FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [MELSEC] -

V2.0

MITSUBISHI ELECTRIC CORPORATION

BCN-P5999-1474-A

Revision history

Date	Document number	Notes
Sep, 2021	BCN-P5999-1474	First edition
Jun, 2022	BCN-P5999-1474-A	Title is changed, and an example of security measures is revised

Contents

Terms and Definitions

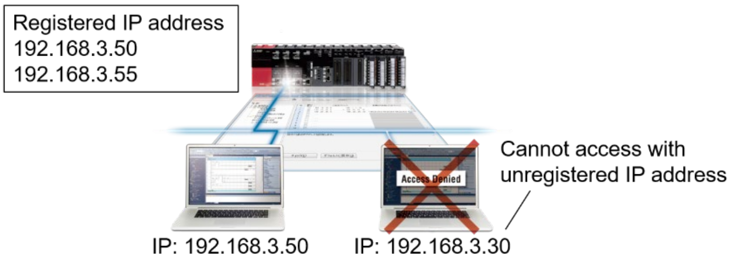
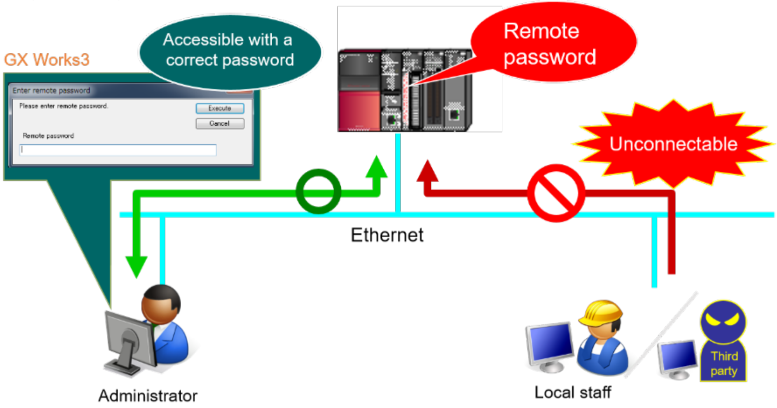
Term	Description
FA[1]	Factory Automation. The use of computer control technologies to automate factories. It also refers to devices used for automation. It is also referred to as Industrial Automation.
IEC62443[2]	Series of the international standards, which provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs), developed the ISA99 committee and adopted by the International Electrotechnical Commission (IEC).
Confidentiality[3]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity[4]	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability[5]	The state that exists when data can be accessed, or a requested service provided within an acceptable period of time.
Factory maintenance	Maintenance in a factory. It is performed to sustain the "Industrial health", "Safety", "Environmental load reduction", and "Operating rate improvement" of the factory.
Supply chain[6]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Vulnerability[7]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Security key authentication	A function implemented in the PLC CPU to prevent unauthorized browsing and execution of programs. The project data locked with a security key can be viewed only with the engineering tool registered with the same security key. In addition, a program locked with a security key can be executed only with a module to which the same security key is registered.
File password	A function that prevents unauthorized reading/wiring of files using a password.
Remote password	A password that prevents unauthorized access to the PLC CPU from remote users.
Block password	A function that prevents unauthorized browsing of programs using a password.
Service setting function	A function that sets Enable/Disable for services on a FA product such as C controller. This function requires security password therefore unauthorized access can be prevented.

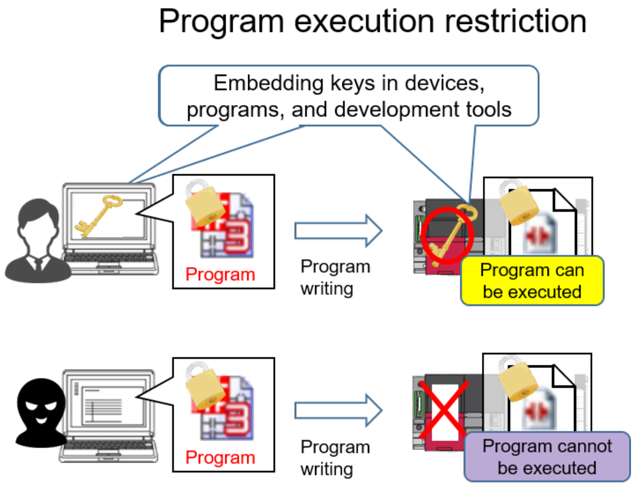
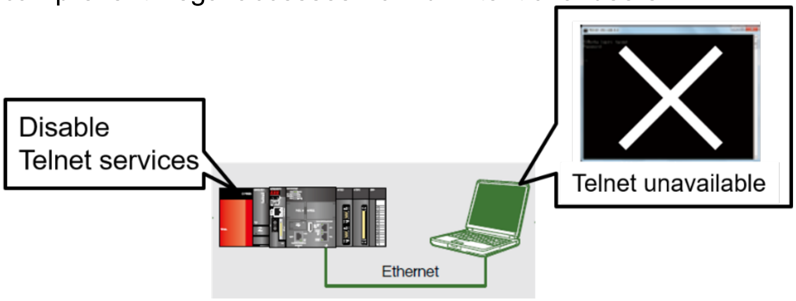
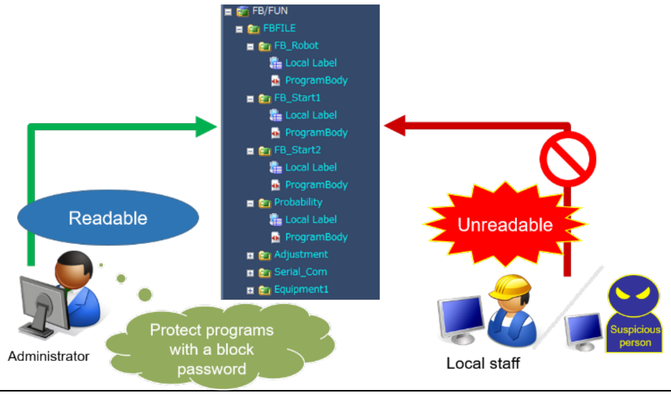
[1] Mitsubishi Electric FA Terminology Dictionary, https://www.mitsubishielectric.com/fa/assist/fa_reference/pdf/k-027-k1209.pdf
[2] International Society of Automation (ISA), https://www.isa.org/intech/201810standards/
[3] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/confidentiality
[4] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/integrity
[5] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/availability
[6] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/supply_chain
[7] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/vulnerability

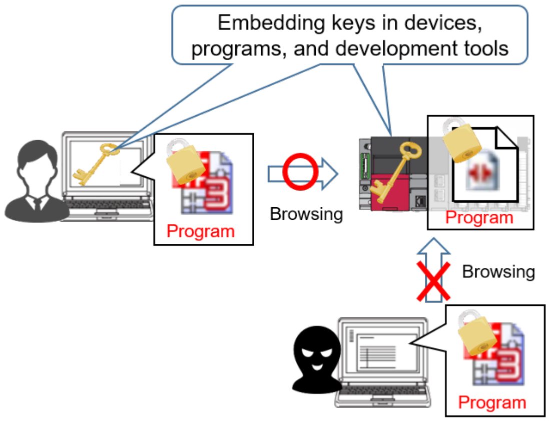
1. Security functions of MELSEC programmable controllers

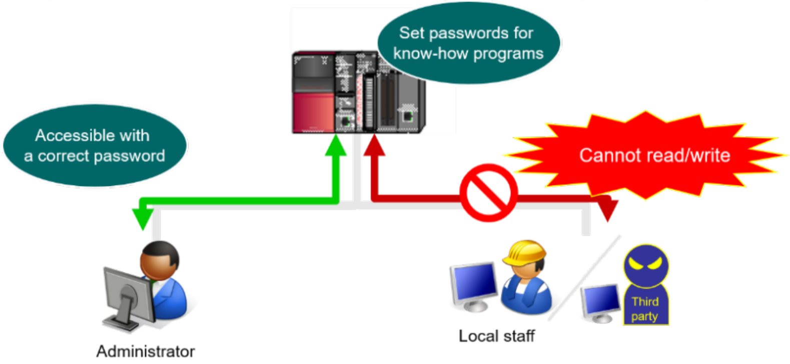
Among the measures for realizing defense-in-depth shown in “FA Products security guideline”, the MELSEC programmable controllers have security functions in "device layer (network)", "device layer (application)", and "device layer (data)". Table 1 shows the security function and purpose in each layer.

Table 1 Security functions of MELSEC programmable controllers

Layer	Purpose of measure	Function	Description
Device layer (network)	Blocking unauthorized communications	IP filter function	The IP addresses of external devices are identified via Ethernet, and the accesses from unauthorized IP addresses are blocked. Blocking the communication from unauthorized IP addresses prevents the accesses to the programmable controller from illegally connected external devices and prevents the illegal update of programs and leakage of the internal data.  Registered IP address 192.168.3.50 192.168.3.55 Access Denied Cannot access with unregistered IP address IP: 192.168.3.50 IP: 192.168.3.30
		Remote password function	A remote password set by parameters is used to authenticate accesses from external devices via Ethernet and restrict accesses from unauthorized external devices. Restricting the access with the password prevents the programmable controller from being illegally accessed from unauthorized persons and external devices and prevents the illegal program updates and internal data leakage  GX Works3 Accessible with a correct password Enter remote password Please enter remote password. Execute Cancel Remote password Remote password Unconnectable Ethernet Administrator Local staff Third party

Device layer (Application)	Program execution restriction	Security key authentication function	A security key is used to prevent programs (in units of program part) from being executed illegally. A program locked with a security key can be executed only with a module to which the same security key is registered. Granting a program a security key prevents the program from being executed by a programmable controller which does not have the correct security key when the program is leaked. This can prevent leaks of production know-how.  Program execution restriction Embedding keys in devices, programs, and development tools Program Program writing Program can be executed Program Program writing Program cannot be executed
	Preventing abuse of service	Service setting function	Services that operate in programmable controller can be set. Restricting the services unnecessary for operating the system can prevent illegal accesses from unintentional users. 
Device layer (Data)	Program browsing restriction	Block password function	A password is used to prevent programs (in units of program part) from being viewed illegally. The password block function prevents programs from being viewed illegally by unauthorized persons using an engineering tool and prevents the leakage of the programs and production know-how.  FB/FUN FBFILE FB_Robot Local Label ProgramBody FB_Start1 Local Label ProgramBody FB_Start2 Local Label ProgramBody Probability Local Label ProgramBody Adjustment Serial_Com Equipment1 Readable Unreadable Administrator Protect programs with a block password Local staff Suspicious person

		Security key authentication function	A security key is used to prevent programs (in units of program part) from being viewed illegally. The project data locked with the security key can be viewed only with the engineering tool to which the same security key is registered. The security key authentication function prevents programs from being viewed illegally by unauthorized persons and prevents the leakage of the programs and production know-how. Program browsing restriction  Embedding keys in devices, programs, and development tools Program Browsing Program Browsing Program

Device layer (Data)	File viewing restriction/writing restriction	File password function	In programmable controllers, a password is used to prevent unauthorized reading/wiring of files. Preventing illegal reading/writing with a file password can prevent a machine malfunction and production stop due to writing of illegal programs and prevent the leakage of the programs and production know-how due to illegal reading.  Set passwords for know-how programs Accessible with a correct password Cannot read/write Administrator Local staff Third party
		File access restriction	File attributes can be set for a file in C controller. Setting file attributes restricts the accesses to the target file to prevent manipulation and leakage of files to the public by unauthorized users.

2. Security function list of MELSEC programmable controllers

The MELSEC programmable controllers have security functions that can be utilized for defense-in-depth and security functions that can be utilized for operation. Table 2 lists the functions that can be utilized for defense-in-depth and support of each model of the MELSEC programmable controllers. For details of each function, refer to the manual of the product.

Table 2 List of security functions that can be utilized for defense-in-depth in each model

Purpose of measure	Function name	MELSEC iQ-R		MELSEC iQ-F	MELSEC Q		MELSEC L
		CPU	C controller	CPU	CPU	C controller	CPU
Blocking unauthorized communications	IP filter function	✓	✓	✓	-	*1	-
	Remote password function	✓	-	✓	✓	-	✓
Program execution control	Security key authentication function	✓	*2	✓	-	*3	-
	Individual identification information	-	✓	-	-	✓	-
Preventing abuse of service	Service setting function	-	✓	-	-	✓	-
Program browsing restriction	Block password function	✓	*4	✓	✓	*4	-
	Security key authentication function	✓	*4	✓	✓	*4	-
File viewing restriction/writing restriction	File password function	✓	*4	✓	✓	*4	✓
	File access restriction	-	✓	-	-	✓	-

*1: By using the IP filter library, it can be executed in the user program.

*2: A simple authentication can be implemented in a user program by using the individual identification information of C controller with C controller module dedicated functions.

*3: A simple authentication can be implemented in a user program by using the individual identification information stored in a specific memory.

*4: When programs are read or written via FTP, the password authentication of the FTP function is used.

Table 3 lists non-defense-in-depth security functions that can be utilized for the operation described in “FA products security guideline" and support of each model of the MELSEC programmable controllers.

Table 3 List of security functions that can be utilized at operation in each model

Function	Description	MELSEC iQ-R		MELSEC iQ-F	MELSEC Q	
		CPU	C controller	CPU	CPU	C controller
Memory initialization	The data in the memory is deleted to prevent the information leak.	✓	✓	✓	✓	✓
Self-diagnosis function	Abnormal operation is detected to prevent malfunctions and illegal operation.	✓	✓	✓	✓	✓
Event history (error history) function	By collecting and saving the errors and abnormalities occurred in the MELSEC programmable controller or on the network, they can be used to detect the cause of the problems.	✓	✓	✓	✓	✓
Data logging function	The specified data is collected at the specified interval or any timing, and the collected data is saved to an SD memory card or function memory as files.	✓	-	✓	✓	-
Backup/restoration function	By taking the backup of the data in the MELSEC programmable controller to an SD memory card or compact flash memory card, the state can be restored to the normal state when an error occurs.	✓	*1	✓	-	*1

*1: It can be performed by using a script file.

3. Examples of security measures

This chapter provides examples of security measures under the defense-in-depth concept described in the FA PRODUCT SECURITY GUIDELINE. When applying the concept of defense-in-depth to FA systems, identify what to protect and take security measures depending on the threats.

3.1. Features of factories and examples of items to be protected

Figure 1 shows a system configuration example. It shows a system for data acquisition and management of traceability in an automobile factory. The factory consists of multiple production lines, each of which consists of the programmable controller for control stored in the control panel, the programmable controllers on the production line, and devices connected to the programmable controllers. In the server room, the production lines are monitored by SCADA[8], and the traceability data acquired is stored in the database server. The server room is connected to the tablet PC on the production site via a wireless network and also connected to the office via the intranet.

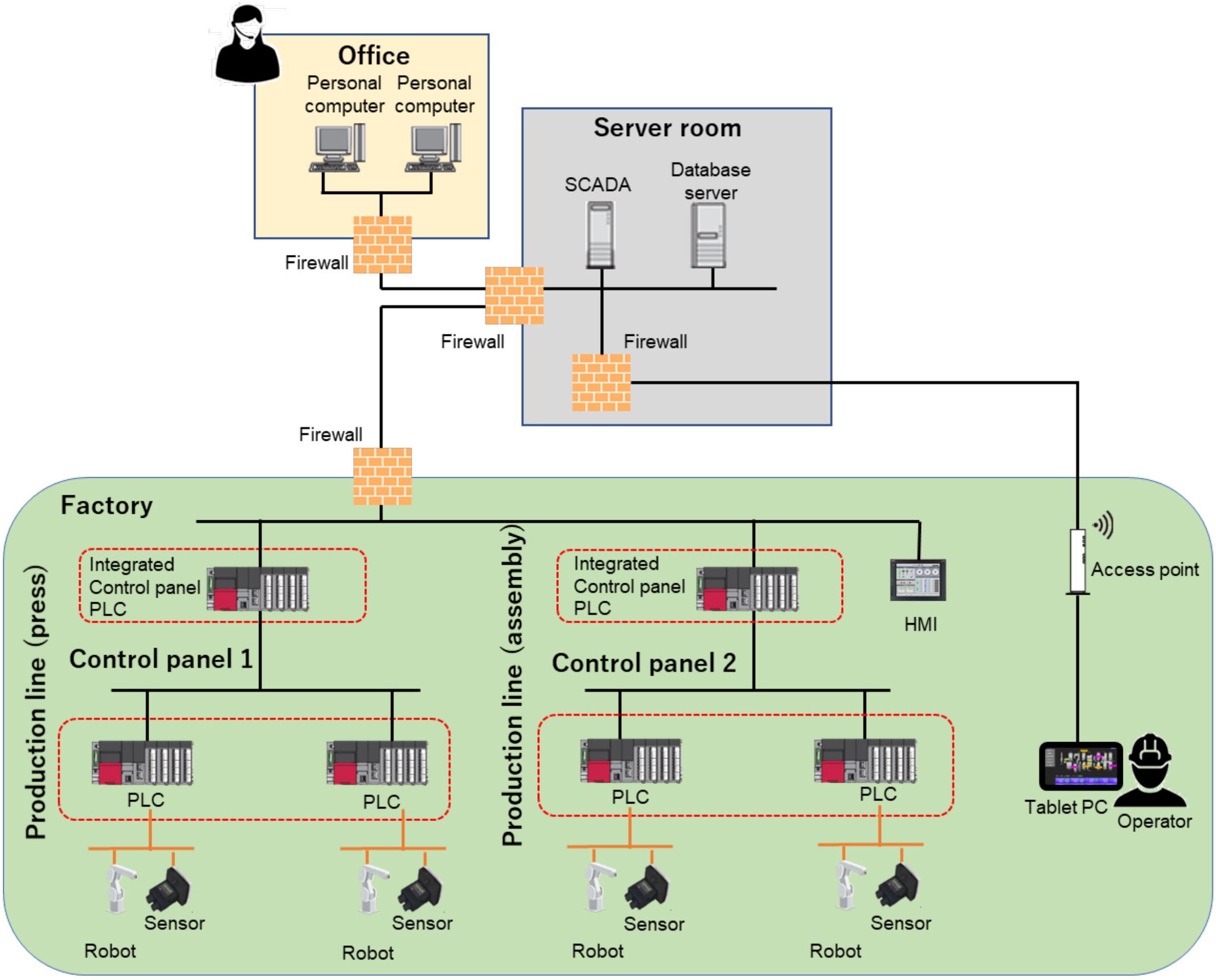


Figure 1 System example

[8] Supervisory Control and Data Acquisition

The features of factories and examples of the items to be protected corresponding to each feature are listed in Table 4.

Table 4 Features of automobile factories and items to be protected

Features	Example of items to be protected
Remote monitoring via the remote connection is performed.	Availability of remote connection, confidentiality of operating status
SCADA controls all the devices.	Availability and integrity of SCADA
A large amount of traceability data is exchanged among the SCADA server, database server, and each device group.	Availability of the network among the SCADA server, database server, and the device group
Shipment is impossible if the inspection data or traceability data is falsified.	Integrity of traceability data
Handling of recipe data is important. Data will be copied by other companies if it is leaked. If the data is falsified, products cannot be manufactured correctly.	Confidentiality and integrity of recipe data

3.2. Example of possible threats

In this system configuration example, it is important to protect and manage the traceability data collected by SCADA. The possible threats include the falsification and destruction of data collected from devices by intrusion into the factory via the network, and the falsification and destruction of traceability data by intrusion or malware infection of devices in the server room.

3.3. Points of security measures

The following shows the three points of security measures for this system configurations considering what to protect from what kind of threats.

(1) Protection of the server room:

- Physical security in the server room (such as access control)
- Installing[9] the antivirus or application white list to the SCADA server
- Setting the authentication and authority of the users who use the SCADA server (administrators, engineers, and operators)
- Sealing the USB ports of SCADA server and database server physically
- Security education for operators

(2) Protection of the FA system-related information that can be browsed from the office:

- Access authority setting of the FA system-related information (design information, manufacture)
- Education for office staffs

(3) Measures associated with connection to a wireless network:

- Security education for operators
- Installing the firewall and encrypting the wireless network communication (such as VPN)
- Adding the firewall and network intrusion protection function (IPS or equivalent)
- Separating the remote maintenance circuit network and FA system network (using VLAN)

[9] Before installing them to the existing environment, it is necessary to inspect them in another similar environment so that production will not be affected.

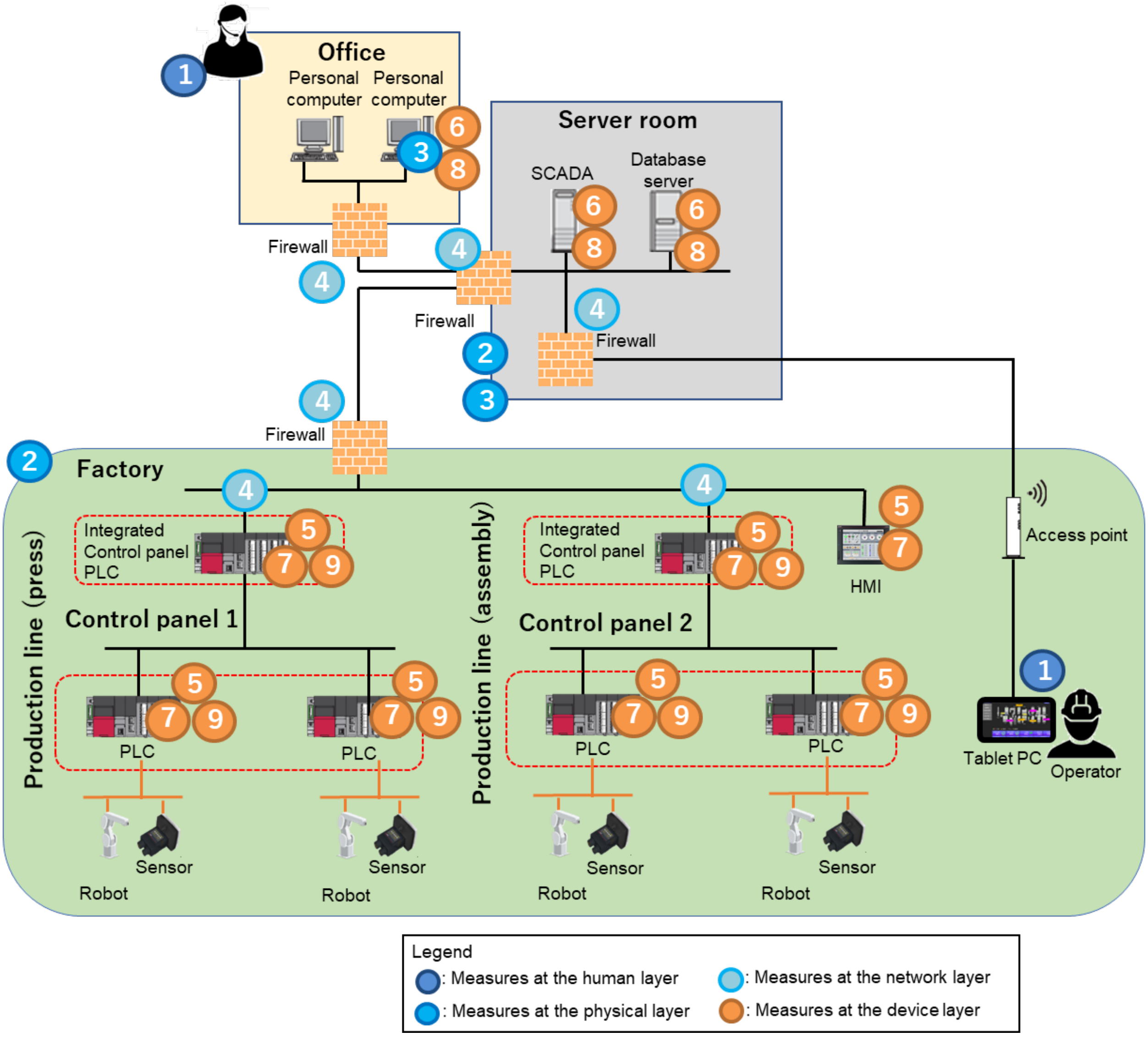


Figure 2 FA system in an automobile factory and defense-in-depth example

Table 5 Example of security measures with defense-in-depth structure

Layer of defense-in-depth	No. in the figure	Function item
Human layer	1	Minimizing the impact by education and prompt instructions
Physical layer	2	Access control
	3	Sealing the USB port and network switch port physically
Network layer	4	Firewall, VPN, IPS, IDS, VLAN
Device layer (Network)	5	★ IP filter, ★ remote password
Device layer (Application)	6	Antivirus, application white list
	7	User authentication, ★ security key authentication, ★ service setting, ★ event history
Device layer (Data)	8	Data encryption, database protection
	9	★ Fie password, ★ block password, ★ file access restriction

The measures marked with ★ are supported by the MELSEC programmable controller.

4. Q&A

[Q1]:

What kind of policies do the MELSEC programmable controllers of Mitsubishi Electric have for product security measures?

[A1]:

Our company adopts the following basic policies: "1) Compliance", "2) Building organizations and systems to ensure safety and security", "3) Promoting defense-in-depth in FA systems", "4) Protection of MELSEC programmable controller in product life cycle", and "5) Reduction of security risks in supply chain". For details, refer to "2 Basic Security Policy for MELSEC Programmable Controllers" of “FA products security guideline” of this document.

[Q2]:

Do the MELSEC programmable controllers of Mitsubishi Electric follow any security standards?

[A2]:

We are preparing to comply with the international security standards for control systems (such as IEC 62443).

[Q3]:

How are cyber security measures taken for the MELSEC programmable controllers of Mitsubishi Electric?

[A3]:

As a company providing devices and services for promoting factory automation, we take the following measures based on the concept of international security standards (IEC 62443).

- Building organizations and systems in our company to ensure security
- Implementing security functions in products and creating security guidelines
- Protection of MELSEC programmable controllers in the production life cycle (planning, design, production, operation, and disposal)
- Security measures in the supply chain

For details of each item, refer to "3 Approaches on FA Cyber Preservation" of the “FA products security guideline”.

[Q4]:

What does Mitsubishi Electric do with the MELSEC programmable controllers to protect customers' system and data from security threats?

[A4]:

We are promoting general security measures based on four core policies described in [A3] as general for the MELSEC programmable controllers. For the MELSEC programmable controllers (programmable controllers and C controllers), we implement functions such as IP filter function, user authentication, and security key authentication to reduce the security risk of our customers. In addition, we implement measures to protect MELSEC programmable controllers from evolving attacks considering security in each phase (plan, design, manufacture, operate, and dispose) of the product life cycle.

For the security functions of MELSEC programmable controllers, refer to "Security functions of MELSEC programmable controllers" and "Security function list of MELSEC programmable controllers" in this document. For the production life cycle, refer to "2.2.5 Implementing secure product life cycle" of the “FA system security guideline”.

[Q5]:

How do I consider security measures for the factory?

[A5]:

The priorities of security measures vary depending on what do you need to protect and what kind of threats are possible in your factory. Refer to "3. Construction and Operation of a Secure FA System " of the “FA system security guideline” and "3. Examples of security measures" in this document to consider security measures according to your factory.

[Q6]:

What should I do with the external storage media (such as an SD card) before disposing the MELSEC programmable controller?

[A6]:

To prevent programs and recipe information from being removed, we recommend initializing the external storage media no longer needed to delete the stored information before disposal.

[Q7]:

What kind of measures does Mitsubishi Electric take for procurement of product parts and devices or the software (including updates) used in the design, development, and manufacturing processes?

[A7]:

In order to reduce risks associated with externally procured hardware and software, we raise security awareness by conducting on-site checks with our suppliers and providing guidelines, and we reduce vulnerabilities through incoming inspections. We also instruct our suppliers on how to prevent leakage of design information and programs related to our products, including security-related information.