 based containerized SCADA system:

Modern SCADA system encompasses IIoT, Cloud, Artificial and Machine Learning abilities:

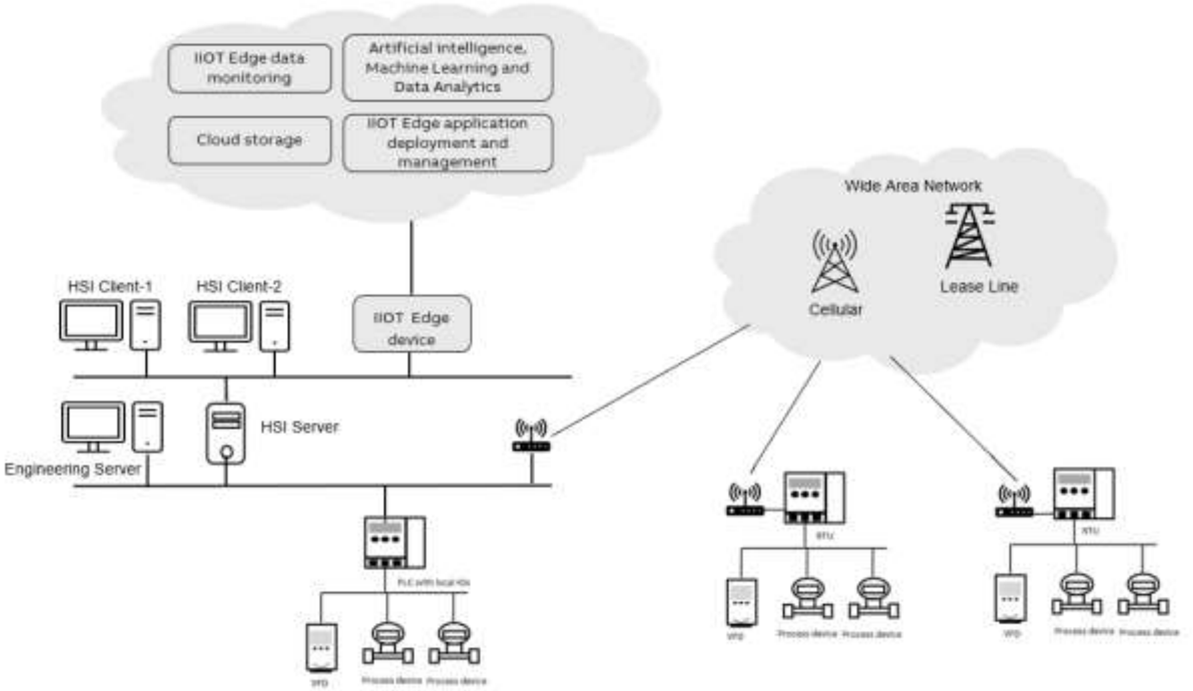


Figure 1.4: Modern containerized SCADA system.

The modernized SCADA system leverages Industry 4.0 technologies and containerization. Key features include,

Edge device that collects the process data from SCADA system and then sends the collected data to cloud computing environment. The cloud computing environment should facilitate hosting of Digital applications that help to setup and operate Edge devices. Cloud computing environment should support excellent capabilities to collect data from Edge devices from manufacturing plants, support to store large amount of industrial data, provide excellent capabilities to run advanced analytics applications by using stored industrial data in Cloud Computing Environment. Cloud computing environment should allow Artificial Intelligence and Machine Learning algorithms to seamlessly access faster and robust processing to derive meaningful insights to end users or customers.

The cloud hosting environment shall also host HMI operator workstations to visualize plant data and control the industrial plant process equipment remotely. Operators should be able to monitor process data in the form of alarms, events, trends, graphic displays, and faceplates.

The cloud environment shall support analysis of industrial data using advanced analytics tools to transform the industrial data into meaningful insights to empower industrial users to make effective decisions. Cloud environment shall also facilitate the implementation of artificial intelligence and machine learning technologies for more advanced solutions for industrial problems.

To reduce the space or storage constraints limited by Edge devices, Cloud Computing environments shall facilitate large storage capacity for industrial process data that is acquired from various process devices in SCADA environments.

Edge systems are designed and developed using Containerization technology. When Edge system integrates with SCADA system, the SCADA system will be enabled to connect with Cloud computing environment. A Containerized SCADA system consists of Edge device which is located closer to industrial control room of a particular manufacturing plant's premises. Edge devices should be capable of supporting establishing stable and seamless connections with connectivity servers of SCADA system and collecting process data. The connectivity server of a SCADA server refers to the server which is capable of establishing and interacting with industrial assets using industry standard or proprietary communication protocols. Some of industry standard protocols are Modbus, OPC, IEC61850. Edge devices should be capable of supporting various industrial protocols such as OPC UA, Modbus, IEC61850 etc. to collect data from connectivity servers of SCADA system to Edge environment. Edge devices could be developed and managed effectively and efficiently using modern Containerization technologies such as Docker and Kubernetes.

Edge devices could be built on a physical platform as well as virtual platform. Physical Edge devices would consist of physical CPU, RAM, Hard disk, Network cards and Motherboard. Edge devices which are built on top of Virtual platforms could provide opportunities to create more secure containerized SCADA environment. It is more secure when edge is hosted on virtual platform as attackers must penetrate host virtual platform and then to actual virtual edge which is difficult to break security of edge. Docker is very popular to set up containerized eco systems. Containerization provides many advantages such as isolation, portability, maintainability, efficiency, reliability and security for better design management of Edge based SCADA system. Portability of Containerization helps to maintain consistent performance of Edge system across different variants of environments, isolation capability of Containerization helps various containers of Edge system to execute independently, therefore if one container is down due to some fault conditions, it will not impact functionality of other running containers. It means when Modbus container is down due to some fault, then the other container such as OPC or any other independent container will not get affected but they will function normally to give desired functionality without any interruption. Containerization provides isolation and a minimal attack surface for cyber security issues, so it provides good security for Edge system. Docker technology has several important concepts such as Docker Engine, Docker image, Docker hub, Docker file and Docker registry. Docker engine is the core or important part of the containerized platform as it manages creation of containers and execution of containers. Docker image serves as template which is required to create Docker containers. A Docker hub is a Cloud service aimed at storage and sharing container images among various developer communities and its users across the globe. Docker file is a script used for building Docker images. Docker registry is a centralized location for storing Docker images where user access and works with Containerization technology.

In real world industrial automation system, a greater number of Docker containers are needed to build an industrial Edge eco system to interact with SCADA system and Cloud Computing environment. Therefore, it is very important to choose an efficient mechanism to use orchestration of Docker containers. Some popular techniques are Kubernetes and Docker Swarm. Kubernetes is used to manage orchestration of large number of Containers seamlessly and help software developers to quickly deploy their applications on container-based edge platform and manage them more effectively and efficiently.

It is known that Edge device collects process data from industrial plants using communication protocols such as Modbus, OPC UA etc and sends the collected data to Cloud computing environment through internet connection. One of the most important aspects of Edge device is that it provides a data filtering mechanism to ensure only desired data is sent to clouds economically and save the data bandwidth. This helps organizations to ensure faster processing of data and quickly provide meaningful insights to end users for most effective decision making.

Cloud Computing environment is designed and developed using Virtualization technology which is accompanied by remote servers to store, access, and manage data through internet connectivity. Cloud Computing technology has core characteristics such as security, agility, high availability, reliability, scalability, device and location independence, multi-sharing, and provides pay per use model for end users. Agility characteristic helps for faster sharing of resources, high availability and reliability characteristics allows to have less failures and reduced downtime of Cloud connectivity, scalability characteristic of Cloud computing environment ensures seamless provisioning of resources as per the desired requirement of the users to scale up or scale down the resource consumption, multi-sharing characteristic ensures efficient resource sharing among users. The other advantage is that the Cloud Computing resources could be accessed globally in a secure way seamlessly. Cloud computing environment providers offer significant benefits to end users to use its resources economically with the concept of pay per use-based billing model. Cloud computing environments are managed by Cloud service providers, so it is easy for end users to maintain their work and focus only on their most important tasks rather than maintaining ineffective and unproductive infrastructure management. End users could focus on building useful applications and focus on enhancing their business.

Edge device relies on stability and reliability of internet connection to effectively transfer data from control room in industrial plant to cloud. A Cloud computing environment should be designed to host SCADA control, HMI tools, Runtime SCADA monitoring and operations workplace, Data storage capabilities to store vast amount of industrial data collected using SCADA system. The process data available in the storage of cloud environment could be utilized by advanced analytics tools, AI & ML technology-based tools to provide meaningful insights and information to industrial plant users. Analytics are applied on industrial plants' data and derive meaningful insights to end users and help end users to optimize their assets to efficiently deliver production by reducing downtime.

4. Cybersecurity

Cybersecurity is a technology, set of processes and best practices that are designed to safeguard communication Networks, industrial assets such as electrical machinery, equipment, intelligent electronic devices, switchgears, communication devices, IIoT devices, Smartphones, Computers, Software and important business specific and plant operational data. Cybersecurity areas are network security which safeguards networks from intrusions via firewalls, Intrusion detection system (IDS)/ intrusion prevention system (IPS), virtual private network (VPNs). Application Security Ensures applications are secured during its development, deployment, operation and maintenance. Information Security technique protects confidentiality, integrity, and availability of data. Endpoint Security Secures individual devices that connect to a network and operates seamlessly to produce desired results. Cloud Security which Focuses on securing cloud-based infrastructure, data, applications. Operational Security consists of robust and most effective policies and best operating procedures to effectively handle and protect data assets. Identity and access management (IAM) technique ensures that only right set of people have appropriate access to industrial plants.

Cybersecurity threats:

General Cyber threats found are malware trojans, ransomware, viruses. Phishing are false emails or messages that pretend users into disclosure sensitive information. Man-in-the-middle (MIM) attacks captures important communication between two parties and prepare to attack on the system and bring the system down. Denial-of-service (DoS) attacks are irresistible systems to make services to be unavailable and cause severe loss to manufacturing plants by blocking their normal operations and reducing productivity. SQL injections are attacking databases through non secure inputs

In traditional SCADA industrial system, the data was restricted to local networks and was not exposed via internet. Modern SCADA industrial system provides more innovative solutions using Edge IIoT, Cloud Computing, Artificial Intelligence and Machine Learning technologies. On the other hand, introduction of these technologies by integrating with SCADA system will expose the industrial plants and its most important and critical assets and data to external world. This will expand the opportunities for cyber criminals to penetrate SCADA system or industrial plants and launch severe and serious attacks and bring down the plant, restrict plant from operation, have sever effect on plant productivity, damage plant's assets, misuse sensitive plant and business data. Therefore, very careful consideration, analysis and management of such cyber security problems is most important to maintain stable health of running industrial plants.

Important considerations in Cyber Security for Industrial Automation systems and manufacturing plants:

Cyber Security Attack Surface and Attack Vector:

Cyber security attack surface:

An industrial plant's attack surface is the combination of all the possible entry points that a hacker could utilize and exploit to bring down a portion or all parts of operating industrial plant. Attack surface includes possible attack zones such as open network ports and vulnerabilities in applications. If the attack surface is larger, then it poses higher possibilities to intrude and take down the industrial system by the attacker. The modern industrial plants utilize digital technologies such as Cloud, Artificial Intelligence, IIoT, Internet, Business Analytics accessed via Tablets, Smartphones, Web browsers. Therefore, the attack surface in modern industrial plants will be higher. There is a strong requirement to proactively and effectively perform assessment, manage such greater attack surface and prevent industrial systems from cyber security attacks. As the digital eco system evolves the attack surface also increases. Evolution of digital eco system could mean adding new software applications, new hardware, new firmware etc. When evolution of digital eco system is being made, it is vital to consider the assessment of software, firmware and hardware and monitor them to find out any vulnerabilities to reduce the attack surface.

Attack surface could be categorized into several parts such as

- Digital attack surface
- Physical attack surface
- Social engineering attack surface

Industrial infrastructure could be hosted on cloud or on premises. Various important and sensitive data of industrial plants such as production data, financial and accounting data, process data, industrial plant specific design and development data etc. So, with use of internet.

Attack vector is a method where an attacker utilizes the identified vulnerabilities and exploit them in industrial systems, thereby gaining unauthorized access illegally and taking down the system by causing severe damage to industrial systems and heavy financial losses. The techniques such as phishing emails sent to employees of industrial organizations and social engineering can be considered as attack vectors. So, attack surface tells what is going to be attacked and attack vector tells how it is going to be attacked.

Understanding the concept of attack surface and attack vector helps industrial organizations to identify the weaker sections of attack surface and make proactive assessment and monitoring to reduce the attack surface. This helps to reduce the chances of attackers intruding to intrude industrial system and cause damage.

4. Cyber Security challenges in Industry 4.0 based Industrial Automation solutions

Edge based IIoT platforms are built on top of docker, Kubernetes, Linux technologies, web applications and mobile applications, and edge computing environments. Therefore, it requires organization to have a diversified view towards each technology and perform security assessments.

Need for cyber security testing and methodologies has been continuously evolving with high demand to protect industry 4.0 based industrial plants.

Significance of cyber security is now a mandatory and high priority task for organizations as digital transformation is being implemented by many industrial sectors rapidly, it is of very high importance to secure data from security breaches, cyber-attacks, unauthorized access to digital eco system and protect business of consumers and producers by maintaining high level of trust in product security.

Test methods in cyber security should be prepared with various techniques to identify security threats and help organizations to protect digital eco systems. Variety of methods could be implemented such as penetration testing, vulnerability security assessments, and compliance tests. Cyber security could be found in various parts of Industry 4.0 based industrial plants such as containerization, virtualization, cloud connectivity, IIoT, Artificial Intelligence.

Cyber security problems for Containerized docker could lead to serious problems and could bring down the industrial system. There are many risks in container security

- Image vulnerabilities and malicious images
- Insecure API endpoints
- Insufficient isolation between container workloads
- Unrestricted access
- kernel exposure to host

Image vulnerabilities and malicious images:

Docker hub is open source, and it is observed that there are huge number of open-source container repositories hosted in the Docker Hub registry. Docker Hub registry consists of many variants of images which are modified and unofficial versions. Therefore, high priority should be taken to ensure security assessments are precisely done periodically and trust the publisher when a new repository is deployed.

Risk mitigation for such problems in image vulnerabilities and malicious images is not to use untrusted and vulnerable builds which helps to avoid the insertion of cyber security vulnerabilities and malicious code into the industrial plants.

One of the good practices is to use Docker certified and Docker Store packages. It is good to explore and stay updated with latest available secure best practices and keep.

Unrestricted Access:

One of the biggest risks that could have in modernized industrial plants is to have Unrestricted access to industrial plants designed using Industry 4.0 control system exposes to severe threats and could cause major damage to entire industrial plant. After entering into the Industry 4.0 based Edge eco system by utilizing unrestricted access, attackers can gain access to multiple containers inside the host. If an attacker gains access to the system file directory, it can significantly lower the effectiveness of the security enforcement. If attackers gain root access to Containers, then there are more chances to gain root access to the host. After gaining access, unexpected types of attacks could be launched on the industrial plants. So, it is extremely important to mitigate the unrestricted access risks or problems. It can be achieved by elimination of root access to all the possible areas, apply and provide the least privilege principle to the users based on their roles in an organization to industrial plant access. It is a good decision to take an assessment and enable the user namespace feature and provide separate user accounts for isolated containers. This will restrict movement between containers.

Host Kernel Vulnerabilities:

This is another type of risk that could cause serious problems to running industrial automation plants. The kernel is very important part and serves as the core of the system. Kernel is exposed to the host and all containers inside Edge system, so kernel vulnerabilities are super critical and are of very high importance to prevent serious cyber security attacks on Kernel and entire Industrial eco system. When a running container causes a kernel panic, there is a high probability that entire host could go down and cause serious threats and problems to production environments and damage reputation of the industrial automation solution provider and production plants could lose trust with their consumers. Therefore, risk mitigation plans for host kernel vulnerabilities are of very high importance for industrial plants. One good idea is to ensure and keep host operating systems up to date and proactively apply security updates. This is to be done in collaboration and acceptance with the Software Development Research and Development units of industrial automation solution provider and other important stakeholders of the organization. It is also very important to engage, educate and train to equip industrial automation plant users, operators, administrators and other employees on such vulnerability prevention.

Another important aspect of host kernel vulnerabilities prevention is to use a minimal operating system with hardened configuration. This will help and ensure

to prevent attackers from exploiting the kernel, utilizing virtual machines (VMs). It is not easy to attack kernel exploitation as any cyber security attack has to be routed through the hypervisor and then through VM kernel to reach the host kernel which could be a tedious job for cyber security attackers.

Docker Container Security Best Practices:

Industry 4.0 based industrial automation offers good benefits to build Artificial Intelligence, data analytics-based applications that could predict industrial failures and enhance the life of industrial plants, effective utilization of assets, allows to replace faulty assets in advance and fine tune the production and manufacturing process with minimal human interference. On the other hand, it is vital to ensure Docker containers are handled properly to ensure maximum security for industrial plants.

Some good practice involves:

Usage of Secure Container Registries:

container registries support to download various container images from central repository effectively and seamlessly but it also poses cyber security risks. This process provides seamless facility for downloading but at the same time, it also poses potential risks that could have severe impact on running industrial plants. Therefore, it is a good idea to follow recommended best practices and utilize trusted registries such as docker trusted registry. It is extremely important to perform stringent security assessment of registry which is used for industrial automation plants. Good practice involves usage of firewalls to protect docker registry from cyber security breaches over web technology.

Software development organizations that build Industry 4.0 based industrial solutions must restrict unauthorized users from downloading or uploading images from registry by implementing role-based access control (RBAC) mechanism. RBAC mechanism is utilized to control what resource that a specific user can access and what resources could be blocked or restricted from accessing. User access management could be time consuming, require engineers with knowledge, skills and efforts but this is mandatory in today's vulnerable world. A cautious effort could save assets and business of entire industrial plant from cyber security threats.

Restrict Root Permissions:

It is very simple and comfortable to run docker containers with root permissions as it facilitates users to achieve desired functionalities quickly. It helps to meet software developers' expectations easily as it offers less complexities in permission management. It is very good and safe practice to avoid root permissions for various security reasons.

Scan Docker Images:

Software development organization that provides Industry 4.0 based industrial solutions must setup strong policies and enforce and ensure that the downloaded docker image must be efficiently scanned periodically for vulnerabilities, identify the presence of vulnerabilities, and remove those vulnerabilities and get a clean image that can be utilized in the Edge eco system for safest operating environment.

Limit Resource Usage for containers:

Cyber security attackers could gain illegal access to Industry 4.0 based industrial plants' docker environment and could exploit containers to consume huge resources. Such a compromise of docker environment could lead to crash of Docker environment-based Edge eco system. Therefore, it is very good practice to set resource quotas for all containers of Edge eco system. Once the quota is set with limitations, then the resource consumption such as CPU, RAM will be limited for each container. This will restrict containers from occupying very large resources in Edge eco system and hence, it keeps the Docker based Edge eco system highly efficient. This will restrict attackers from misusing containers as they will not be able to control containers to consume very large resources on the Edge eco system.

Build Networks and APIs for Security:

It is well known that Docker containers utilize application programming interfaces (APIs) and networks to communicate with each other seamlessly. It is very important to build strong security policies and practices to efficiently monitor communication of Docker containers regularly to prevent cyber security attacks proactively. It is desired to build a very Strong security measures and resilience mechanism to monitor and restrict cyber security breaches quickly, efficiently and effectively without compromising the security of industrial control systems or industrial plants.

Monitoring Docker Containers:

Monitoring containers that are installed to provide industrial solutions in industrial plants provides industrial users to gain visibility and observability over containerized workloads. It is good idea to identify and utilize the specialized container monitoring tools that are readily available in the marketplace. Such tools must be assessed properly to get best tool for monitoring purposes.

Kubernetes security:

Kubernetes is one of the well-known and widely used orchestration platforms for running distributed systems. Kubernetes helps to effectively, efficiently and seamlessly perform the container management and deployment. Kubernetes supports users in automation of application container deployment, scaling functionalities and effective management of containers that are deployed in Industry 4.0 based digital solutions for manufacturing and industrial sectors.

Kubernetes security plays a significant role in preventing the modern Industry 4.0 based digital industrial automation systems.

Kubernetes provides seamless, very efficient, and facilities faster paced deployments to containerized Edge eco systems. On the other hand, it is also possible to observe and experience cyber security problems if proactive steps are not taken to protect Kubernetes deployments along with Edge eco system.

DevSecOps could help to implement very efficient processes and take security measures to safeguard Kubernetes deployments and Industry 4.0 based digital Edge eco system in an industrial plant. It is very vital for DevSecOps organization to stay updated with modern cyber security problems, challenges and solutions to effectively and efficiently provide security to Kubernetes environments.

It is very important for an organization that develops software solutions for industrial plants using Industry 4.0 based digital solutions to upskill on DevSecOps best practices:

CI/CD refers to Continuous Integration / Continuous Development which is a very popular concept in software development organizations to effectively and efficiently manage build deployments to develop and test environments in an organization. Other usage includes deployment of the test automation configuration to test system where test automation scripts are present for highly efficient test automation activities to assess product under test automatically with less human intervention. The major focus of DevSecOps is to integrate continuous regular/periodic vulnerability scanning measures into CI/CD pipelines and ensure that all the software builds are automatically scanned for cyber security problems, The reports must be generated automatically that contain all the security problems with clear description. This will help organizations to take appropriate actions and safeguard Industry 4.0 based industrial plants. This is considered to be a shift left-based proactive approach, and it helps to obtain quick feedback. Such feedback helps to solve the cyber security problems of industrial plants more efficiently and at a very early stage of software development of Digital solutions.

Commonly known cyber security threats in Kubernetes:

Vulnerable container images:

It is observed that many reusable containers are available that are developed by various developers across the globe. So trust on such containers could drastically go down as they are created by many unknown people, and it is difficult to know the intention behind the development of such containers. So, it is possible to have security problems, Container images could be unsecured. Therefore, it is possible to have high severity security risks due to presence of such vulnerabilities that could route to severe damage to industrial production environment, loss in revenue for production business and damage to reputation of brand. Therefore, it is highly recommended for cyber security professionals and software development teams to ensure such cyber security problems are regularly scanned and eliminated before deployment to Industry 4.0 based Edge environments.

Kubernetes API vulnerabilities:

It is highly recommended to take proactive precautions on cyber security problems and properly perform assessment and secure Kubernetes API as it poses potential vulnerability. API vulnerabilities is one of the major security problems in Kubernetes usage and management. If Kubernetes API endpoints are not protected properly then cyber security attackers could gain unauthorized access to Edge eco system and could exploit and lead to loss of revenue in business operations, shutdown of manufacturing plants and it could result in compromise of highly important and sensitive data of the production and business environment. Such unprotected and vulnerable Kubernetes API endpoints could serve as gateway for cyber security hackers and allow them to perform attacks such as injection attacks, denial of service (DoS) attacks which block industrial plant operations.

Therefore, it is good idea to set high priority to secure API endpoints by using strong authentication and authorization implementation mechanism and avoid such cyber security attacks by hackers. Such proactive and preventive measures ensure highly effective and efficient approach to secure organization's important assets; it also helps to secure confidential data in the production environment.

Cluster misconfiguration:

Misconfiguration refers to important settings which are not properly applied. A cluster with misconfiguration will be riskier as it could have possibilities to have potential security vulnerabilities. Therefore, it is very critical to carefully and precisely configure clusters to ensure that all the required network policies are perfectly implemented along with strong and secure access controls. It is a good idea to regularly and periodically perform audits to ensure there are no misconfigurations that could result in cyber security problems, the outcome of audit is the report and after analyzing the report all the problems must be eliminated.

Unrestricted network access:

Unrestricted network access means that users will have no restrictions on accessibility of network resources such as network switches, network routers, firewalls, nodes, industrial machines and equipment in an Industry 4.0 based industrial plants. Unrestricted network access to users could lead to misuse of system resources and could lead to data breaches. It could lead to man in the middle attacks, Denial of service which causes in disruption of business operations and bring down the system along with compromise of sensitive data security of industrial plants. So, it is very important for industrial plants to implement network policies to restrict access to important and sensitive areas of network. Network policies are very crucial in safeguarding sensitive data of business organizations or industrial plants. Any damage due to cyber security due to this issue could result in loss of revenue, business sustainability and customer trust.

Using default Kubernetes settings:

It is often simple and easy to use Kubernetes with default settings for deploying clusters could sometimes lead to cyber security risks. Kubernetes settings are already pre-configured and help users to quickly start their work but could lead to unauthorized access. Therefore, it is very important to analyze and improve the settings to ensure more secure configurations are provided to industrial plants that are built using Industry 4.0 technology. The process of applying settings could involve firewall configuration, turn off unused services. It is very important to make sure that encryption is activated in the desired areas.

RBAC and permissions:

Cybersecurity problems will not only emerge from external environments out of organization, but it could also occur if the system is mishandled by internal workers or users of industrial plants who do not have authority to use the system. If operators are provided with full access to industrial system, then they could try to create engineering models without having prior knowledge or skills and deploy to system. Another possibility is that operators could terminate some resources unintentionally or accidentally. It is also possible that sensitive and important information of industrial plants could be deleted or moved to other sources. Therefore, it is very important for industrial organizations to prevent both internal and external cyber security problems by carefully assessing of role of each worker in an organization and ensuring that role-based access control (RBAC) is provided to each authorized users based on their role to work with system. This significantly helps to safeguard industrial system and supports to build trust with customers.

Kubernetes Secrets are objects that are created to store and handle confidential data in a secure manner, some good examples are OAuth-tokens, SSH keys and passwords. Sensitive data are those that have very important data which are used to access and control system resources. Therefore, any leak of these secrets could lead to security breaches and attackers could take system down by impacting production environments, reduce production up time, misconfiguration of industrial assets, and cause loss in revenue. Therefore, it is very important to encrypt Secrets and provide access to Secrets to only those desired components that require such secrets.

Managing IT and OT layers:

IT refers to Information Technology and OT refers to Operations Technology.
OT layer of industrial automation-based plants plays a critical role in managing control of physical industrial processes. To keep the industrial in operating condition this layer is very crucial, all the industrial sensors, actuators, instrumentation are driven by control process and the industrial data collected from sensors and actuators are transferred to human machine interface via industrial communication protocols. This is the layer which is actually responsible for controlling the whole industrial plant's assets, processes and responsible for production of goods and services. This layer is extremely important to get business revenue and trust from the end customers. A compromise of OT layer could bring down entire industrial plant down and cause significant production loss, asset failures, business loss and compromise of vital industrial data.

With emergence of Industry 4.0, IT layer is also playing significant role in industrial automation in managing business level planning and integration. This layer includes Manufacturing Execution Systems, Enterprise Resource Planning systems that handles company's resources.IT layer connects factory floor to business.
With introduction of cloud technology, it is possible to host applications of Operations Technology as well as applications of IT layer. An attack on IT layer could cause significant loss to business due to compromises in business data. It could cause failure of assets, disruption of plant operation, productivity and business loss if OT layer is compromised. So, it is vital for organizations to have better policies and follow best practices to secure entire organization that encompasses IT layer and OT layer.

Cyber security threats for PLC and SCADA based industrial automation systems:

Like cyber security threats that are rising in information technology sector, industrial automation sector is also at increased risk of having cyber security attacks. The threats are expected to increase in future. One such attack on industrial plants to be observed is Stuxnet that caused damage to industrial assets. Stuxnet is a malicious computer worm intended to target SCADA systems, it was observed in the year 2010.
It has the capability to target PLC (Programmable Logic Controller). PLC is very popular intelligent electronic device used in industrial automation to control industrial processes. PLC allows industrial users to develop customizable logical programs via various programming languages such as Function Block Diagram, Structured Text, Continuous Flow Charts, Ladder Logic. Such customizable logical program plays most important role in controlling the industrial plant's processes. For example, it is possible to write a PLC program to switch on a lamp automatically when the ambience is dark. PLC programs could vary from simple logic to complex logic based on the type of industrial process control applications. The PLC program continuously executes and helps to automatically handle various industrial plant process with less human intervention. Any malfunction in PLC could seriously distract the running plant and impact plant's production or could damage industrial assets and humans. Stuxnet worm initially enters into computer system and then gains access to PLC software and then try to attack and cause PLC to misbehave.
Stuxnet is designed to have three modules such as worm, link file and rootkit. Worm executes routines that are related to main payload of the attack. When multiple copies of worm are replicated then the link file automatically executes them to create additional damage to the PLC system. Rootkit was designed to hide all Stuxnet related files to block users from detecting Stuxnet files which further expand the damage to PLC systems. So if modern SCADA Industry 4.0 gets designed then chances of introducing such malicious code could increase. This is because the attack surface increases due to introduction of Cloud computing, IIoT, internet exposure, and Artificial Intelligence. It opens the door to Cyber criminals due to increased attack surface. Such attack surface not only opens doors for malicious code such as Stuxnet but also allows more sophisticated malicious code build using advanced technologies such Artificial Intelligence and Machine Learning. So controlling such malicious code could be even more difficult than traditional SCADA system. Therefore, a careful selection of technology is must and when such technologies are selected, it is very important to manage attack surface and develop excellent security mechanisms and resilience methodologies to protect industrial plants. Develop mechanisms to continuously and frequently scan for all vulnerabilities and threats in the zones of attack surface introduced by Industry 4.0 technologies, develop strict guidelines and rules to implement Industry 4.0 technology considering zero trust principles. Use Artificial Intelligence based threat detecting and controlling tools.

Artificial Intelligence and Cyber Security:

Compared to traditional Cyber security attacks, Artificial Intelligence based Cyber security attacks could be more dangerous and difficult to control such attacks. With rapid growth in implementation of Artificial Intelligence solutions, it is now very complex to analyze cyber threats, remove them and maintain modern IIoT and Cloud based industrial SCADA control system and industrial plant. Cyber criminals could use innovative approaches using Artificial Intelligence and Machine Learning technology to penetrate the industrial plants. With use of Artificial Intelligence, Cyber criminals could launch high frequency, massive attacks to breach industrial plant and bring it down, cause damage to industrial assets and revenue losses to business. In some cases, it would be difficult to track activities performed by AI based cyber-attacks and predict future possible attacks. So, handling such AI attacks is very difficult by traditional cyber security software. It is important for industrial users to look for modern, robust AI-based cyber security prevention tools to secure industrial plants.

CONCLUSION:

Evolution of Industry technologies with Cloud Computing, IIoT, Artificial Intelligence, Machine Learning, Data Analytics has opened new opportunities for innovation of industrial solutions. Such solution would improve autonomous decision making in plant operations, improve productivity, predict asset failure in advance, reduced downtime. Traditional SCADA, PLC based industrial automation solutions, were more secure due to the local setup of control systems. But new Industry 4.0 based solution could expand the room for cyber security threats due to exposure of industrial assets outside the plant. So, it is extremely important for industrial plants to have highest priority for prevention from cyber security attacks. Cyber security attacks are very dangerous and could bring down the entire industrial plant. More serious situation could lead to malfunction of industrial plant assets resulting in unpredictable operational behavior which could be damage of industrial asset, damage to human, shutdown of entire industrial plants. So, A strict framework is needed to protect entire industrial plant, a carefully designed cyber security safety framework could protect vulnerable areas introduced due to implementation of Cloud Computing, Artificial Intelligence, IIoT. Such implementation could increase attack surface and attack vector. A strict policy could handle vulnerabilities seamlessly. Trained Industrial plant's employees could build knowledge, skills and capabilities to demonstrate careful handling of industrial assets and systems and prevent cyber security attacks. On the other hand, users should be allowed to access only those parts of the industrial system where they are designated to work. An unlimited exposure to entire plant could lead to misuse of access credentials and could result in increased vulnerabilities to industrial system. So, role-based access control is very important to implement. Unauthorized access, Root & Administrator privilege to container environment, Image vulnerabilities and malicious images, Insecure API endpoints, Insufficient isolation between container workloads, Unrestricted access, kernel exposure to host could increase threat to system. So it is very important to set organizational guidelines and policies to prevent modern Industry 4.0 based industrial plants from cyber security threats. Policies should include strict measures to prevent attacks, regular scans to find threats in systems, usage of advanced monitoring and scanning tools for cyber threats, upgrading knowledge and skills of employees, keep upgrading with latest news and skills on cyber security attacks and prevention.

Terminology:

1. IIoT – Industrial Internet of Things
2. AI – Artificial Intelligence
3. ML – Machine Learning
4. SCADA – Supervisory Control and Data Acquisition
5. IT – Information Technology
6. OT – Operations Technology
7. I4.0 – Industry 4.0
8. PLC – Programmable Logic Controller
9. RTU – Realtime Terminal Unit
10. VFD – Variable Frequency Drive
11. HSI – Human System Interface
12. HMI – Human Machine Interface
13. RBAC – Role Based Access Control
14. API – Application Program Interface
15. CI / CD – Continuous Integration / Continuous Development
16. DevOps – Development and Operations
17. DevSecOps – Development, Security and Operations
18. VM – Virtual Machine
19. DOS – Denial of Service
20. MIM – Man In Middle
21. IAM – Identify Access Management
22. VPN – Virtual Private Network
23. SQL – Structured Query Language
24. IPS – Intrusion Prevention System
25. IDS – Intrusion Detection System
26. NLP – Natural Language Processing
27. CPU – Central Processing Unit
28. RAM – Random Access Memory
29. WWW – World Wide Web
30. OPC – OLE for Process Control
31. OPC UA – Open Platform Communications Unified Architecture

REFERENCES

[1]. https://new.abb.com/process-automation/edgenius

[2]. https://new.marketplace.ability.abb/s/products/process-automation/abb-ability-edgenius?language=en_US

[3]. https://new.abb.com/process-automation/edgenius/abb-ability-edgenius-dashboard-visualize-your-needs-and-realize-your-opportunities

[4]. https://www.docker.com/

[5]. https://kubernetes.io/

[6]. https://new.abb.com/control-systems/symphony-plus/symphony-plus-scada