FLEXIBLE FACTORY
PARTNER ALLIANCE

Flexible Factory Security Guidelines

for secure factory network with wireless communications

Contributors:

FFRI, Inc research-feedback@ffri.jp	Takahiro Matsuki
Kaspersky Labs Japan jp-sis@kaspersky.com	Masato Matsuoka
NEC Corporation iot-sec-pr@ioth.jp.nec.com	Shinnosuke Katsukura Ryosuke Kawai Masahiko Kuwata Yoshimitsu Okayama
NTT Communications Corporation iot-td@ntt.com	Shuhei Tarashima Hiroto Nomura Kazuhiko Ota

Cooperation Partner :
Flexible Factory Project, a collaborative research project managed by National Institute of Information and Communications Technology

The Flexible Factory Security Guidelines have been produced by
Flexible Factory Partner Alliance
info@ffp-a.org

Copyright © 2019 Flexible Factory Partner Alliance. All right reserved.

Preface

The manufacturing industry is increasingly adopting information and communication technology (ICT). This trend is expected to continue strongly in the face of issues such as decreasing numbers of skilled works, diversification of customer needs, and intensified global competition. ICT is required not only to improve efficiency of production but also to achieve added value from on-demand manufacturing. Flexible operations and processes are important where tight collaboration is required among human and things. In this sense, communications will be used extensively and wireless connectivity will be introduced to exchange data between manufacturing machines and mobile objects and equipment such as robots, and automated transport vehicles.

The Flexible Factory Security Guidelines have been prepared to provide guidance about how to consider the cyber security issues of factory networks where wireless communications are introduced. Since it is difficult for manufacturing staff who are not network security experts to maintain a secure network, necessary knowledge is explained for them to plan and implement security measures with help from security vendors.

The Flexible Factory Security Guidelines have been created by volunteers from security vendors and IT vendors under coordination by the Flexible Factory Partner Alliance, with support from the Flexible Factory Project, a collaborative research project managed by the National Institute of Information and Communications Technology (NICT).

April 2019
Flexible Factory Partner Alliance

Table of Contents

1. Introduction

1.1. Background

Utilization of wireless networks at manufacturing sites is expected to expand rapidly in the future. There is also concern about an increase in cyber security risk. Cyber security incidents may also threaten the physical safety of the manufacturing site.

As an example of cyber-attacks, many manufacturing industries were victimized by the ransomware virus “WannaCry” in 2017. The European overseas affiliate of a prominent Japanese automobile manufacturer was infected via testing equipment and infection spread to servers and other companies in the company network one after another. The scope of the damage was not limited to business system servers and PCs, but also included manufacturing and production systems in factories, control equipment, warehouse systems, and entry management systems. Also, in another Japanese automobile factory and a Taiwanese semiconductor factory, operation was temporarily stopped by infection.

These cases were not necessarily caused by wireless networks. However, extra attention should be paid to security in wireless networks because the attack surface of a wireless network could be larger than that of a wired network.

This document presents guidelines for promoting practical security measures in a manufacturing site network including a wireless network.

1.2. Position of the Guidelines

The guidelines support security measures for those who are responsible for Information Systems, Production Technology, Production Facilities, Facility Maintenance and corresponding sections. The organization chart is depicted in Figure 1 with respect to production technology but not limited to production technology.

The target manufacturing environments are sites with wireless networks or mixed wired and wireless networks. The guidelines focus on wireless networks in particular. Referring

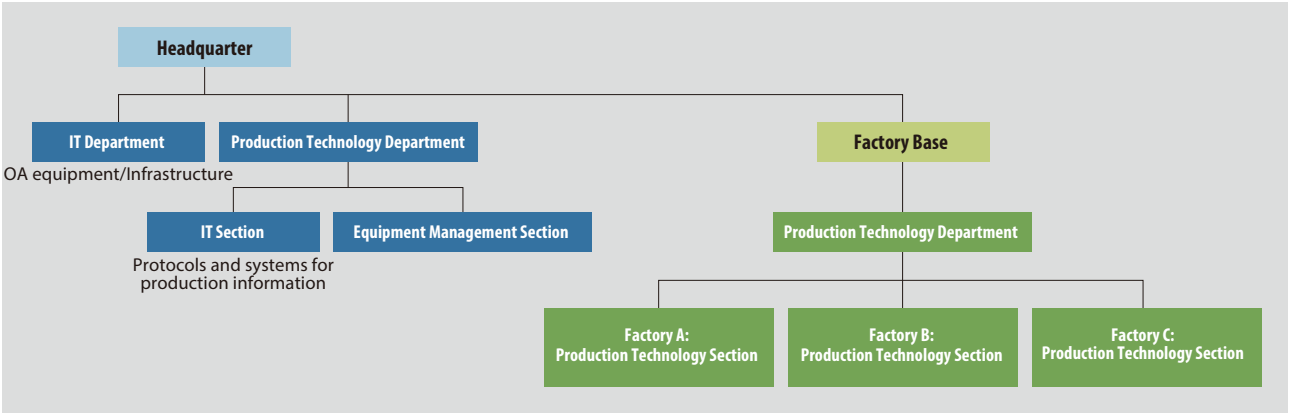


Figure 1. Examples of departments and sections whose staff should read the security guidelines. Related departments and sections, such as for operation and maintenance, are also recommended to read the guidelines. Note that this organizational structure may differ according to your organization.

to existing guidelines is also recommended for general security measures for wired networks.

1.3. Structure of the Guidelines

The guidelines consist of 5 Sections:

Section 1 presents the background and strategic position of the guidelines. It also describes usage of the guidelines and definitions of terms. Section 2 introduces the IEC 62443 reference model as a security framework for a factory network. Section 3 shows typical security risks in manufacturing site networks, considering assets to protect, and assumed threats. It also explains the framework and relationships mentioned in Section 2. Section 4 shows concrete security countermeasures from the four viewpoints of technical procedure, physical procedure, operational procedure and managemental procedure. Section 5 shows preparation and strategic thinking for security assessment and penetration testing at a manufacturing site.

1.4. How to Use the Guidelines

The guidelines have been prepared for two main purposes:

- to promote basic understanding of cyber security and necessary actions for introduction and management of devices, equipment and systems to be connected with factory networks, when planning, designing, operating and maintaining them.

- to be a reference document for communicating with security vendors, cyber security risk assessors and auditors.

Since the guidelines do not cover system configuration, assets, cyber security threats and risks for all types of manufacturing sites, actual cases should be considered using the examples described here as references.

1.5. Definitions

Asset: Anything configured in a factory network for manufacturing, including hardware, software, functions and infrastructure.

Conduit: A logical grouping of communication assets that protects the security of the channels it contains.

Defense-In-Depth architecture: Techniques to reduce security risks with not only a single layer but multiple layers of security provisions.

DMZ (DeMilitarized Zone): physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network.

DoS attack (Denial of Service attack): One type of attack to stop services. One widely

known way is sending huge number of packets (traffic) to specific servers or sites. In a broad sense, sending a small volume of packets, and physical attacks (destroying devices, wireless interference, etc.) to stop service is also included. Attacks that send packets from multiple sources are specifically called Distributed Denial of Service attack (DDoS attack).

Eavesdropping: Unauthorized interception of a conversation, communication or digital transmission in real time.

Falsification: Practice of omitting or altering equipment, data, or processes in such a way that they are no longer accurate.

Field devices: Actuators (such as positioning elements, valve and damper drives, and frequency converters) and sensors (such as measurement transducers, probes, and monitors).

IACS (Industrial Automation and Control System): System or collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

Jamming: Radio jamming to make it impossible to properly use radio waves required for communication and radar.

Process: Series of operations performed in the making, treatment or transportation of a product or material.

Physical device: Hardware used for manufacturing, processing, transportation, medical or other activities. It includes (a) sensors and actuators, equipment, and machinery under control, (b) control equipment, such as distributed control systems, programmable logic controllers, SCADA systems, associated operator interface consoles, and field sensing and control devices used to manage and control a process, and (c) computers and network equipment that are attached to communication sub-networks or inter-networks and can use services provided by the networks to exchange data with other attached systems.

Security risk: Expectation of loss or damage expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence that may damage normal operation in manufacturing.

Spoofing: Pretending to be an authorized user to perform an unauthorized action.

Threat: Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Vulnerability: Flaw or weakness in a system's design, implementation, operation or management that could be exploited to violate the system's integrity or security policy.

Zone: Grouping of logical or physical assets that share common security requirements.

2. Cyber Security Framework

In order to understand the cyber security of manufacturing sites, it is necessary to have a common framework for factory networks to describe assets to protect, threats and risks, countermeasures and assessments. The framework used by the security guidelines is based on the cyber security framework of the IEC/TS 62443-1-1 technical specification [1] (referred to as IEC 62443 hereafter) provided by the International Electrotechnical Commission (IEC).

In a factory network, an Industrial Automation and Control System (IACS) is configured with field devices, controllers, and Supervisory Control and Data Acquisition (SCADA) under a Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP). The IACS network shall be carefully segregated from other networks with respect to management authority, uniform policy and trust level, functional criticality, and amount of communication traffic over domain boundaries.

2.1. IEC 62443 Reference Model

Figure 2 shows the relationship between the IEC 62443 Reference Model and target readers of this document. There are 5 levels of devices and systems in the IEC 62443 (Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models IEC/TS 62443-1-1, pages 63-65, Edition 1.0 2009-07).

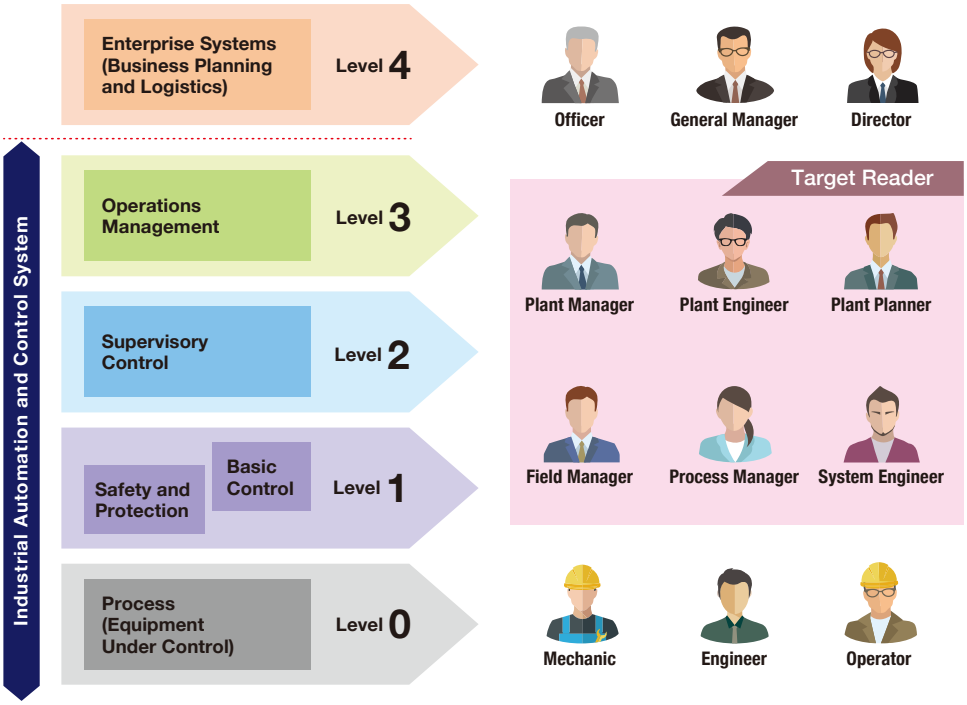


Figure 2. The IEC 62443 Reference Model and target readers.

The IEC 62443 Reference Model defines a generic view of an integrated manufacturing or production system composed of five logical levels:

Level 4 Enterprise System

This level, described as business planning and logistics in IEC 62264-1 [2], is defined as including the functions involved in the business-related activities needed to manage a manufacturing organization. Functions include enterprise or regional financial systems and other enterprise infrastructure components such as production scheduling, operational management, and maintenance management for an individual plant or site in an enterprise.

Level 3 Operations Management

Level 3 includes the functions involved in managing the work flows to produce the desired end products. Examples include dispatching production, detailed production scheduling, reliability assurance, and site-wide control optimization.

Level 2 Supervisory Control

Level 2 includes the functions involved in monitoring and controlling a physical process. There are typically multiple production areas in a plant such as distillation, conversion, blending in a refinery or turbine deck, and coal processing facilities in a utility power plant.

Level 1 Local and Basic Control

Level 1 includes the functions involved in sensing and manipulating a physical process. Process monitoring equipment reads data from sensors, executes algorithms if necessary, and maintains process history. Level 1 controllers are directly connected to the sensors and actuators of a process for continuous control, sequence control, batch control, and discrete control. Many modern controllers include all types of control in a single device.

Also included in Level 1 are safety and protection systems that monitor the process and automatically return the process to a safe state if it exceeds safe limits. This category also includes systems that monitor the process and alert an operator of impending unsafe conditions.

Level 1 equipment includes, but is not limited to Distributed Control Systems (DCS), Programmable Logic Controller (PLC) and Remote Terminal Unit (RTU).

Level 0 Process

This level is defined to include actual physical processes[1]. For example, the sensors and actuators directly connected to a process or process equipment are included. Physical processes include a number of different types of production facilities in all sectors including, but not limited to, discrete parts manufacturing, hydrocarbon processing, product distribution, pharmaceuticals, pulp and paper, and electric power.

It is useful to map the Reference Model to actual IACS structure for design and operation with respect to security measures. Devices, equipment, and systems in each level should be considered as assets to be protected. It is also necessary to consider multiple aspects of assets in each level, such as hardware and software resources, data, functions, and network interfaces.

[1] In IEC 62443, process is used to describe equipment under the control of an industrial automation and control system.

2.2. Zone and Conduit Model

A zone and conduit model, which is also referred to in IEC 62443, is used to describe logical groupings of assets in factories. By grouping assets, a common security policy can be defined for all assets in each zone. A conduit is thought of as a pipe that connects zones or that is used for communication within a zone. It encloses or protects communication channels that are the links between the assets and ensures a secure end-to-end process.

An example of a network configuration mapped to a zones and conduits model is shown in Figure 3. Appropriate security measures to protect assets shall be assessed for each zone with respect to anticipated threats and risks according to the security policy.

Defense-In-Depth architecture is also required for IACS protection. Implementing only one security measure is generally insufficient because IACS consists of various elements and is exposed to a variety of threats, as will be shown in Sections 3 and 4. Therefore, Defense-In-Depth architecture, which is often illustrated as a Swiss cheese model as in Figure 4, minimizes security risks by combining different security measures.

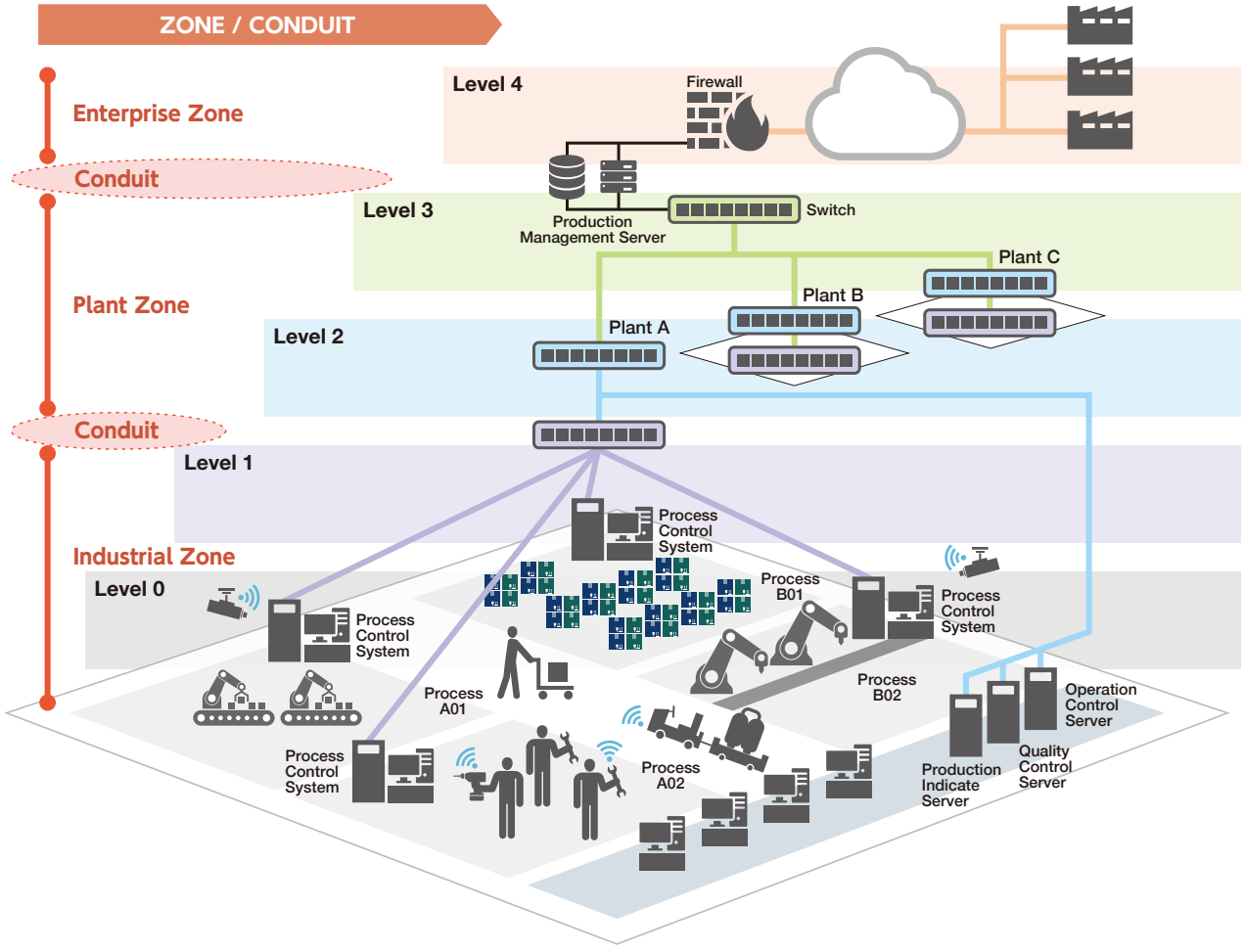


Figure 3. Example of network configuration mapped to zones and conduits model.

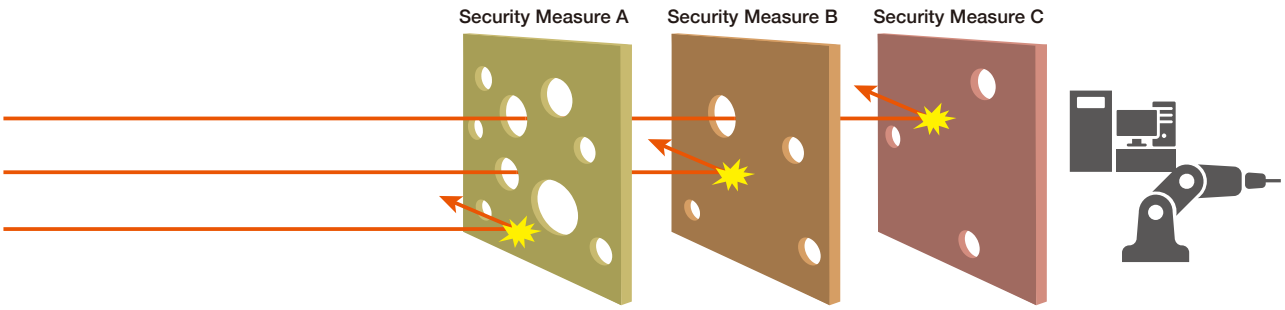


Figure 4. Swiss cheese model for Defense-in-Depth security measures.

3. Typical Model and Security Risks

In this section, a typical model of a network system in an automobile plant is discussed as an example of how to identify assets to be protected and threats to be anticipated. For other types of plant or factory, it is recommended to use this example as a reference for identifying assets and threats.

3.1. Typical Model

A typical example of a configuration model for a network system in an automobile plant is shown in Figure 5. In this example, a production management system is linked to the site management systems in press, welding, painting, and assembly sites. Each site management system has functions such as task dispatching, detailed production scheduling, and reliability assurance. The process control and monitoring systems are networked with the site management system. They send commands to field devices while monitoring the status of field devices to execute manufacturing processes. The field devices include devices such as Automated Guided Vehicles (AGVs) and impact wrenches which have wireless interfaces to connect to the network.

The site-management system, according to the production schedule, dispatches a task, through the information and control networks, to the process control system to activate

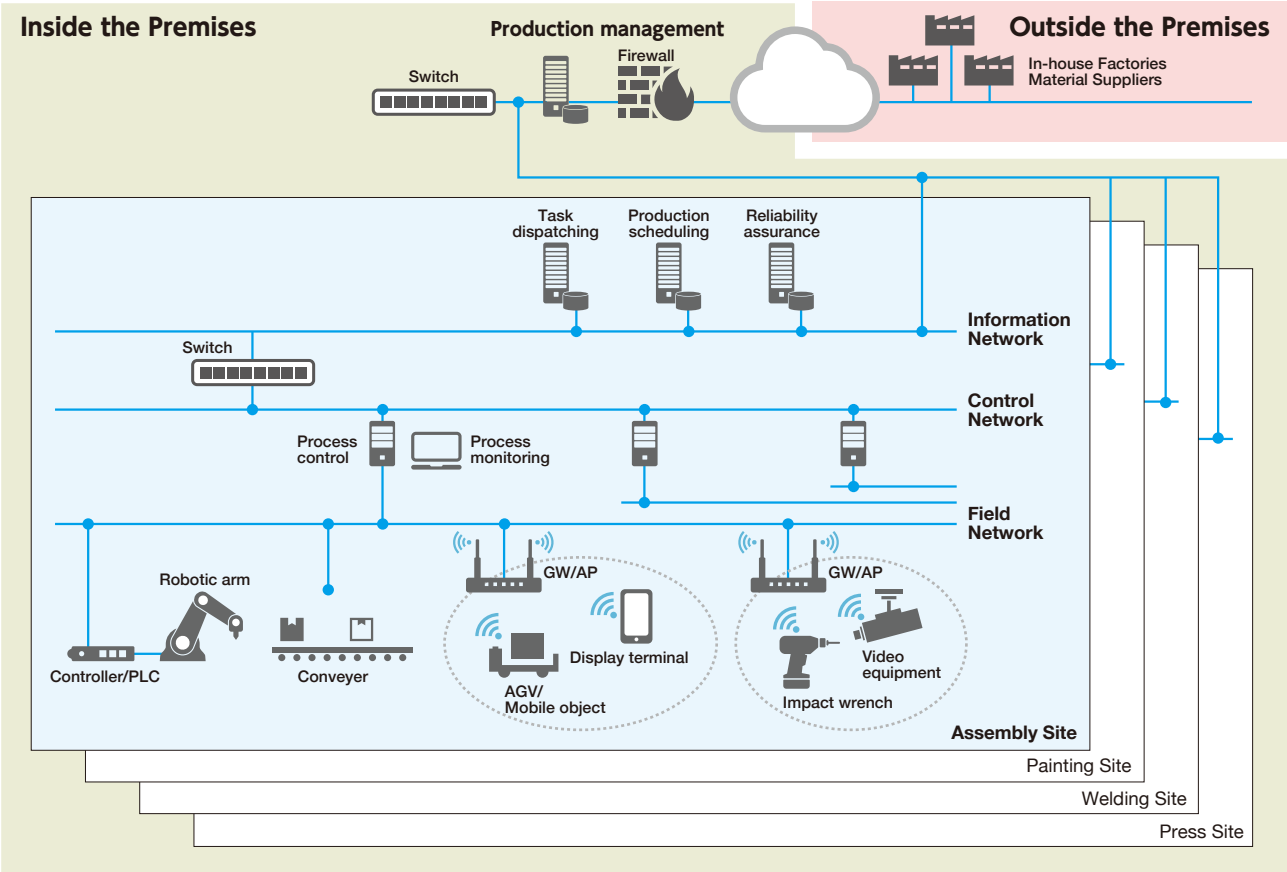


Figure 5. System configuration of automobile plant.

a conveyer. The process control system sends a command to the conveyer through the field network. The PLC of a robot arm sends status information to the process control and process monitoring systems through the field networks. It relays the information, through the control and information networks, to the site management system for reliability assurance. Although it is not indicated in Figure 5, DMZ is recommended to be set between the control and information networks. Examples of configurations including DMZs are shown in [3].

In this typical model, most network interfaces are assumed to use wired communications, and some production equipment and devices use wireless communications. In the following sections, examples of assets to be protected and anticipated threats are shown based on this model. The situation will differ depending on the type and the scale of the factory, and other factors. Equipment and devices, and management and operation for production will be different in each factory site, and the model should be adapted accordingly.

3.2. Assets to be protected

Table 1 shows examples of assets to be protected in the model of Figure 5. The levels correspond to the levels of devices and systems defined in IEC 62443. Each row represents a unique system or network asset that should be managed with regard to

Table 1. Table of assets to be protected.

Level	Resource	Data	Function	Wireless Interface
4	**Production management server (HW/SW), such as for ERP**	Financial data, human resource data, distribution data, manufacturing data, service and supply chain data, authentication data	Management of manufacturing planning and execution, procurement, and product data, data transmission and reception, authentication	LAN (wired)
	Internal/external procurement system (HW/SW)	Procurement data, authentication data	Management of procurement, data transmission and reception, authentication	
	Network (HW/SW)	All above data	Data transmission and reception	
3	**Servers (HW/SW) for task dispatching, detailed production scheduling, reliability assurance, and site-wide control optimization, such as in MES**	Operational information, operational records, product quality data, authentication data	Process planning, manufacturing process management, process & product quality control, on-site inventory control, production tracking, maintenance of equipment, data transmission and reception, authentication	LAN (wired)
	Network (HW/SW)	All above data	Data transmission and reception	
2	**Supervisory controller (HW/SW) for monitoring and controlling field devices, such as SCADA[2], operator HMI**	Process flow data, recipes, process status data, authentication data	Process control, process monitoring, data transmission and reception, authentication	LAN (wired), Fieldbus
	Network (HW/SW)	All above data	Data transmission and reception	
1	**Local or basic controller (HW/SW) for sensing and manipulating field devices, such as DCS controllers, PLCs, RTUs**	Commands to field devices, status of field devices, monitoring and actuating program data, authentication data	Field device control for sensing and manipulating, data transmissions and reception, authentication	LAN (wired/ wireless), Fieldbus, Serial Interface (wired)
0	**Field devices (HW/SW) e.g. sensors and actuators**	Process steps, sensed data, authentication	Sensing, actuating, transmission and reception, authentication	LAN (wired/wireless), Serial Interface / USB (wired), BT/BLE/ ZigBee (wireless)

[2] A slightly different view of the SCADA reference model is also provided in IEC 62443, where supervisory controllers are included in level 3.

security. The items in each column are specific asset elements that can be identified and managed with regard to security. The columns show different aspects of an asset, named “Resource”, “Data”, “Function” and “Interface”. Resource includes both hardware (HW) and software (SW). Data includes data that should be assessed separately from software. Function includes the specified functions to be executed by or using the asset. Interface includes the interface of the asset with the network.

Table 2 shows examples of assets for process equipment and devices in levels 0-1. There are various types of equipment and devices, including sensors, cameras, measurement tools, robots and AGVs. The network interfaces of the devices in Table 2 are for wireless communications. However, wired communications with Ethernet, serial bus and others are also used in factory sites.

3.3. Anticipated threats and risks

Examples of threats and risks corresponding to asset elements of the previous section are shown in Figure 6. Examples of threats include unauthorized access, eavesdropping, and DoS attacks. Examples of risks include stoppage or illegal operation of hardware or software assets, loss of data, exposure of confidential data, interruption of data transmissions, and failure of network interfaces.

Particular examples of threats and risks for each aspect of assets are given below.

Resource

Possible threats to hardware assets include physical destruction, theft or unauthorized access. Risks from these threats include the possibility of hardware being physically damaged or disabled, or used for unauthorized operations. Possible threats to software assets are erasure, unauthorized copying or unauthorized modifications. Risks from these threats include the possibility of software becoming unusable, malfunctioning or being used for unauthorized operations.

Data

Possible threats to data assets include unauthorized copying, erasure and falsification. Risks for data assets include loss of data, and unauthorized leak of confidential data. Such threats and risks may apply to various types of data assets, including information necessary for process control, quality control, production management, and procurement systems.

Function

Various functions of equipment and devices such as data transmission and reception, and authentication functions should consider risks such as the risk of being interrupted or altered. Related threats include unauthorized remote access and connection of rogue devices or equipment, and DoS attacks.

Interface

Major risks for network interfaces are failure to connect to the network and interruption of communications. Threats contributing to these risks include unauthorized network access and DoS attacks. Wireless network interfaces have additional threats due to the nature of radio propagation in the air, as discussed in the following section.

Table 2. Examples of assets for process equipment and devices in level 0-1.

Resource	Data	Function	Wireless Interface
Remote controller	Control command	Remote control	IEEE 802.15.4g, others (using specific frequency)
Movable control systems e.g. for stacker cranes, AGV, shuttle conveyor, various mounting machines / injector	Control command, monitoring status	Movable control	IEEE 802.11
Flow line analyzing system	Beacon data, terrestrial magnetism data, acceleration data, orientation data, images (bar code), video	Flow line analyzing system	IEEE 802.11/ 802.15.4g, BLE
PLC (informing status to the upper controller)	PLC status	PLC status acquisition	IEEE 802.11/ 802.15.4g
Maintenance support equipment	Images, audio, video call indicator	Remote maintenance support from supervisor	IEEE 802.11, BT, ZigBee
Position detection equipment for production management	Real-time position of workers and goods, position and route of fixed-course pick-up vehicles	Position monitoring for production management	IEEE 802.11/ 802.15.4g, BLE, UWB
Position detection equipment for asset management	Location of equipment and materials	Position monitoring for asset management	BLE
(Revolving) warning light	Monitoring status of equipment	Equipment status display	IEEE 802.15.4g
Production instruction display device	Work instructions (set-up, procedure, transport)	Displaying work instructions	IEEE 802.11
Picking instruction device	Picking instructions (for sorting, separation)	Sending picking instructions	Others (using specific frequency)
Safety check system (worker)	Safety confirmation data, worker vital information, equipment installation data, warning alarms	Checking that workers are safe	IEEE 802.15.4g, BLE
Safety check system (environment)	Toxic gas detection, oxygen concentration, radiation exposure	Checking that the environment is safe for workers	Others (using specific frequency)
Poka-yoke (error-prevention) device	Images	Error-prevention	IEEE 802.11
Poka-yoke (error-prevention) device	Screw tightness information	Error-prevention, inline inspection	IEEE 802.11, BT, BLE
Parts stock monitor device	Number of parts	Inventory management	RFID using Sub-1 GHz
Inspection equipment	Image (dimensions, strain, and dents), sound (of a drive unit) X-ray image, video (recording of bad states, contamination)	Production inspection	IEEE 802.11
Electric power measuring equipment	Electric energy, current waveform	Measuring power, energy consumption	IEEE 802.11/ 802.15.4g, BT
Water flow measuring equipment	Amount of water	Measuring water flow	IEEE 802.11
Air flow instruments	Air flow	Measuring air flow	IEEE 802.11/ 802.15.4g, BT
Thermometer and hygrometer	Ambient temperature and humidity, device/tool temperature	Measuring temperature and humidity	IEEE 802.11/ 802.15.4g, BT, LPWA
Torque measuring instruments	Torque, torque waveform	Measuring torque measurement	IEEE 802.11, BT
Equipment and environmental monitoring equipment	Image, sound, or smell	Monitoring state of equipment and environment	IEEE 802.11
Bacteria monitoring equipment	Number of bacteria	Hygiene management	IEEE 802.11
Air monitoring equipment	Amount of dust (particles), CO2 concentration, Volatile Organic Compounds (VoC) concentration	Air monitoring	IEEE 802.11 /802.15.4g, BT
Luminometer	Intensity of illumination	Illumination management	IEEE 802.15.4g
Carried electronics check system	Radio waves, thermography	Monitoring carried electronics	IEEE 802.15.4g
Security camera	Image	Security monitoring (intrusion detection)	IEEE 802.11
Production state display device	Production state, such as retention and operation/non-operation	Display of production status	IEEE 802.11/ 802.15.4g
Operation logging device	Work certification data, work logs, work errors record	Recording operations	IEEE 802.11
Counter	Number of counts	Counting functions	IEEE 802.11/ 802.15.4g

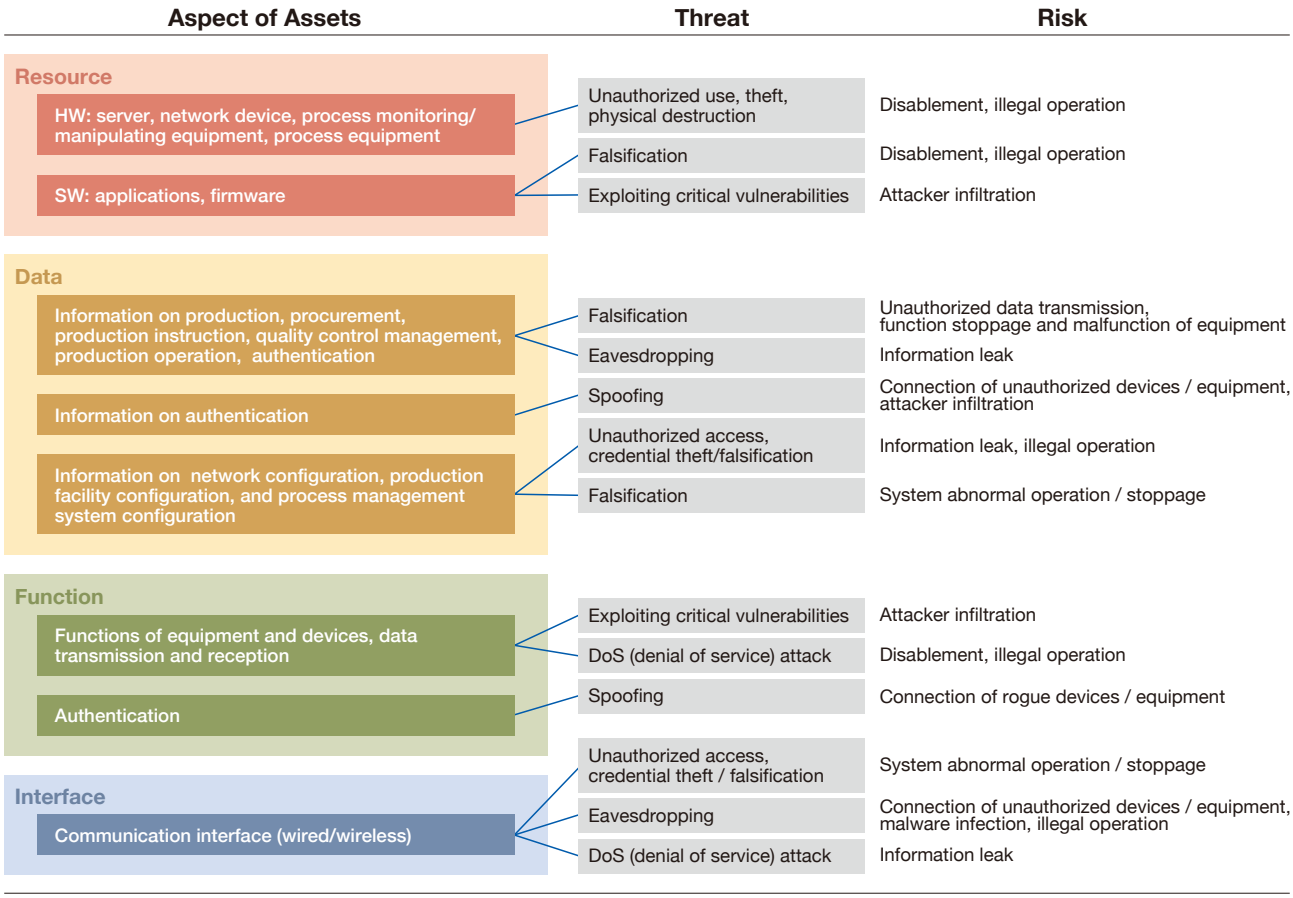


Figure 6. Examples of threats and risks for each aspect of assets

3.4. Threats specific to wireless networks

In modern factories, wireless communications are used widely for factory applications with significant advantages compared to wired connections. Equipment and devices with wireless interfaces are easy to install and relocate, which lowers cost and reduces time to start operation. There are no physical connectors and cables, and so physical contact failures and cable disconnections are never a problem. And for mobile objects, such as AGVs and robots, and workers with handy and wearable terminals, wireless communications are indispensable.

In order to achieve a secure wireless network, significant properties of wireless communications due to the nature of radio propagation should be considered as follows.

Influenced by physical objects: Radio propagation has properties of reflection, transmission and absorption, diffraction, shielding, and shadowing. Radio propagation between transmitter and receiver terminals depends on the layout of a facility, including pipes, pillars and walls, celling, machines, products, carriers, and people. Selection of types of wireless terminals and locations suitable for the particular physical space is important to reduce the risk of not being able to establish reliable wireless links. Ongoing monitoring of the states of radio channels during operations is also important for implement countermeasures to reduce the risk.

Influenced through the air: A malicious radio transmitter may cause degradation of wireless transmission and reception, and disrupt a wireless link. Wireless systems outside a factory, such as wireless LAN systems in nearby residential areas, may cause interference inside the factory if they use the same frequency band. Also, wireless systems used inside a factory may unintentionally interfere with one another. Mobile devices with wireless interfaces brought into the factory by workers, such as smart phones and music players with Wi-Fi and Bluetooth, may be a threat for factory wireless systems that use the same frequency bands. Coordinated management of wireless devices and systems, and ongoing monitoring of the status of wireless utilization are important.

Accessible over the air: There are additional risks for wireless interfaces due to radio waves spreading widely inside and outside a factory site. There are no physical connectors and a connection protocol can be modified just by changing software settings, so unauthorized access by wireless terminals in vulnerable wireless systems is a significant threat. Spoofing of SSID and spoofing of AP may allow unauthorized access and disruption of legitimate communications. Unauthorized access can result in information leak by eavesdropping, and abnormal system operation or stoppage due to falsification of network operations. A wireless interface should avoid the use of inappropriate cryptography, such as WEP, or improper authentication, such as sharing a password among multiple users.

Properties and threats of wireless communications with respect to security are summarized in Figure 7. Since a wireless link is invisible, it is difficult to know when and where trouble happens. Therefore, additional care is recommended, compared with when using wired communications.

Property	Threat
Influenced by physical objects	Link quality is influenced by surroundings and objects inside a factory, including machines, products, carriers, human, and it is changed dynamically by their movement.
Influenced through the air	Communication link is degraded or disrupted by intentional (malicious) or unintentional radio transmission.
Accessible over the air	Eavesdropping, falsification, and SSID/AP impersonation which are not easily recognized because there is no physical connection.

Figure 7. Properties and security threats of wireless communications.

4. Security Measures

In this section, security measures are introduced from four viewpoints, technical, physical, operational and managemental perspective. Security measures described in this section are listed in Figure 8. In Section 5, these measures are mapped to the assets and threats described in Section 3.

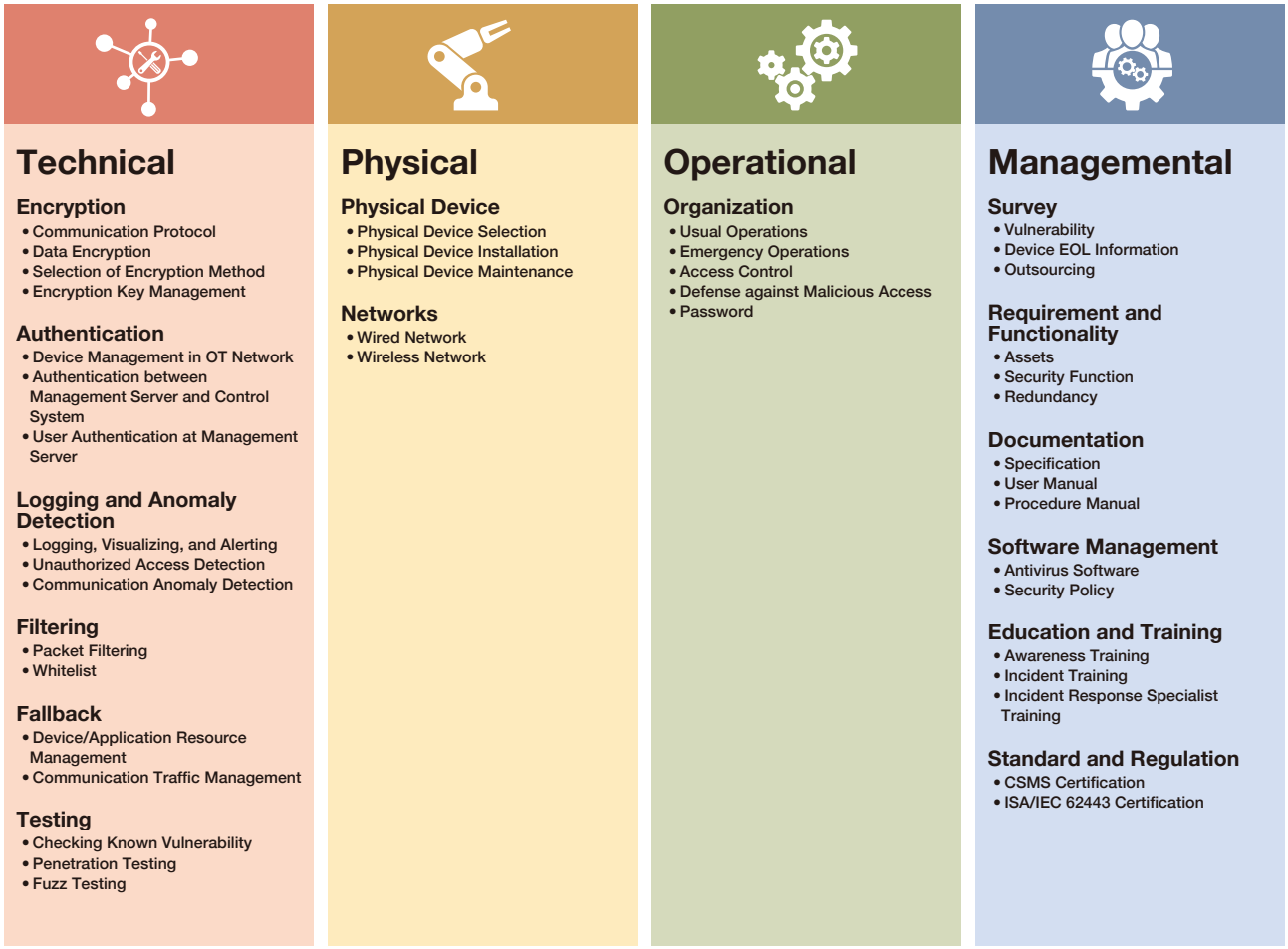


Figure 8. Security measures at-a-glance.

4.1. Technical Procedures

4.1.1. Encryption

4.1.1.1. Communication Protocol

Machine-to-Machine (M2M) communications should be securely encrypted in order to avoid wiretapping and packet eavesdropping. A typical secure communication protocol is SSL/TLS. If devices, equipment or systems are old and do not have any secure encryption function, applying tunneling techniques is highly recommended to block external accesses.

4.1.1.2. Data Encryption

Encryption of stored data is also recommended to avoid wiretapping and eavesdropping. Considering Advanced Persistent Threat (APT), data encryption is also effective to mitigate the risk of falsification: encrypting process recipes and related data also makes it possible to obfuscate which data is critical.

4.1.1.3. Selection of Encryption Method

Encryption compromises [4] should be properly considered when selecting state-of-the-art encryption methods. Encryption strength should be carefully selected considering both security requirements and hardware resources.

4.1.1.4. Encryption Key Management

A system is vulnerable if encryptions are decipherable. Encryption keys must be protected by appropriate methods or tools. The most common method is to employ encryption applications that manage keys with an access password to control use of the key. Physical tools such as Hardware Encryption Module (HSM) can also be a solution.

4.1.2. Authentication

4.1.2.1. Device Management in OT Network

In an Operational Technology (OT) network, centralized device management is highly recommended in order to prevent malicious hackers from attacking the OT network. A typical approach is to use MAC address for device authentication: if the MAC addresses of the devices are not registered in management servers, then communications of the devices are denied in the network. Though MAC address-based management is effective, it is preferable to be used in combination with other security measures since MAC address can be easily spoofed. IEEE 802.1X is also a well-known authentication standard, but at the time of writing, this standard is not available for some IoT/OT devices.

4.1.2.2. Authentication between Management Server and Control System

Communications between management servers and control systems are typical targets for attack because most protocols between them are publicly available. Therefore, security functions like password authentication should be applied to protect them. Also, using devices compliant to the standard for process control between industrial devices such as OLE for Process Control-Unified Architecture (OPC-UA), is effective.

4.1.2.3. User Authentication at Management Server

A system is vulnerable if any user can access management servers from any place. Access should only be accepted from limited and access-controlled places, and password authentication should also be performed using passwords distributed to only registered individuals.

4.1.3. Logging and Anomaly Detection

4.1.3.1. Logging, Visualizing, and Alerting

Logging functions such as acquiring operation logs of facilities, devices, and servers, and data aggregation for state analysis should be implemented for early detection and prediction of anomalies occurring in the system. An automatic alert system is also necessary for when components in the system operate anomalously. Anomalous

operations include unusual features of communication such as frequency, amount, packet header information, and unexpected stoppages. Notice that some anomalies are difficult to be defined as rules. In such cases automatic anomaly detection may be difficult. Therefore, improving the interpretability of logs for humans, and methods for visualization of operation logs is also important. Logs from each security tool (cf. Section 4.1.3.3), server access logs, and anti-virus logs (cf. section 4.4.4.1) should also be collected and analyzed from the viewpoint of cyber security. Aggregated log analysis can be effective for detecting malicious cyber activity.

4.1.3.2. Unauthorized Access Detection

Unauthorized accesses to important assets, such as access to a USB port should be logged. Further, if such access is not scheduled, this should automatically trigger an alert and logical connection to the system should automatically be shut off by using functions such as Simple Network Management Protocol (SNMP).

4.1.3.3. Communication Anomaly Detection

Security tools for detection of communication anomalies aim to detect and identify communications with anomalous behaviors (such as frequency, volume, or source/destination devices) and anomalous contents (such as IP headers of packets, commands or parameters). Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitor and detect malicious communication and activity, such as exploitation packets from malware, and lateral movement of malware. Since communications may be tampered with, functions for detecting falsification of communication data and then excluding such data from processing targets should also be prepared (for example, validation checks for edits of information transmitted from the production management server or the process monitoring/control device).

4.1.4. Filtering

4.1.4.1. Packet Filtering

Unauthorized packets should be filtered by gateways (GWs), switches and routers so as not to forward such packets to servers, equipment and devices in the system.

4.1.4.2. Whitelist

Unauthorized communication (for example, identified by source and destination pair, protocol, application, etc.) should be blocked by network devices such as GWs, switches and routers.

4.1.5. Fallback

4.1.5.1. Device/Application Resource Management

Resources used by applications, such as RAM and CPU, and authority to use applications should be properly limited in order to ensure that resources are always available in servers such as management servers, monitoring servers, control servers, and request servers, and to ensure that communication is possible in the system.

4.1.5.2. Communication Traffic Management

Communication traffic should be limited in order that communication of essential control protocols is not prevented. Bandwidth control devices, such as traffic shapers, should be introduced near several servers such as management servers, request servers, and

control servers and monitoring/control equipment.

4.1.6. Testing

4.1.6.1. Checking Known Vulnerabilities

Known vulnerabilities of system components and communication protocols should be checked (cf. Section 4.2.1.1). If such vulnerabilities are found, appropriate measures should be taken, such as using the latest protocols (cf. Section 4.1.1.1), updating the firmware of devices to the latest version, and applying security patches when they are released.

4.1.6.2. Penetration Testing

Penetration testing checks whether attackers can penetrate servers in the network system, such as management servers, request servers, monitoring servers, and control servers. Specifically, a penetration test includes checking vulnerabilities and specifying planning deficiencies.

4.1.6.3. Fuzz Testing

In fuzz testing (or fuzzing), unexpected types of data, such as data with unexpected size, time interval, metadata or format, are fed into the system to find unpredictable vulnerabilities [5]. Fuzzing can be used not only for testing the security of the system but also for discovering unexpected operations of the equipment, which may contribute to improving the safety of the system.

4.2. Physical Procedures

4.2.1. Physical Devices

4.2.1.1. Physical Device Selection

Selecting physical devices which are certified by security third parties is a highly reliable approach for securing the entire system. A typical authentication system is EDSA authentication which is based in the international standard IEC 62443-4 [6]. In IEC 62443-4, security requirements of single control devices are specified. Also, for some physical devices, production and support termination are announced in advance by the manufacturer. When such physical devices break down, they are very likely to affect the system operation since they are difficult to exchange. Therefore End-of-Life (EOL) information of physical devices should be confirmed (cf. Section 4.4.1.2).

4.2.1.2 Physical Device Installation

Since physical devices may be stolen, they should be installed considering the minimization of such risks. There are several options that may be selected: (1) placing devices where people cannot approach within a few meters of the target equipment, (2) enclosing the physical devices, (3) securing devices with cable locks, (4) installing security cameras, (5) limiting authority to enter the room where physical devices are installed, (6) notifying installation places only to minimum necessary stakeholders, (7) introducing sensors that issue alarms when devices are moved from the original place. It is also important to periodically keep evidence of physical devices by taking photos. In

addition, if there is a port physically accessible to the physical device, there is a risk of information theft and falsification inside the physical device due to operation error or malicious access (cf. Section 4.3.2). To deal with these issues, unused physical ports should be physically shut down or logically invalidated. Also, administrator alert functions should also be implemented to alert administrators when unauthorized connections are detected.

4.2.1.3 Physical Device Maintenance

Maintenance of physical devices and equipment is critical to keep them working properly. Maintenance will reduce unexpected risks of anomalous behavior caused by failure, impediment or other reasons. Inspection by human and/or other independent systems should be conducted to identify such conditions on physical devices. While maintenance is always important to keep the quality and performance of devices and equipment, describing particular actions for physical device maintenance is out of this guidelines' scope which is focused on security vulnerabilities.

4.2.2. Networks

4.2.2.1. Wired Network

Communication paths of control protocols and information protocols should be physically separated. Also, network interfaces of devices and industrial switches transmitting and receiving control messages should be adapted for priority controls (such as VLAN and QoS), safety protocols (such as CIP Safety), and motion control (such as CIP Sync). Priority of control protocols should be specified.

4.2.2.2. Wireless Network

A wireless network has several specific threats due to the properties discussed in Section 3.4. With respect to "influenced by physical objects" and "influenced through the air" properties, disconnection is the major risk. The most typical countermeasure is to perform a site survey. A site survey includes: (1) finding frequency bands that can be used to reach the target device or equipment by investigating transmission qualities in the site, (2) estimating appropriate device arrangement via surveying transmission qualities in the site, (3) installing physical shields, such as a Faraday cage that can prevent radio interference, and (4) designing radio channels so that radio waves in the system do not interfere with each other.

With respect to "accessible over the air" , data theft and falsification are typical concerns. To avoid data theft, communication should be encrypted by latest methods without vulnerabilities (c.f. Section 4.1.1) and access passwords should be set appropriately (c.f. Section 4.3.2.2). In order to prevent data falsification, appropriate authentication (cf. Section 4.1.2) should be employed so as not to allow unauthorized devices to connect to the system. Additionally, from the user equipment (UE) perspective, SSID/AP impersonation can also be a threat with the potential risk of data theft and falsification. To address this issue, SSID stealth should be set. Also, if possible, impersonation detection functions, such as the Wireless Intrusion Prevention System, WIPS, should be installed in the system.

4.3. Operational Procedures

4.3.1. Organization

4.3.1.1. Usual Operations

Procedures to configure devices and equipment in the system should be well organized. Operation settings should be doubly checked and made foolproof by checking values input by humans in accordance with the system user manual to avoid mistakes and malicious actions of operators (cf. Section 4.4.3.2). Management terminals should not be used for any other purposes, and should not connect to any other service network. It is important to clarify the rules for management of sensitive information, such as configuration information, and call attention to strict control over related parties and supplier vendors. Authentication access logs should be checked in order to detect unauthorized logins, which are indicated by repetitive authentication errors, at an early stage. It is also important to employ automation for procedures where human error may occur.

In addition, it is important to clarify procedures for distribution of bug-fixing patches when vulnerabilities are found. Procedures for conducting verifications and software updates should be clearly stated in manuals [7].

4.3.1.2. Emergency Operations

Organizing teams of people for handling system failure and system-down is necessary for quickly adapting to irregular situations. Since different emergency situations have different levels of risk, several task forces should be organized according to the risk level.

4.3.2. Access Control

4.3.2.1. Defense against Malicious Access

In order to avoid mistakes of operators and prevent insiders from attacking the system, operation settings should be doubly checked and made foolproof. For example, checking of values input by humans should be implemented to avoid mistakes and malicious actions of operators.

4.3.2.2. Passwords

To prevent illegal login, appropriate authentication should be provided in user interfaces such as management servers. An ID and a password should be provided to each user and they should not be shared by multiple users. Authentication access should be logged so that signs of unauthorized logins such as repetitive authentication errors can be detected at an early stage. Initial passwords should be changed by users to stronger ones. When remote access to management servers is required, access should be appropriately restricted by using bidirectional authentication and IP address restriction.

4.4. Managemental Procedures

4.4.1. Survey

4.4.1.1. Vulnerability

Information about known vulnerability issues of software and hardware should be gathered. If such vulnerabilities are found in the system, they should be fixed and the corresponding problems must be resolved. In case bug-fixing patches exist, downloading them from legitimate sites is preferable.

4.4.1.2. Device EOL Information

For some equipment, manufacturers announce termination of support or production in advance. Such equipment could interfere with the system operation because it is impossible to exchange at the time of failure. Therefore, when installing the equipment, it is necessary to confirm the End-of-Life (EOL) information. Even after installation, EOL information should be periodically checked. Collecting information about successor and alternative equipment is also important. Furthermore, it is also desirable to check the supply chain of the equipment, and to procure from multiple suppliers to reduce the risk of shortage of equipment. Ideally, the system should be designed to be independent of specific equipment or manufacturer. When the EOL of equipment is identified, due to the end of production or, for example, due to bankruptcy of the manufacturer, replacement plans for development, verification, installation, labor and costs, and so on must be established and completed before the EOL.

4.4.1.3. Outsourcing

When system design or development is outsourced, integrators should be selected, managed and inspected appropriately. To that end, it is desirable to establish criteria for selection, management and inspection, and to commit to them.

4.4.2. Requirements and Functionality

4.4.2.1. Assets

Functionalities and assets that should be protected in the system (cf. Section 3) must be first identified. Then, appropriate methods must be selected to protect them. Examples of such methods include, (1) memory protection, (2) stored data encryption (e.g., pgcrypto module in PostgreSQL), (3) communication encryption (e.g., secure protocols), (4) data audits (e.g., pg_audit module), (5) information access restriction, and (6) alarm installation to physical accesses (e.g., physical keys and device enclosures). When such functionalities and assets are managed by databases, measures for SQL injection should also be prepared (e.g., sql_firewall module). Furthermore, functions to detect assets in the system automatically are also effective to protect them.

4.4.2.2. Security Functions

Security requirements to deal with potential threats should be well clarified. Technical and physical procedures (cf. Section 4.1 and Section 4.2) should be implemented to satisfy the security requirements. Also, sufficient resources should be prepared in the system to operate the corresponding security functions [8]. For example, in the case of embedded software, security requirements include (1) the requirements for tamper resistance, and (2) the policy for communication with third party applications. Note that, in general, communications to third party applications should not be allowed. Security

functions include (1) means to detect the signs of anomalies [7], (2) means to prevent operation mistakes and malicious operations, such as regulation of key information registration, user manuals and automated configuration, and (3) resistance to electromagnetic noise of production equipment. Furthermore, the restoration priorities of equipment when abnormalities occur should also be clarified.

4.4.2.3. Redundancy

As for critical equipment that affects the operation of the entire system, redundant equipment should be prepared so that the system will not stop when problems happen. Redundancy is also important for emergency stop of the system and critical data storage.

Furthermore, it is effective to implement mechanisms for notifying the service provider of a failure or functions for automatically switching to a redundant machine, for example, implementing hot standby.

4.4.3. Documentation

4.4.3.1. Specification

The security requirements, functions and system configuration clarified in Section 4.4.2 should be specified in the specification document.

4.4.3.2. User Manual

In addition to the specification in Section 4.4.3.1, manuals used by operators should also be prepared. In the manuals, procedures must be clearly shown for operators not to make mistakes.

4.4.3.3. Procedure Manual

Procedures should be described clearly in manuals (cf. Section 4.4.3.2) so that mistakes related to devices, equipment and operations do not occur in operation.

4.4.4. Software Management

4.4.4.1. Antivirus Software

Antivirus software should be installed as extensively as possible. Also, regular malware scanning, detection of files saved in formats other than specified formats, and periodical software update, should be set as default settings.

4.4.4.2. Security Policy

Unnecessary running of applications in equipment should be detected and be automatically stopped if it is found. Disk areas accessible by each application should be constrained by disk partition in order to reduce the risk of information theft and falsification through unauthorized accesses. In addition, policies for checking the reliability of each application should be defined in advance. Such policies include confirmation of application developers, tampering, vulnerabilities, suspicious operations and communications, and backdoors.

4.4.5. Education and Training

4.4.5.1. Awareness Training

An organization which has low cyber security awareness is weaker than an organization with high awareness because individuals may not realize an incident is undergoing even if they have seen a sign of it.

4.4.5.2. Incident Training

Training people and organizations by training programs with various incident simulation types is very important to improve their resilience against cyber security incidents which may have not been occurred in the factory. It will also help people to have clear images of the damage and effective countermeasures in specific cases.

4.4.5.3. Incident Response Specialist Training

Incident response specialist training is technical training that educates Incident Response (IR) engineers to solve problems when responding to an incident. Also, it will help them to communicate with third party specialists who may help them to solve problems during incident response work.

4.4.6. Standard and Regulation

4.4.6.1. CSMS Certification

CSMS certification is for improving cyber security management to fight against cyber security risks at a factory.

4.4.6.2. ISA/IEC 62443 Certification

ISA/IEC 62443 certification is to empower individuals who are in charge of cyber security at a factory. Each category of certificates is proof of the responsible people in the organization.

5. Security Assessment at Factory Sites

In IEC62433 [1], security assessment is described as “risk assessment” that identifies vulnerability and threats to the resources in a factory to reduce potential risks. The purpose of a “security audit” is to figure out the appropriate countermeasures, in other words, “security control” to protect the factory.

“Risk assessment” and “security audit” are usually conducted by a third party who has well established knowledges and skills, that is, cyber security risk assessors and auditors. It is critical not to stop the factory even if a cyberattack happens.

It is important to ask for a full process schedule and milestones to understand it and manage it with a vendor, and what kinds of reports are to be delivered during assessment and/or audit services.

Usually factory staff do not need to be concerned with specialized IT or cybersecurity terminology, but cyber security risk assessors and auditors may be communicating with specialized terminology which factory staff may not be familiar with. It is necessary for factory staff to try to fill any communication gaps, by asking questions such as “What does it mean to the factory and production system?” before and during the assessment and/or audit services.

Tables 3-5 represent factory components and typical risks and countermeasures. Threats in the tables imply examples of situations as following.

Credential theft/falsification: An attacker intents to get information remotely.

Data/File falsification: An attacker intents to do something wrong in production process by falsify the data and files remotely.

Data/command eavesdropping: An attacker intents to obtain process recipes and instructions remotely.

Improper operation: Devices have been exposed to an attacker to do something malicious.

Production process falsification/theft: An attacker intents to falsify/theft process recipes and instructions via devices in production line.

Data/command eavesdropping: An attacker intents to obtain process recipes and instructions remotely.

DoS attack: An attacker intents to do something wrong in production process.

The tables help factory staff to improve communication with the cyber security risk assessor and auditor, and also to understand the reasons behind the countermeasures that they recommend.

Table 3. Factory components and typical risks and countermeasures in level 2-4.

Level	Resource	Data	Function	Interface (Wireless connections may be replaced by wired alteratives.)
4	Production management server (HW/SW)	Information on: production, procurement, authentication, etc.	Production management, procurement management, data transmissions and reception, authentication	LAN
	Internal/ external procurement system (HW/SW)	Information on: procurement, authentication, etc.	procurement management, data transmissions and reception, authentication	–
	Network(HW/SW)	Information on: production, procurement, authentication, etc.	Data transmissions and reception	–
3	Production request Server, quality management server, (HW/SW, e.g. SCADA sever)	Information on: production instruction, quality control management, production operation, authentication, etc.	Production management, quality management, production operation management, data transmissions and reception, authentication	LAN
	Network (HW/SW)	Information on: production instruction, quality control, production operation, authentication, etc.	Data transmissions and reception	–
2	Process monitoring/ control server (HW/SW)	Information on: process management, authentication, and etc.	Process management, data transmissions and reception, authentication	LAN
	Network (HW/SW)	Information on: production instruction, quality control, production operation, authentication, and etc.	Data transmissions and reception	–

Risks	Threats	Countermeasures																
		Technical						Physical		Operational		Managemental						
		4.1.1.Encryption	4.1.2. Authentication	4.1.3. Logging and Anomaly Detection	4.1.4. Filtering	4.1.5. Fallback	4.1.6. Testing	4.2.1. Physical Devices	4.2.2. Networks	4.3.1. Organization	4.3.2. Access Control	4.4.1. Survey	4.4.2. Requirements and Functionality	4.4.3. Documentation	4.4.4. Software Management	4.4.5. Education and Training	4.4.6. Standard and Regulation
Production Data falsification/theft	Credential theft/falsification		●	Applicable to all.	●		●				●	●		Applicable to all.	●	Applicable to all.	Applicable to all.
	Data/File falsification	●	●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●		●		
	Improper operation	●	●					●	●	●							
	Production process falsification/theft	●	●		●		●	●		●	●	●	●				
Procurement Data falsification/theft	Credential theft/falsification		●		●		●				●	●			●		
	Data/File falsification	●	●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●		●		
	Improper operation	●	●					●	●	●							
Network shutdown, process data theft	Credential theft/falsification		●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●		●		
	DoS attack				●	●			●				●				
Failure of production management, process data theft	Credential theft/falsification		●		●		●				●	●			●		
	Data/command falsification	●	●		●		●		●		●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●		●		
	Improper operation	●	●		●			●	●	●							
	Production process falsification/theft	●	●					●		●	●	●	●				
	DoS attack				●	●			●				●				
Network shutdown, process data theft	Credential theft/falsification		●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●	●	●		●			●	●		●		
	DoS attack				●	●			●				●		●		
Failure of process control, process data theft	Data/command falsification	●	●		●		●		●		●	●			●		
	Credential theft/falsification		●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●				
	Improper operation	●	●					●	●	●							
	Production process falsification/theft	●	●					●		●	●	●	●		●		
	DoS attack				●	●			●				●		●		
Network shutdown, process data theft	Credential theft/falsification		●		●		●				●	●			●		
	Data/command eavesdropping	●	●		●		●		●			●	●		●		
	DoS attack				●	●			●				●		●		

Table 4. Factory components and typical risks and countermeasures in level 0-1.

Level	Resource	Data	Function	Interface (Wireless connections may be replaced by wired alteratives.)
1	Local process monitoring/manipulating equipment, e.g. DCS controllers, PLCs, RTUs(HW/SW)	Information on: state of production and operations management, Instruction of process, authentication, and etc.	Monitoring and control of production and operations Equipment control, data transmissions and reception, authentication	LAN/Serial/IEEE 802.11
	Remote controller	Controlling command	Remote control	IEEE 802.15.4g
	Movable control systems e.g. for Stacker cranes, AGV, shuttle conveyor, various mounting machines / injector	Controlling command, monitoring status	Movable control	IEEE 802.11
0	Flow line analyzing system	Beacon, terrestrial magnetism, acceleration, orientation, image (bar code), video	Flow line analysis	IEEE 802.11/802.15.4g, BLE
	PLC (informing status to the upper controller)	PLC status	PLC status acquisition	IEEE 802.11/802.15.4g
	Maintenance support equipment	Image, audio, video Call indicator	Remote maintenance support from supervisor	IEEE 802.11, BT
	Positioning equipment for production management	Real-time position of workers and goods, position and route of fixed-course pick-up	Positioning for production management	IEEE 802.11/802.15.4g, BLE, UWB
	Positioning equipment for asset management	Location of equipment and materials	Positioning for asset management	BLE
	(Revolving) warning light	Monitoring status of equipment	Equipment status display	IEEE 802.15.4g
	Production instruction display device	Work instructions (set-up, procedure, transport)	Work instruction	IEEE 802.11
	Picking instruction device	Picking instruction (sorting, separation)	Picking instruction	Others (using specific frequency)
	safety check system (worker)	Confirming safety equipment installation, warning alarm, vital information	Safety information for workers	IEEE 802.15.4g, BLE
	safety check system (environment)	Toxic gas detection, oxygen concentration, radiation exposure	Safety information for environment	Others (using specific frequency)
	Poka-yoke (error-prevention) device	Image	Error-prevention	IEEE 802.11
	Poka-yoke (error-prevention) device	Screw tightness information	Error-prevention, inline inspection	IEEE 802.11, BT, BLE
	Parts stock monitor device	Number of parts	Inventory	RFIC using Sub-1Ghz

Risks	Threats	Countermeasures															
		Technical						Physical		Operational		Managemental					
		4.1.1.Encryption	4.1.2. Authentication	4.1.3. Logging and Anomaly Detection	4.1.4. Filtering	4.1.5. Fallback	4.1.6. Testing	4.2.1. Physical Devices	4.2.2. Networks	4.3.1. Organization	4.3.2. Access Control	4.4.1. Survey	4.4.2. Requirements and Functionality	4.4.3. Documentation	4.4.4. Software Management	4.4.5. Education and Training	4.4.6. Standard and Regulation
Failure of control, process data theft	Data/command falsification	●	●	●	●		●		●		●	●		●	●	●	●
	Credential theft/falsification		●	●	●		●				●	●		●	●	●	●
	Data/command eavesdropping	●	●	●	●		●		●			●	●	●	●	●	●
	Improper operation	●	●	●	●			●	●	●				●		●	●
	Production process falsification/theft	●	●	●				●		●	●	●	●	●		●	●
	DoS attack			●	●	●			●				●	●	●	●	●
Production stoppage, Failure of function	Data/command falsification	●	●	●			●		●		●				●	●	●
Production stoppage, Failure of function																	
Failure of function	DoS attack				●	●			●				●		●	●	●
Failure of control																	
Production stoppage, Failure of function	Credential theft/falsification		●	●			●				●				●	●	●
Failure of function	Data/command falsification	●	●	●			●		●		●				●	●	●
Lost equipment & material, Failure of function																	
Failure of function																	
Production stoppage, Failure of function																	
Production stoppage, Failure of function																	
Injury of worker, Production stoppage	DoS attack				●	●			●				●		●	●	●
Worker health damage, Increase of defective products Production stoppage																	
Increase of defectice products Production stoppage																	
Increase of defectice products Production stoppage																	
Production stoppage, Failure of function																	

Table 5. Factory components and typical risks and countermeasures in level 0.

Level	Resource	Data	Function	Interface (Wireless connections may be replaced by wired alteratives.)	
0	Inspection equipment	Image (Dimensions, strain, and dents), Sound of the drive unit, X-ray image, video(Bad state, contamination)	Production Inspection	IEEE 802.11	
	Electric power measuring equipment	Electric energy, current waveform	Power, energy consumption	IEEE 802.11/802.15.4g, BT	
	Water flow measuring equipment	Amount of water	Water flow measurement	IEEE 802.11	
	Air flow instruments	Air flow	Air flow Measurement	IEEE 802.11/802.15.4g, BT	
	Thermometer and hygrometer	Ambient temperature and humidity, device/tool temperature	Temperature and humidity measurement	IEEE 802.11/802.15.4g, BT, LPWA	
	Torque measuring instruments	torque, torque waveform	Torque measurement	IEEE 802.11, BT	
	Equipment and environmental monitoring equipment	Image, sound, or smell	Status of equipment and environmental monitoring	IEEE 802.11	
	Bacteria monitoring equipment	The number of bacteria	Hygiene management	IEEE 802.11	
	Air monitoring equipment	Amount of dust (particles), CO2 concentration, Volatile Organic Compounds (VoC) concentration	Air monitoring	IEEE 802.11/802.15.4g, BT	
	Luminometer	intensity of illumination	Illumination management	IEEE 802.15.4g	
	Carried electronics check system	Radio waves, thermography	Monitoring carried electronics	IEEE 802.15.4g	
	Security camera	Image	Security intrusion detection)	IEEE 802.11	
	Production state display device	Production state, operation/non-operation state	Display production status	IEEE 802.11/802.15.4g	
	Operation recording device	Work certification, work logs, work error record	Recording operations	IEEE 802.11	
	Counter	Number of counts	Counting	IEEE 802.11/802.15.4g	

Risks	Threats	Countermeasures																
		Technical						Physical		Operational		Managemental						
		4.1.1.Encryption	4.1.2. Authentication	4.1.3. Logging and Anomaly Detection	4.1.4. Filtering	4.1.5. Fallback	4.1.6. Testing	4.2.1. Physical Devices	4.2.2. Networks	4.3.1. Organization	4.3.2. Access Control	4.4.1. Survey	4.4.2. Requirements and Functionality	4.4.3. Documentation	4.4.4. Software Management	4.4.5. Education and Training	4.4.6. Standard and Regulation
Increase of defective products																		
Increase of defective products																		
Increase of defective products																		
Increase of defective products																		
Increase of defective products																		
Increase of defective products																		
Increase of defective products Worker health damage																		
Worker health damage	Data/command falsification	●	●	●			●		●		●				●	●	●	
Increase of defective products, Worker health damage																		
Worker health damage																		
Increase of defective products or operations																		
Failure of intrusion detection																		
Over/Under production																		
Unrecorded operations																		
Increase of defective products Over/Under production, Production stoppage																		

References

[1] Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models, IEC/TS 62443-1-1, Edition 1.0 2009-07, International Electrotechnical Commission (IEC).

[2] Enterprise - Control System Integration - Part 1: Models and terminology, IEC 62264-1, Edition 2.0, 2013-05, International Electrotechnical Commission (IEC).

[3] Secure Architecture Design, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), https://ics-cert.us-cert.gov/Secure-Architecture-Design

[4] CRYPTREC Encryption, https://www.cryptrec.go.jp/english/list.html

[5] Fuzzing, The Open Web Application Security Project (OWASP), https://www.owasp.org/index.php/Fuzzing

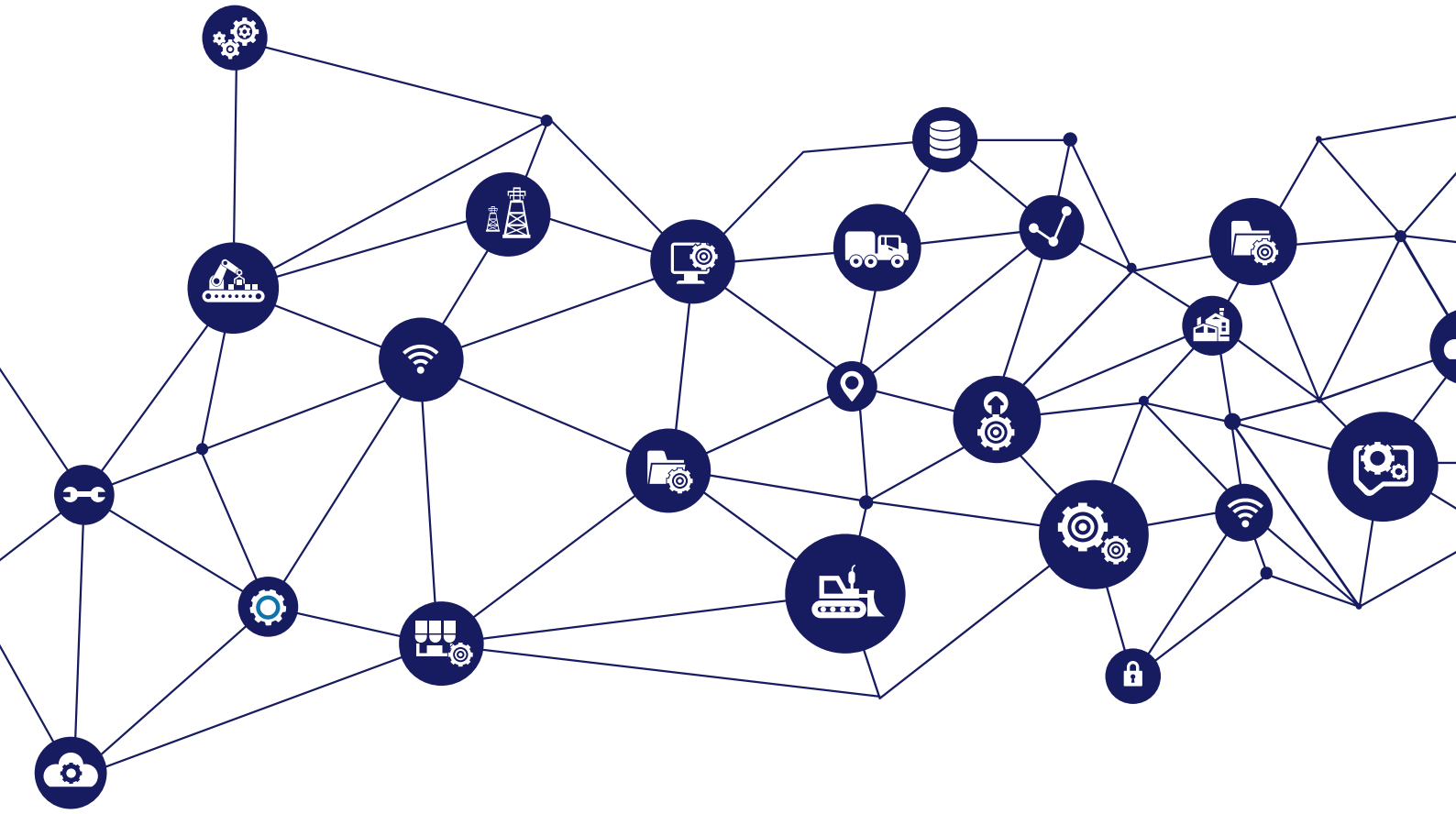
[6] Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1, Edition 1.0 2018-01, International Electrotechnical Commission (IEC).

[7] Guidance for Practice Regarding "IoT Safety/Security Development Guidelines," Information-technology Promotion Agency (IPA), https://www.ipa.go.jp/files/000063228.pdf

[8] C. H. Gebotys, "Security in Embedded Devices", Springer, 2010.

Abbreviations

AGV	Automated Guided Vehicle
AP	Access Point
APT	Advanced Persistent Threat
BLE	Bluetooth Low Energy
BT	Bluetooth
CIP	Critical Infrastructure Protection
CPU	Central Processing Unit
CSMS	Certified Software Measurement Specialist
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service attack
DMZ	Demilitarized Zone
DoS	Denial of Service
EDSA	Embedded Device Security Assurance
EOL	End of Life
ERP	Enterprise Resource Planning
GW	Gateway
HMI	Human Machine Interface
HSM	Hardware Encryption Module
IACS	Industrial Automation and Control System
ID	Identifier (or Identification)
IDS	Intrusion Detection System
IEC	The International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
LPWA	Low Power Wide Area
M2M	Machine to Machine
MAC	Media Access Control
MES	Manufacturing Execution Systems
OLE	Object Linking and Embedding
OPC-UA	OLE for Process Control-Unified Architecture
OT	Operational Technology
PC	Personal Computer
PLC	Programmable Logic Controller
QoS	Quality of Service
RAM	Random Access Memory
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UE	User Equipment
USB	Universal Serial Bus
UWB	Ultra-WideBand
VLAN	Virtual LAN
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System



FLEXIBLE FACTORY
PARTNER ALLIANCE

Contact:
https://www.ffp-a.org/
info@ffp-a.org