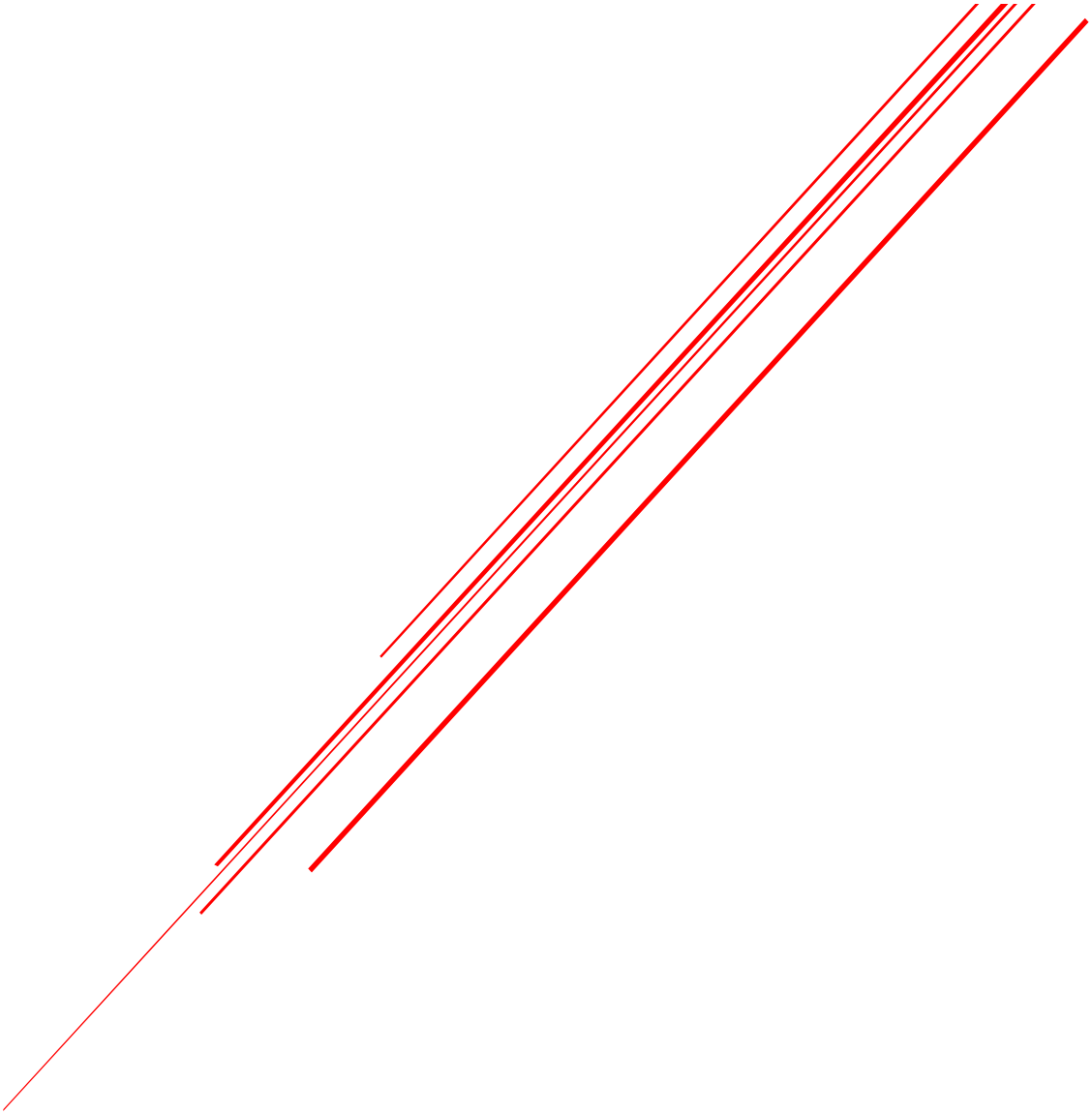
FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [GOT3000] -

V1.0



MITSUBISHI ELECTRIC CORPORATION

BCN-P5999-1860-A

Revision history

Date	Document number	Notes
Dec. 2025	BCN-P5999-1860-A	First edition

Contents

Terms and definitions

Term	Description
FA	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.[1]
IEC 62443	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 by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC).[2]
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information[3].
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.[3]
Availability	The state that exists when data can be accessed, or a requested service provided within an acceptable period of time.[3]
Supply chain	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.[4]
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.[5]
Engineering tool	A generic term for "GT Designer3 (GOT3000)" and "Data Transfer Tool", which are the peripheral software of the GOT3000 series.
External devices	A generic term for devices that can communicate with the GOT3000 series. They include GOTs, CPU modules, personal computers, and applications that run on personal computers.
Screen operation	Refers to operations of the engineering tool, such as manipulation of objects on the base screen or other screens and screen switching (including starting of utility or add-on function).
Access	Reading, writing, editing, moving, and deleting data stored in the GOT3000 series.
Event	Certain actions and processing that occur in the GOT3000 series.
User	A generic term for the people who operate, access, and manage the GOT3000 series screens.
Event history	Logs that contain events that occurred in the GOT3000 series. The event history is recorded with the operation log and system log.
Protected assets	A generic term for the package data, resource data, and security function setting information stored in the GOT3000 series.
Authentication	Collates the operator name and password entered by the user with the operator management information.
Password authentication	Processing to verify the password entered by the user with the operator management information file.
Operator information	Setting information of each operator, such as the operator name and the password.
Group information	Setting information of the group, such as the group name and the operation authority settings.
Operator authentication setting	Common settings relevant to operator authentication.
Operator management information	A generic term for operator information, group information, and operator authentication settings.
Operator management information file	The file that stores the operator management information.

[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/supply_chain
[5] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/vulnerability

Term	Description
Operation authority	The authority for enabling individual users to operate GOT3000 series screens or access the GOT3000 series.
Administrators group	The group defined by the system to which all the operation authorities are granted.
Users group	The group defined by the system to which the user screen operation authority is granted.
User-defined group	The group for which the user can set the group name and operation authority.
User screen	A generic term for the base screen, window screen, mobile screen, and add-on screen.
Certificate	The file required for the encrypted communication between the GOT3000 series and the external devices.
Certificate setting information	The setting information file required for the GOT3000 series to create the certificate.
Non-contact tag	A tag from which information can be read by scanning it with a mobile terminal.
Mobile code	A computer program imported from another personal computer via a network and automatically executed without requiring user operations such as downloading and installing.

1. Introduction

1.1 Background

With the rapid development of the Internet and IT/IoT technologies, the use of IT in FA systems is growing to improve productivity in factories. FA systems have been generally assumed to be "not infected with malware and not subject to cyber-attacks because they are 'private' and 'closed'". However, the growing use of IT increases security risks in FA systems. In 2017, a major security incident was caused by malware called WannaCry12 which initially targeted IT systems, and subsequently brought the factories of multiple companies to a halt. (Figure 1)

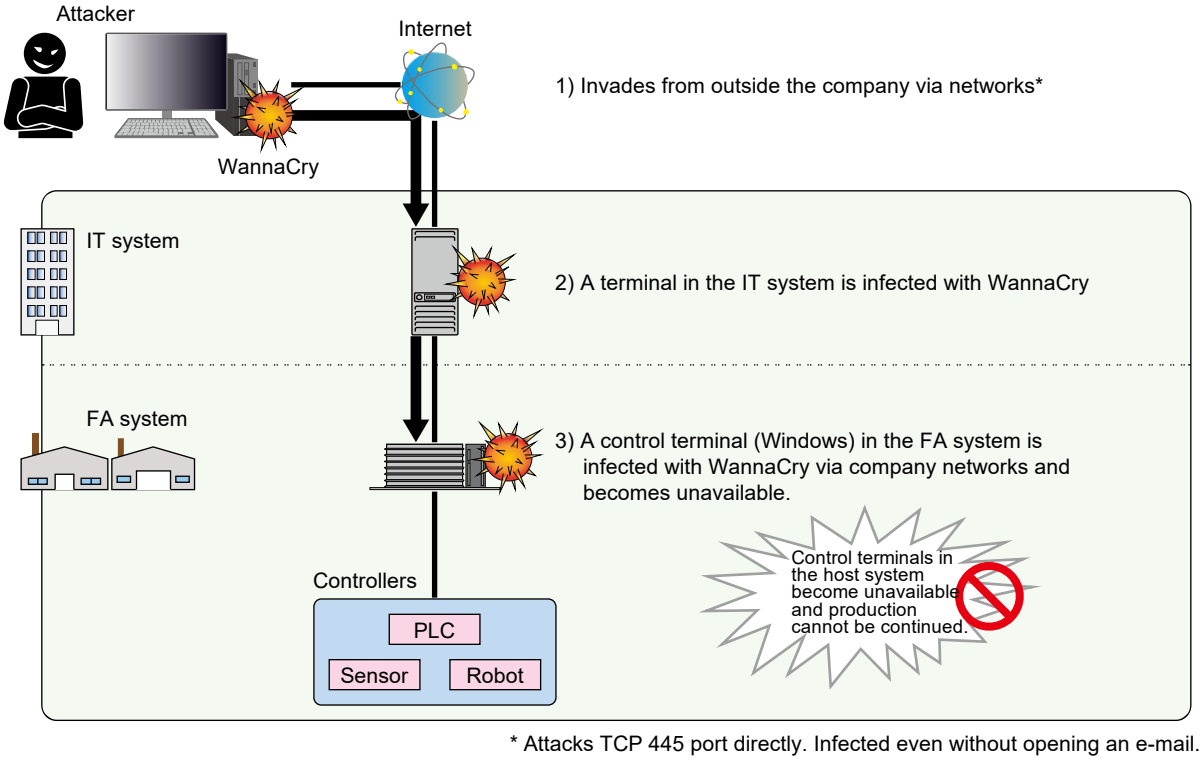


Figure 1 Examples of infection route of WannaCry into the FA system and damage

To protect FA systems from such threats, it is important to hierarchically combine multiple security measures from physical security for factories such as access control to cyber security measures for networks and FA devices in factories. This improves security by "raising the difficulty and costs of mounting attacks " and "enhances the ability to detect and prevent attacks" thereby reducing the opportunity and influence of attacks. This concept for security measures is called "defense-in-depth", and is recommended in the international standard IEC 62443[6]. As a company manufacturing and selling FA products, Mitsubishi Electric (hereinafter referred to as "our company") has started developing GOTs compliant with IEC 62443 to provide customers with safe and secure FA systems.

[6] For information on IEC 62443, refer to the "FA SYSTEM SECURITY GUIDELINE".

1.2 Defense-in-depth to protect FA products

Defense-in-depth in security measures is the concept of taking measures from different viewpoints such as "human operation", "device and facility use", "network access", "data access", and "application execution". Our company separates these viewpoints into viewpoints related to environments (outside of the product) and defense-in-depth related to the inside of the product, and defines them as the "human layer", "physical layer", "network layer", and "device layer" (Figure 2). Defense-in-depth allows the influence of attacks to reduce by raising the costs of mounting attacks and enhancing the ability to detect and prevent attacks.

The security function of our products is one of countermeasures at the device layer or network layer in defense-in-depth. To protect FA systems from cyber-attacks, countermeasures are required at each of the human layer, physical layer, network layer, and device layer. For example, it is recommended to consider the installation of firewalls for preventing intrusion into the factory network, the installation of anti-virus software in personal computers, and the entry and exit control at factories.

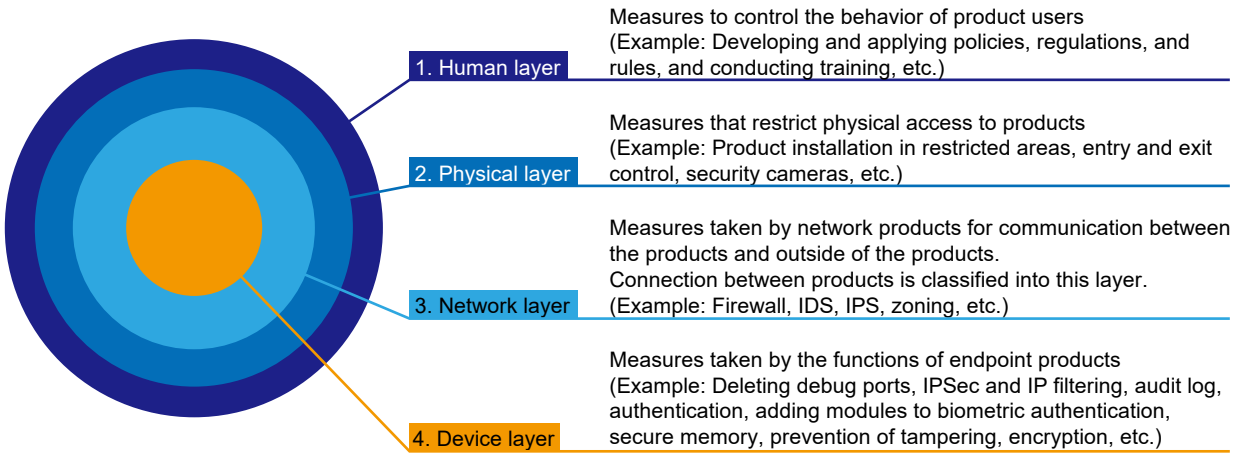


Figure 2 Concept of defense-in-depth

2. Security of the GOT3000 series

2.1 Positioning of this chapter

The purpose of this guideline is to explain the way of thinking of our company about the security of GOT3000 series, and to provide the following information so that the GOT3000 series will be used safely and securely in the customer's FA system.

- Security strategy in the GOT3000 series (2.2):
  Identifies potential threats to the GOT3000 series, and explains the security threat response policies. The response policies include those performed by the GOT3000 series itself and those performed in combination with other products.
- Method for installing the GOT3000 series (2.3 and 2.4):
  Explains the security functions of the GOT3000 series, how to set the functions, and how to install the GOT3000 series in the FA system.
- Method for operating and maintaining the GOT3000 series (2.6):
  Explains recommendations on how to manage users and passwords for operation of the GOT3000 series.
- Method for removing and discarding the GOT3000 series (2.7)
  Explains recommended methods (e.g., the deletion function of data in the product) when removing and discarding the GOT3000 series.

For the detailed specifications and operation methods of each function of the GOT3000 series, refer to the following manuals as needed.

- GOT3000 Series User's Manual (Utility Function, Maintenance and Inspection)
- GT Designer3 (GOT3000) User's Manual (Screen Design)

Read this guideline and the related manuals listed above carefully to fully understand the security of the GOT3000 series, and use it to establish and maintain a safe and secure FA system.
For the basic security policies for our FA products, including the GOT3000 series, our efforts in regard to product lifecycle, and examples of FA system configurations, refer to the following reference document.

- FA SYSTEM SECURITY GUIDELINE (XFB3-20PS002)
- Basic Security Policy for Factory Automation Products (XFB3-20PS005)

2.2 Security policies for the GOT3000 series

This chapter explains the following contents on the security strategy of the GOT3000 series.

- Assumed usage environments for the GOT3000 series (installation environment, networks, operation and maintenance methods, user tasks, administrator tasks, etc.)
- Threats to the GOT3000 series
- Threat response policies
- Security functions of the GOT3000 series
- Security measures to be taken outside this product

2.2.1 Usage environments assumed for the GOT3000 series

Figure 3 shows an assumed environment in which the GOT3000 series is installed. In addition, Table 1 shows prerequisites for ensuring security in the installation environment in Figure 3. The usage environments, including installation environments and prerequisites, are the basis for the security policies described in the subsequent sections.

The GOT3000 series is assumed to be used in equipment installed in a production site of a factory. In addition to the GOT3000 series, devices connected via the CC-Link IE TSN network or Ethernet are also installed in this equipment, and the inside of this equipment is within the trust boundary[7]. SD cards and maintenance personal computers are connected to the GOT3000 series, but they are located outside the trust boundary because they are portable and can be used outside the equipment. In addition, there is a server room in the factory, and production monitoring personal computers and various servers are installed in the room. Networks in the factory where the GOT3000 series is installed are assumed to be connected to the Internet via firewalls and routers, not directly.

[7] It is the boundary separating an area that premises trust from other areas. As an example, trust boundaries often include security functions such as the authentication function, and users who are successfully authenticated can enter the trust boundary. On the other hand, users who failed to be authenticated cannot access the inside of the trust boundary.

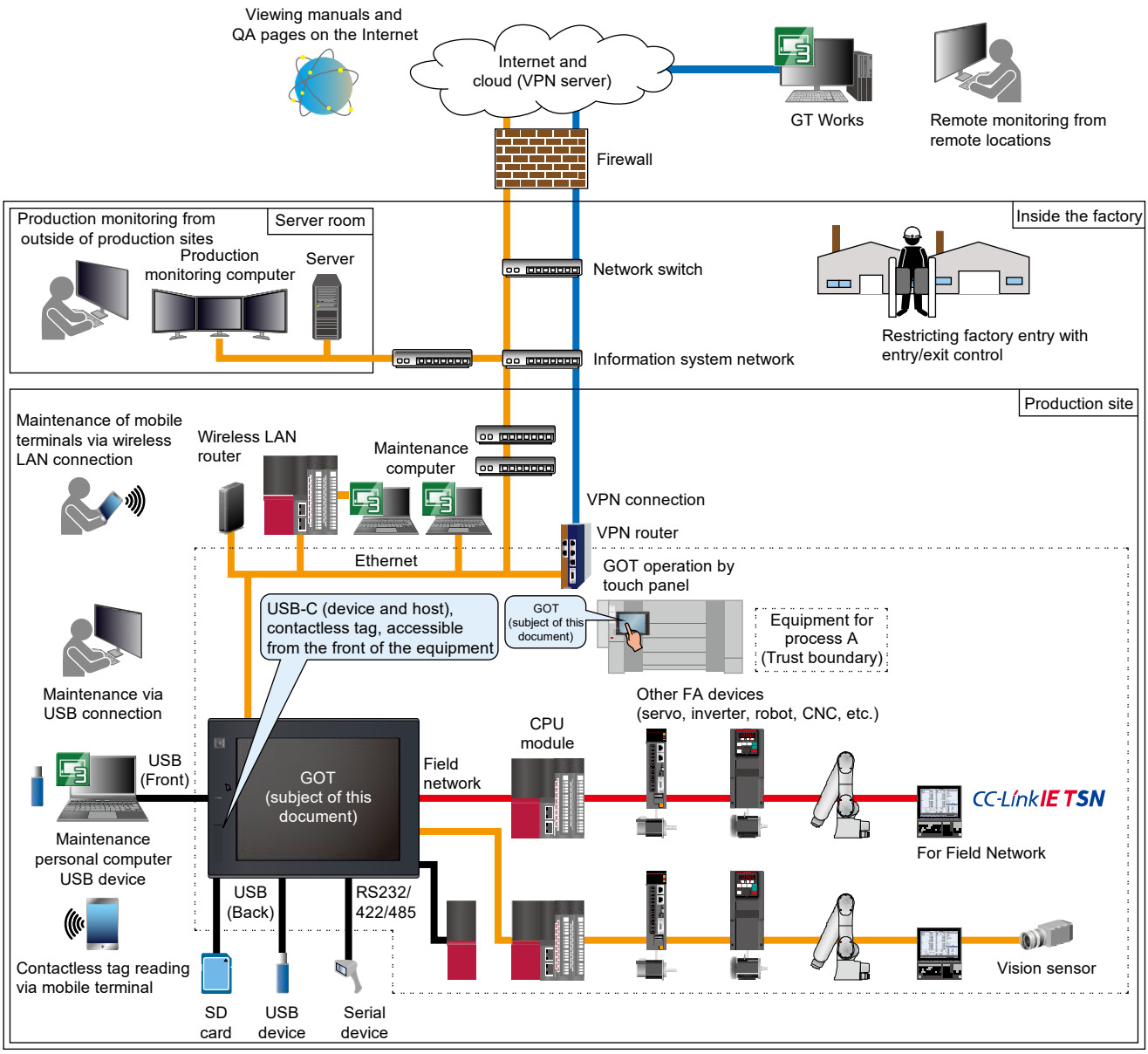


Figure 3 Assumed environment for GOT3000 installation

Table 1 Prerequisites for installation environments

No.	Prerequisite	Description
1	Implementation of entry and exit control	In the factory, persons who enter the area are restricted by the entry and exit control. It is not possible to access FA products (e.g., add or remove a device) in the assembly lines without permission of the administrator.
2	Access to the inside of the operation panel	The GOT3000 series is mounted on the operation panel and locked. It is not possible to access interfaces in the operation panel without permission of the administrator.
3	Storage (SD card, USB memory) management	SD cards and USB memory are used in the operation panel, and persons cannot access interfaces in the operation panel without permission of the administrator.
4	Network partitioning	The network to which the GOT3000 series is connected is separated from external networks by devices such as firewalls and virtual private networks (VPNs).

Table 2 explains the devices and networks in Figure 3.

Table 2 Devices, applications, and networks in installation environments

No.	Term	Description
1	CPU module	A built-in device that executes various functions according to inputs from field devices (e.g., switches and sensors) and controls the field devices (e.g., actuators). Examples of our products are the MELSEC iQ-R and MELSEC-Q series.
2	Production monitoring personal computer	A device in which software for monitoring the status of the control line system is installed. Examples of status monitoring software in our products are GENESIS64 and GT SoftGOT3000.
3	Maintenance personal computer	A device in which an engineering tool necessary for maintenance of the GOT3000 series is installed. An example of the engineering tool in our products is GT Works3. GT Works3 can be connected by the USB or Ethernet. The software can also be connected to the GOT3000 series via our PLC connected by Ethernet.
4	Field Network	A network used for communication between the GOT3000 series and field devices.
5	Information system network	A network that is located inside of the firewall and is used for communication between the GOT3000 series and devices such as production monitoring personal computers. An example of the control information network is the TCP/IP communication of Ethernet.
6	Mobile terminal	A device in which software for monitoring the status of the control line system is installed. An example of the status monitoring function in our products is the GOT Mobile function.
7	Firewall	A device that is equipped with filtering functions such as packet filtering, communication restriction functions such as bandwidth restriction, and address conversion functions such as Network Address Translation (NAT) and Network Address Port Translation (NAPT).
8	Network switch	A device that separates networks with virtual routers or Virtual Local Area Networks (VLAN) by using the information of the network layer in the OSI reference protocol. A combination of network routers and network switches is also possible.
9	External network	A network that is located outside the firewall and out of the range of factory's network administration privileges. An example of external networks is the Internet.
10	Field device	A device that generates values to be input to the CPU module and outputs values generated by the CPU module. An example of field devices is servo.
11	VPN router	A router that is equipped with the VPN function. It performs the encryption of transmission data and the decryption of received data to protect data from peeking and tampering. VPN connection is also possible without using a VPN router by performing the encryption and decryption inside the GOT.

Access to devices and others can be physically restricted by restricting entry to each area in the factory or by applying physical locks to device storage areas. These physical access controls are also important security factors, and Table 3 shows area classification assumed when the GOT3000 series is used.

Table 3 Area classification and operation methods

No.	Term	Description
1	Server room	A room that stores important devices for the continuous operation of the control system, including devices for controlling networks. Measures (e.g., locking or access control so that only specific persons can enter and exit from the room) are taken to protect against unauthorized access and acts of destruction.
2	Device in each process	A device that is equipped with the CPU module and others. To protect against unauthorized access and destructive actions, measures are taken to ensure that only specific individuals among those who are allowed to enter the production site can perform operations (e.g., locking or access control to allow only specific individuals to access or enter/exit). The GOT3000 series is mounted on the operation panel of the equipment.
3	Production site	An area where only users of the control system can enter.
4	Factory	An area that has both accessible areas and a server room.

Users are the operators of the equipment to be installed in the production site of the factory. They work using the GOT3000 series, and have authorities for setting and executing some security functions.
The following describes items that users should perform in the assumed usage environment.

Table 4 Items users should perform

No.	Description
1	Obtain permission to use the GOT3000 series from the administrator.
2	Receive training on security policies from the administrator, and understand procedures.

The administrator manages the equipment to be installed in the production site of the factory. The administrator uses the GOT3000 series to perform operations and management, and has the authority to set and execute all security functions.
The following describes items that the administrator should perform in the assumed usage environment.

Table 5 Items the administrator should perform

No.	Description
1	Assign appropriate authorities to users according to the security policies and their procedures.
2	Fully understand the security policies and their procedures. In addition, get training so that processes and settings can be performed according to the security policies and their procedures.
3	Manage event histories at appropriate time intervals according to the user's manual describing the security.

2.2.2 Threats to the GOT3000 series

Our company considers that Figure 3 in 2.2.1 is the usage environment assumed for the GOT3000 series. Figure 4 shows threats to the GOT3000 series and Table 6 describes such threats based on our knowledge from the risk assessment of the product and common knowledge of attack cases.

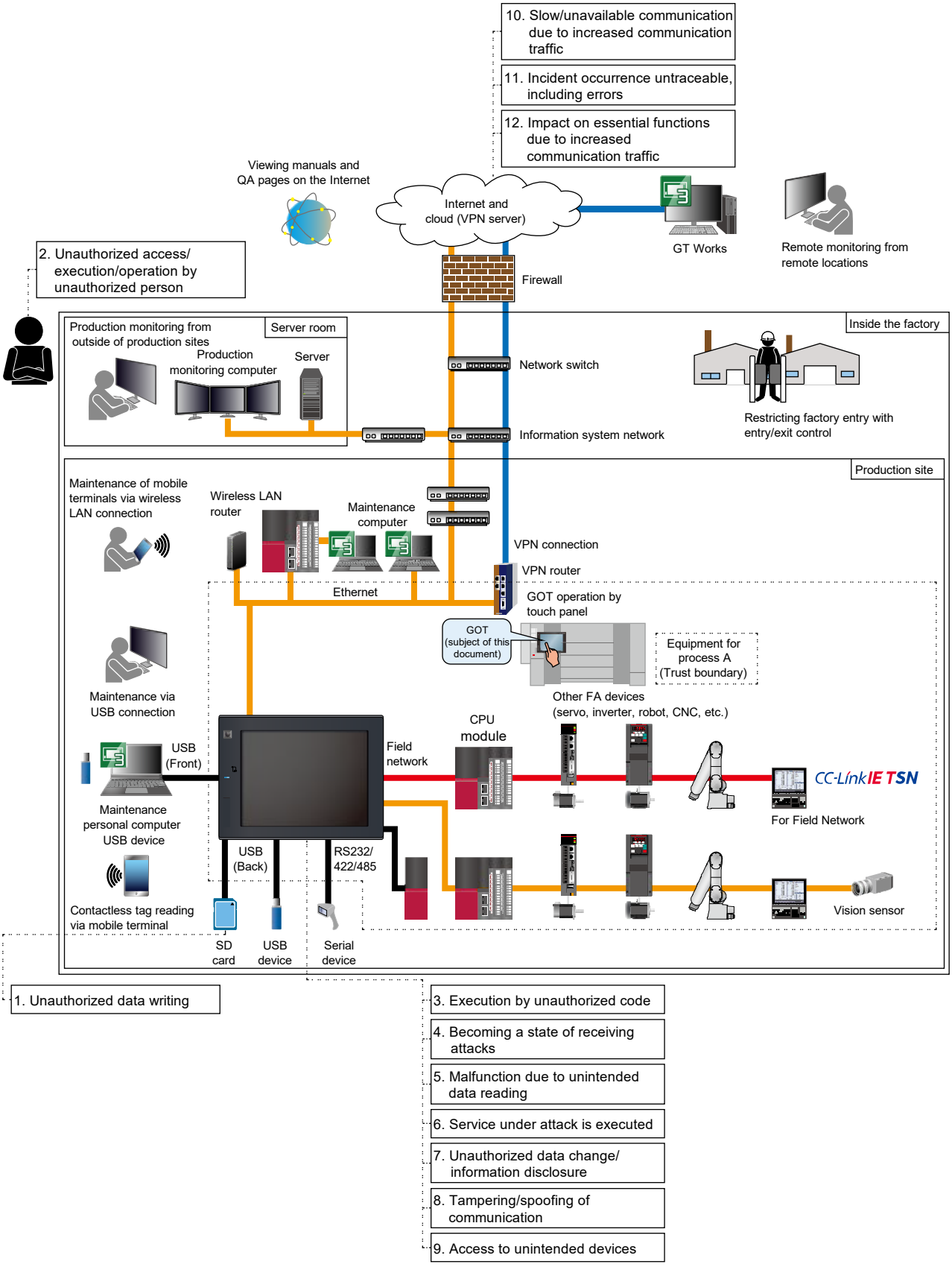


Figure 4 Threats to the GOT3000 series

Table 6 Explanation of threats

No.	Threat name	Description
1	Unauthorized data writing	Unauthorized data may be written due to operational mistakes.
2	Unauthorized access/execution/operation by unauthorized person	A person with no authorities may be able to access, execute, and operate the GOT3000 series due to operational mistakes.
3	Execution by unauthorized code	A malicious code may be loaded due to operational mistakes, and the code may be automatically executed.
4	Becoming a state of receiving attacks	Due to poor maintenance, security problems such as vulnerabilities may remain uncontrolled, resulting in a state where the product is exposed to attacks.
5	Malfunction due to unintended data reading	Configuration errors may cause unintended data to be read, resulting in an effect on operation.
6	Service under attack is executed	Due to inadequate maintenance, functions that are subject to attacks may become executable.
7	Unauthorized data change/information disclosure	Due to inadequate maintenance of the system, data written by the GOT3000 series and saved in a lost controller may be disclosed to a finder of the controller. In addition, due to operational mistakes, data may be illegitimately altered.
8	Tampering/spoofing of communication	Communication data may be tampered or altered. In addition, there is a risk of spoofing by being connected to a disconnected session.
9	Access to unintended devices	If a wrong device is added to the system due to poor maintenance, there is a risk of the occurrence of access to an unintended device.
10	Slow/unavailable communication due to increased communication traffic	If communication traffic in the network increases due to operational mistakes, there is a risk where necessary communication becomes slow or unavailable.
11	Incident occurrence untraceable, including errors	Due to operational mistakes, there is a risk where the occurrence of incidents, including access to unauthorized devices and errors, cannot be traced.
12	Impact on essential functions due to increased communication traffic or others	If network traffic increases due to operational mistakes or other errors, there may be an impact on the behavior of essential functions.

2.2.3 Threat response policies

Figure 5 shows the threat response policies for the GOT3000 series. The response policies include not only those performed by the GOT3000 series, but also those performed in the customer's usage environment.

To implement the defense-in-depth described in 1.2, security measures must also be taken at the human, physical, and network layers, which are difficult to be handled by the GOT3000 series. Therefore, it is necessary to improve security measures for the entire FA system, in addition to measures for the GOT3000 series.

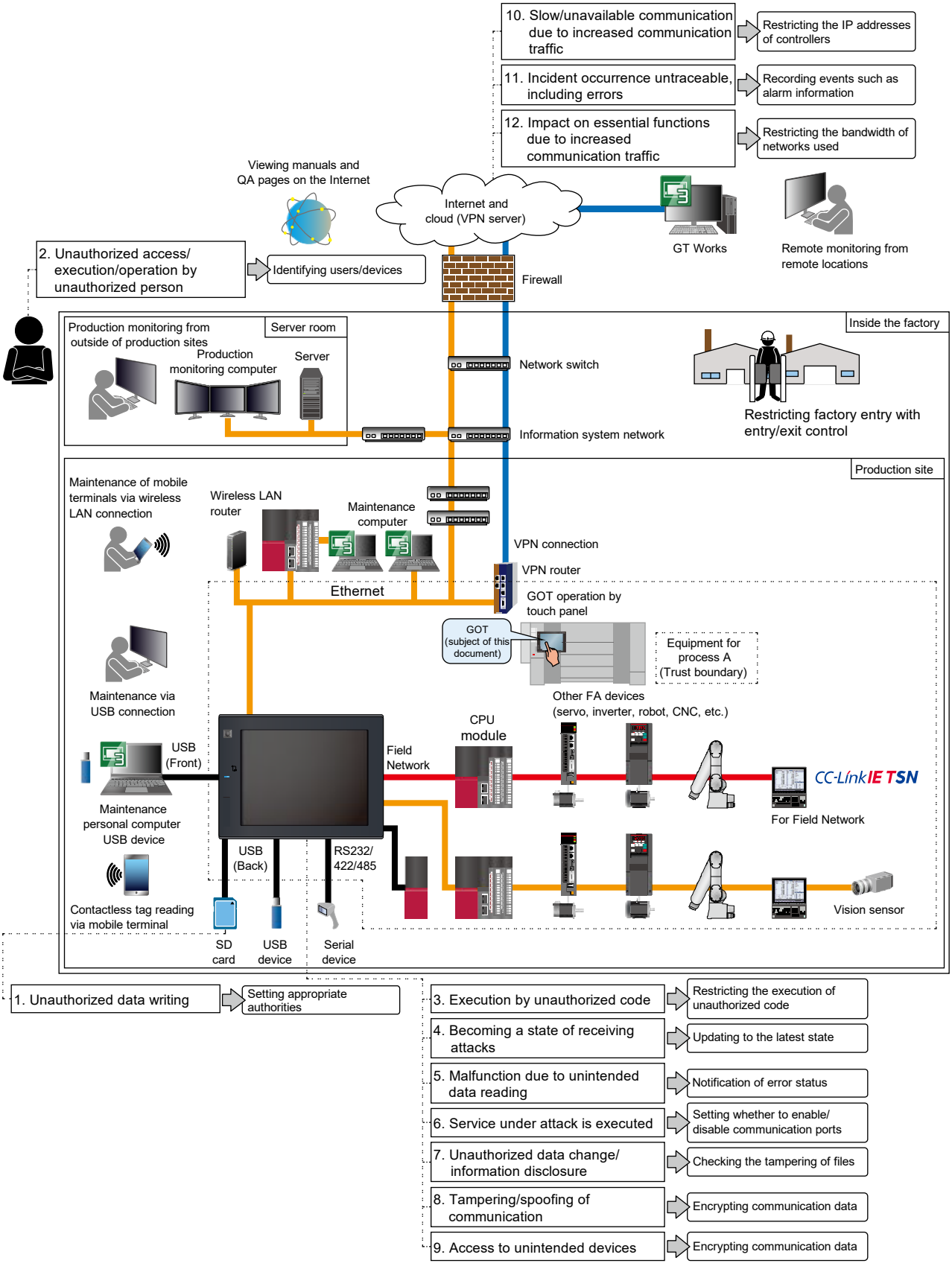


Figure 5 Threat response policies for the GOT3000 series

Table 7 Threat response policies for the GOT3000 series

No.	Threat name	Response policy	Related function/measures
1	Unauthorized data writing	● Setting appropriate authorities	● Operator authentication function
2	Unauthorized access/execution/operation by unauthorized person	● Identifying users/devices	● Operator authentication function
3	Execution by unauthorized code	● Restricting the execution of unauthorized code	● Mobile code execution control function (disables JavaScript)
4	Becoming a state of receiving attacks	● Updating to the latest state	● Firmware update function
5	Malfunction due to unintended data reading	● Notification of error status	● Operation setting function
6	Service under attack is executed	● Setting whether to enable/disable communication ports	● Port forced close function
7	Unauthorized data change/information disclosure	● Checking the tampering of files	● Information protection function
8	Tampering/spoofing of communication	● Encrypting communication data	● Encrypted communication function
9	Access to unintended devices	● Encrypting communication data	● Encrypted communication function
10	Slow/unavailable communication due to increased communication traffic	● Restricting the IP addresses of controllers	● IP filter function
11	Incident occurrence untraceable, including errors	● Recording events such as alarm information	● Operation log function
12	Impact on essential functions due to increased communication traffic or others	● Restricting the Ethernet communication function	● DoS attack restriction function

2.2.4 Security functions of the GOT3000 series

The GOT3000 series includes the security functions as shown in Table 8 to implement the threat response policies described in 2.2.3.

Table 8 Security functions of the GOT3000 series

Function name	Description	Threat to be handled
Security function setting function	Changes the security-related function operations of the GOT3000 series into the operations required to establish a secured system.	-
Operator authentication function	Restricts users who can access.	1. Unauthorized data writing 2. Unauthorized access/execution/operation by unauthorized person
Mobile code execution control function (disables JavaScript)	Restricts the mobile code that is executed in web browsers.	3. Execution by unauthorized code
Firmware update function	Updates firmware by using the engineering tool.	4. Becoming a state of receiving attacks
Operation setting function	Performs a specific operation if an error occurs, and notifies the user of the error status.	5. Malfunction due to unintended data reading
Port forced close function	Opens/closes the port numbers that are open by default, and sets whether to use them.	6. Service under attack is executed
Input data verification function from external devices	Verifies whether data input from the outside of the trust boundary is in accordance with the specifications.	-
Security verification function	Checks whether the security functions operate according to intended settings periodically.	-
GOT all information initialization function	Deletes all data in non-volatile memory.	-
Information protection function	・Checks that files affecting control have not been tampered. ・Protects the confidentiality of owned security information by encryption or access control by operator authentication.	7. Unauthorized data change/information disclosure
Encrypted communication function	Encrypts the communication data for communication with target devices across the trust boundary.	8. Tampering/spoofing of communication 9. Access to unintended devices
IP filter function	Restricts the IP addresses of the devices to be connected.	10. Slow/unavailable communication due to increased communication traffic
Operation log function	Records security-related events using the alarm monitoring function and operation log function in security mode 2.	11. Incident occurrence untraceable, including errors

Function name	Description	Threat to be handled
DoS attack restriction function	Restricts the Ethernet communication function of the GOT3000 series when a DoS attack occurs.	12. Impact on essential functions due to increased communication traffic
GOT data package acquisition function	Batch acquisition of data in the GOT to a data storage such as an SD card or USB memory.	-
Restore function	Restores the data acquired using data package acquisition into the data storage by transferring the data to the GOT.	-

2.2.5 Security measures to be taken outside this product

Figure 6 and Table 9 show the recommended security measures to be implemented in the customer's usage environment, considering the prerequisites (Table 1) for the usage environment (Figure 3) of the GOT3000 series and the threat response policies (2.2.3).

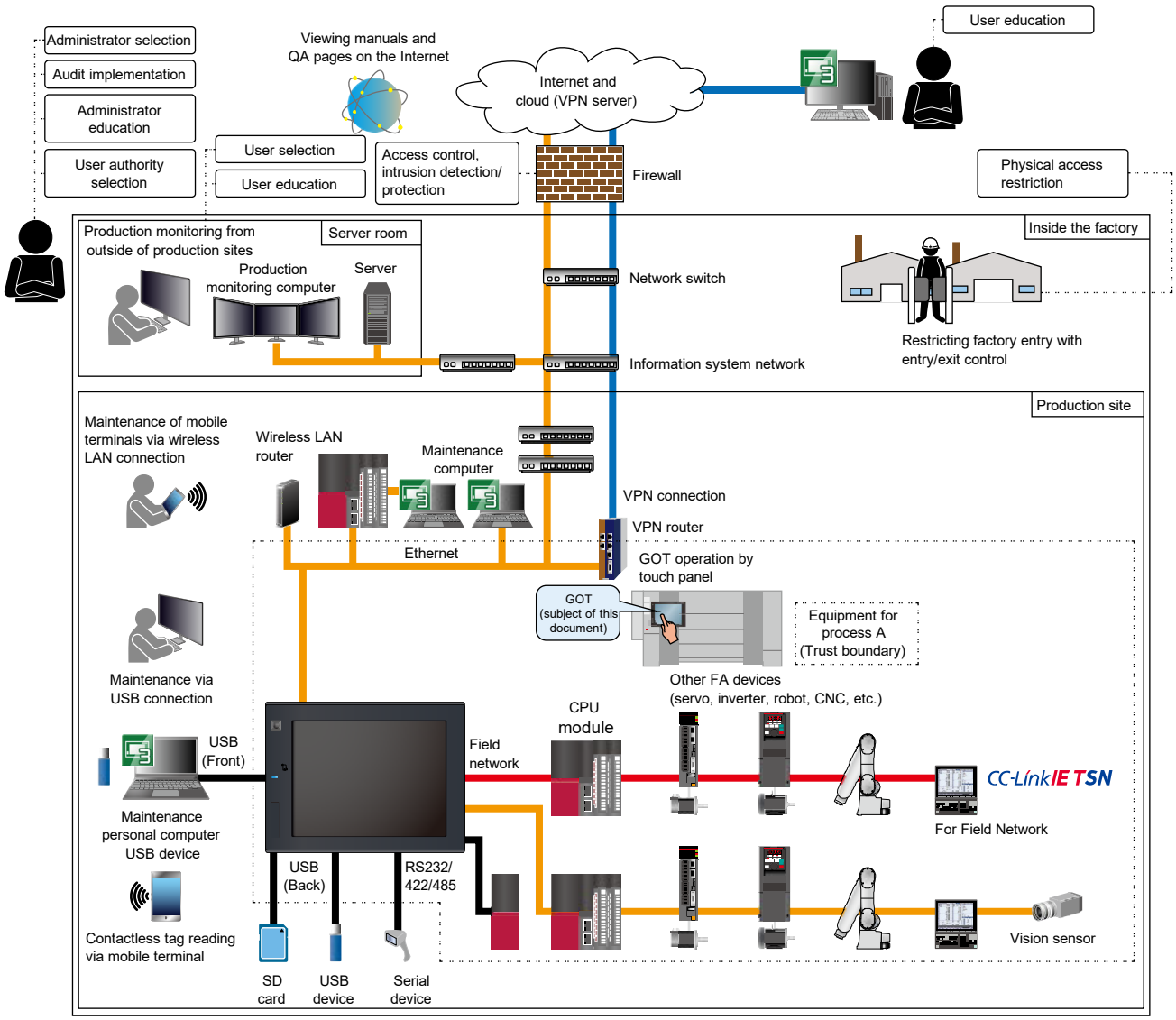


Figure 6 Security measures to be implemented in usage environment

Table 9 Explanation of security measures in usage environment

Layer in defense-in-depth	Measure name	Description	Threat to be targeted
Physical layer	Physical access restriction	Restrict opportunities of being physically accessed by unauthorized persons by installing the GOT3000 series in a safe location under monitoring.	● Unauthorized access/execution /operation by unauthorized person
Human layer	User selection	The GOT3000 series shall be able to be used only by users who have received permission from the administrator.	● Unauthorized access/execution /operation by unauthorized person ● Unauthorized data writing
Human layer	Administrator selection	Select an administrator who will not abuse authorities.	
Human layer	Administrator education	The administrator understands security policies and procedures, and is trained to follow the procedures and configure the security settings.	
Human layer	User authority selection	The administrator assigns appropriate usage authorities to users according to the security policies and their procedures.	
Human layer	User education	Users are appropriately trained by the administrator, and understand security policies and their procedures.	
Human layer	Audit implementation	The administrator audits the operation logs at appropriate intervals according to the user's manual describing security.	● Incident occurrence untraceable, including errors
Network layer	Access control, intrusion detection/protection	Prevent attacks by outsiders from external networks by installing devices such as firewalls.	● Slow/unavailable communication due to increased communication traffic ● Impact on essential functions due to increased communication traffic

2.3 Installation of GOT3000 series

This chapter explains how to install the GOT3000 series in a system and how to set and use the security functions of the GOT3000 series.

2.3.1 Procedures for installing and setting up the GOT3000 series

In a system using the GOT3000 series (Figure 7), it is recommended to operate the GOT3000 series according to the procedure shown in Figure 9 to ensure compliance with IEC62443-4-2 (with each security function set). Following the procedure allows the GOT3000 series to start with its internal data in a secure state. (Figure 8)

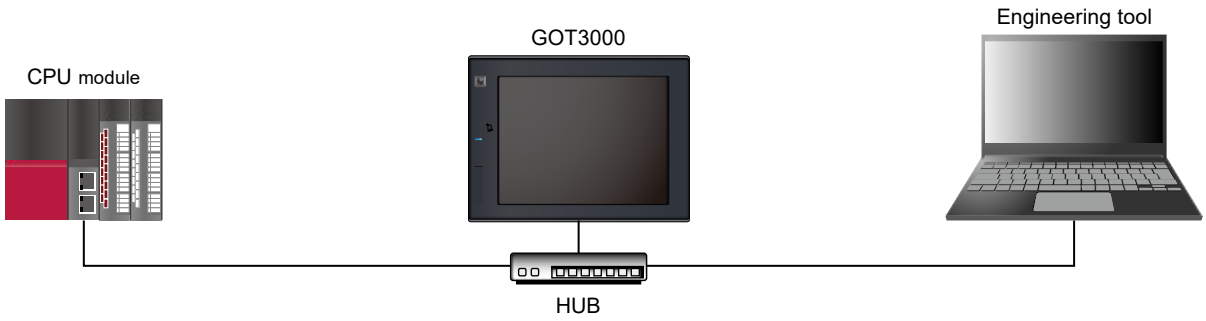


Figure 7 System configuration example

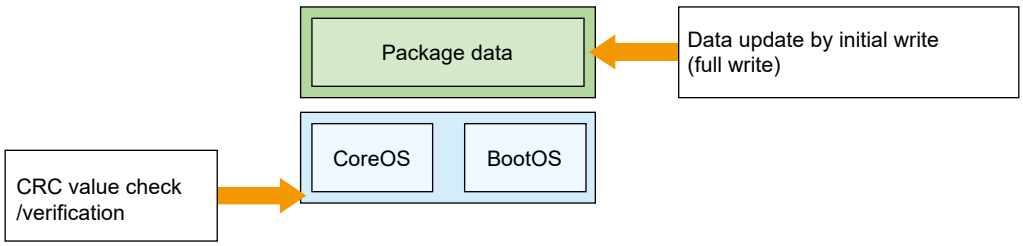


Figure 8 Internal data on the GOT3000 series at the time of factory shipment.

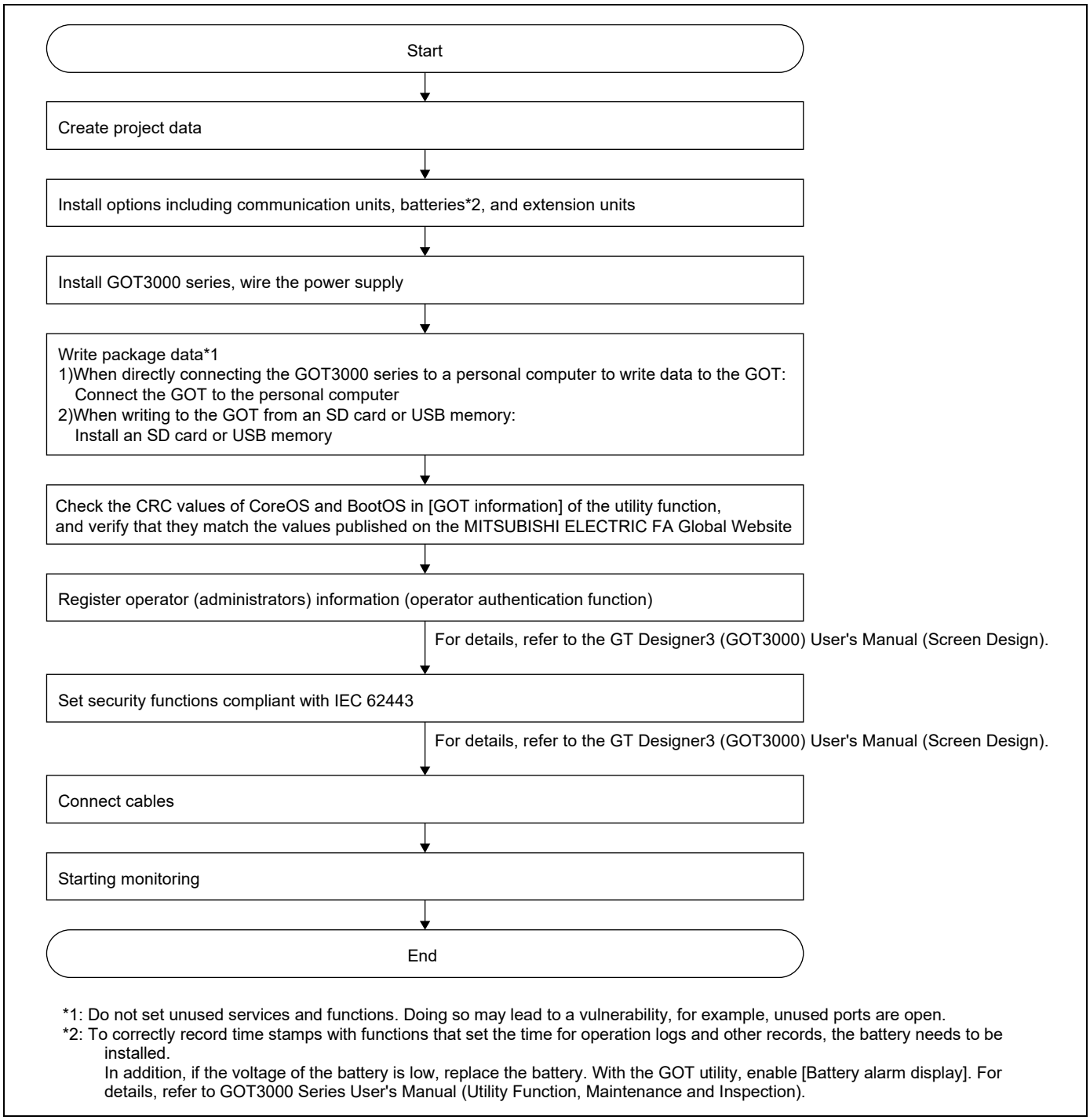


Figure 9 Procedure before operation

・Security function settings compliant with IEC 62443-4-2 and security policies

Perform the following items (Table 10) as security function settings compliant with IEC 62443-4-2. Also, during operation,

follow the procedure shown in Table 11.

Table 10 Security function settings compliant with IEC 62443-4-2

No.	Item	Settings for security functions	Reference
1	Security function setting function	Set the security mode to mode 2.	2.4.1
2	Operator authentication function	Set the operation authorities for each user group appropriately.	2.4.2
3		Set a password that is not easy to guess.	
4		Change the password periodically.	
5		Set an appropriate message to notify the user at logon.	
6		Protect the network connected with an extension unit of the GOT3000 series by using the security function of the unit itself or a mechanism (e.g., firewall) outside the product because communication requests via the extension unit of the GOT3000 series are not subject to operator authentication.	
7		Set operator authentication before accessing protected assets.	
8	Mobile code execution control function (disables JavaScript)	To disable JavaScript in the web browser, you need to set the GS device. Set the GS device (GS2562.b12).	2.4.3
9	Port forced close function (default open port usage setting function, USB host/device disable function (disables the front USB interface of the GOT))	Enable this function.	2.4.6
10		Close the unused ports with the default open port usage setting function.	
11		Perform communication using the built-in Ethernet port of the GOT3000 series.	
12	GOT all information initialization function	Before disposal, delete all the data stored in the GOT3000 series with the GOT all information initialization function.	2.4.9
13	Information protection function	Enable this function.	2.4.10
14	Encrypted communication function	Enable this function.	2.4.11
15		Encrypt communication with target devices across the trust boundary.	
16		Perform encrypted communication via the built-in Ethernet port of the GOT3000 series.	
17		Set the term of validity of the certificate used for encrypted communication to one year (default setting).	
18		Before using encrypted communication, correctly set the GOT internal time.	
19	IP filter function	Enable this function.	2.4.12
20		Restrict access from the target device with the IP filter.	
21	Operation log function	Set the correct time so that time stamp will be correctly recorded.	2.4.13

No.	Item	Settings for security functions	Reference
22	GOT data package acquisition function Information protection function	Back up the GOT data in an encrypted state using the information protection function.	2.4.15
23	Restore function Information protection function	Use the encrypted GOT data package acquisition file for restoration.	2.4.16
24	DoS attack restriction function IP filter function Port forced close function	As countermeasures against DoS attacks, use the IP filter function, default open port usage setting function, DoS attack restriction function, and other examples of countermeasures against unauthorized access.	2.4.6 2.4.12 2.4.14

- To use the GOT3000 series in compliance with IEC 62443-4-2, perform necessary security functions at each stage of installation, operation, maintenance, and disposal of the GOT3000 series according to the procedure shown in Figure 9.
- Do not set GOT internal devices to OPC-UA tags.
- Check our website for vulnerability periodically, and update the software if any vulnerabilities are found.
- If you change a system device, perform operational verification to confirm that the device is being accessed as intended.
- Ensure that the SD card and USB memory used with the GOT3000 series have sufficient free space. Use the file management function of the GOT3000 series to check free drive space and the size of each file to be used, and select the capacity of the SD card or USB memory based on the expected file size during operation.

Table 11 Implementation items related to security policies and the usage environment

No.	Item	Details	Reference
1	Precautions for removing/disposing of connected devices	When removing or disposing of a device connected to the GOT3000 series, be aware that protected assets (data) may be stored on the device. Before disposing of the device, delete this data or take other appropriate actions.	2.7
2	Connected device	Before use, verify that the devices connected to the GOT3000 series are set and operate as intended.	-
3		When communication with the GOT3000 series is no longer required, end the session immediately.	-
4	Backup implementation and management	The protected assets of the GOT3000 series and connected devices in the system may be lost due to sudden disasters or failures. Perform periodic backups and manage the backup data properly.	2.4.15 2.4.16 2.6
5	Password management	Manage passwords properly to prevent them from being leaked. Do not reuse passwords.	2.4.2

2.4 Methods for setting and using security functions

This chapter explains how to set and use security functions of the GOT3000 series. It also explains important security items and precautions when setting and using each function.

For the GOT3000 series versions that satisfy the security requirements of IEC 62443-4-2, check the Mitsubishi Electric Factory Automation Global Website.

For the operating procedures of the functions, refer to the following manuals.

- GOT3000 Series User's Manual (Utility Function, Maintenance and Inspection)
- GT Designer3 (GOT3000) User's Manual (Screen Design)

This chapter describes the following security functions to satisfy IEC62443-4-2.

- Security function setting function (2.4.1)
- Operator authentication function (2.4.2)
- Mobile code execution control function (disables JavaScript) (2.4.3)
- Firmware update function (2.4.4)
- Operation setting function (2.4.5)
- Port forced close function (2.4.6)
- Input data verification function from external devices (2.4.7)
- Security verification function (2.4.8)
- GOT all information initialization function (2.4.9)
- Information protection function (2.4.10)
- Encrypted communication function (2.4.11)
- IP filter function (2.4.12)
- Operation log function (2.4.13)
- DoS attack restriction function (2.4.14)
- GOT data package acquisition function (2.4.15)
- Restore function (2.4.16)

2.4.1 Security function setting function

The security function setting function specifies the mode of security-related operations of the GOT3000 series for establishing a secure system.

Table 12 Security mode

No.	Security mode	Description
1	Mode 1 (Security mode 1)	GOT2000 series compatibility mode
2	Mode 2 (Security mode 2)	A mode that satisfies the requirements of IEC 62443-4-2 necessary for secure system configuration

According to the security mode, the operations of functions will vary as described below.

Table 13 Differences of functions between the modes

No.	Function	Security mode 1	Security mode 2
1	Operator authentication	Operations on the GOT are possible only on the user-created screens.	Effective for all the operations on the GOT.
2	Screen security (security level and group management specifications)	Select an authentication method from "Level authentication" and "Operator authentication".	The authentication method is "Operator authentication" only.
3	Functional operation security	Set a password for each function.	Disabled (Because operator authentication is used for authentication.)
4	Data transfer security	Set a dedicated password.	Disabled (Because operator authentication is used for authentication.)
5	Operation log function	Records the log of the specified events and operations.	In addition to the specified events and operations, security-related events are logged without specification.

2.4.1.1 Recommended items

- To comply with IEC 62443-4-2, select security mode 2 and configure a secure system.

2.4.2 Operator authentication function

The operator authentication function of security mode 2 restricts screen operation and access to protected assets of the GOT3000 series for each user. In addition, the level and group settings can restrict executable operations by user.
By enabling the operator authentication function, information leakages due to access to the GOT3000 series by unauthorized persons, incorrect device operation due to setting change, or other risks can be prevented.
If the operator authentication function is not enabled, users who can connect to the GOT3000 series can use all functions of the GOT3000 series, which may cause information leakage and other threats such as incorrect device operation.
To use the GOT3000 series in compliance with IEC 62443-4-2, set the security mode to mode 2 in GT Designer3 and perform operator authentication with the operator name and password.

2.4.2.1 Assigning operation authorities to the operator

Assign various operation authorities to operators in the "Group" settings. Therefore, each operator must belong to one group. By setting various operation authorities to groups, an operator can exercise operation authorities on the GOT3000 series within the range of the operation authorities assigned to the group to which the operator belongs.
There are following group types, including Administrators group and Users group by default.

Table 14 User group (security mode 2)

No.	Group name	Operation authority of group	Operation authority setting change
1	Administrators (Administrators group)	Has all the operation authorities.	Not allowed
2	Users (Users group)	Screens set at the operator's level or lower can be operated.	Not allowed
3	User-defined group	The user can set the group name and operation authority.	Allowed

* Multiple groups cannot be set for one operator.

The operators who are set to the Administrators group can perform all operations for the GOT3000 series. Therefore, care should be taken when managing operators who are set to the Administrators group. In addition, when creating a user-defined group, it is recommended to assign minimum operation authorities according to the role of the group to be created.

2.4.2.2 Recommended settings

To use the GOT3000 series in compliance with IEC62443-4-2, set the operator authentication function as follows, perform operator authentication, then access the protected assets.

- Set "Strong" for the strength of password, and set a password that is not easy to guess.
- Enable the password expiration date setting, and change the password periodically.
- Set notification messages for the following information to give warnings to logged-on users when the operator authentication is set. Set notification messages in GT Designer3.
  - Type of equipment to be accessed
  - Responsibility of the operator if the operator has performed operations that affect the equipment
  - Permitting log on only when the operator agrees that operations are recorded in the operation log

2.4.2.3 Precautions

The following describes precautions for using this function.

- Incorrect login

  If authentication fails consecutively the specified number of times or more, it is considered as an incorrect login, and login is blocked for a certain period. Until a certain period passes, a login is blocked even if a different operator name is used.
  - The number of consecutive failed login attempts before a login attempt is considered incorrect and the login prohibition duration can be changed in the settings.
  - Operators with operation rights for operator management information set to "Authorized" can unlock the incorrect login state.
- Operator account lock

  If authentication with the same operator name fails consecutively the specified number of times or more, the account for that operator is locked. The locked operator account cannot be logged in until it is unlocked by the administrator or sub-administrator using the utility operation.
  - If a logged in operator is locked, the operator, once logs out, can no longer log in again until the account is unlocked.
- If the password has expired, the change password screen will appear at the time of login. Login becomes possible after the password is changed.
- Actions when the password is lost

  Delete the operator information of operator who has forgotten the password, and register the operator information again. If the administrator password is forgotten, delete the operator management information file, and register all the operator information again.
- Changing the operator management information

  When the operator management information is updated while logged in, the information is applied at the next login.
- Password expiration date setting

  When the password expiration date setting is enabled, the password expiration date is reset by converting the operator management information file from G3U to CSV using the operator management information conversion tool, changing the password in the CSV file, converting the file back to G3U, and importing it to the GOT3000 series.

- Operator ID External Notification device

  The Operator ID External Notification device is not updated if login does not occur after successful authentication, such as for a password change. Since this device is for reference only, if the device value is changed with a CPU module or other equipment, the ID may not match the currently logged-in operator ID.
- Post-logout screen switching function

  If the hidden screen number is set to "-1", the window cannot be closed by the post-logout screen switching function.
- When automatic logout does not occur

  While an OPC UA client is accessing the OPC UA server (GOT), the operator remains logged in even after the automatic logout time has elapsed.

  If automatic logout is required for the OPC UA server function, configure a mechanism to prevent the OPC UA client from accessing the OPC UA server (GOT) when there is no OPC UA client operation for a certain period of time.

Example) When no operation is performed for a certain period of time, the OPC UA client terminal is locked and cannot be operated until authentication is performed.

2.4.3 Mobile code execution control function (disables JavaScript)

The mobile code execution control function restricts the mobile code that is executed in the web browser of the GOT3000 series.

The mobile code execution control function prevents malicious code from being read and executed.

2.4.3.1 Precautions

This function prevents the execution of JavaScript. It does not determine if the JavaScript code is malicious.

2.4.4 Firmware update function

The firmware update function updates the firmware of the GOT using the engineering tool.

The firmware update function is used to update the firmware version to the latest version and address the known vulnerabilities.

The following are subject to updating.

- CoreOS
- BootOS
- System application

2.4.4.1 Updating CoreOS

Update the CoreOS by using an SD card.

After update is completed, check the GOT utility function "GOT information" to confirm that the CoreOS has been updated.

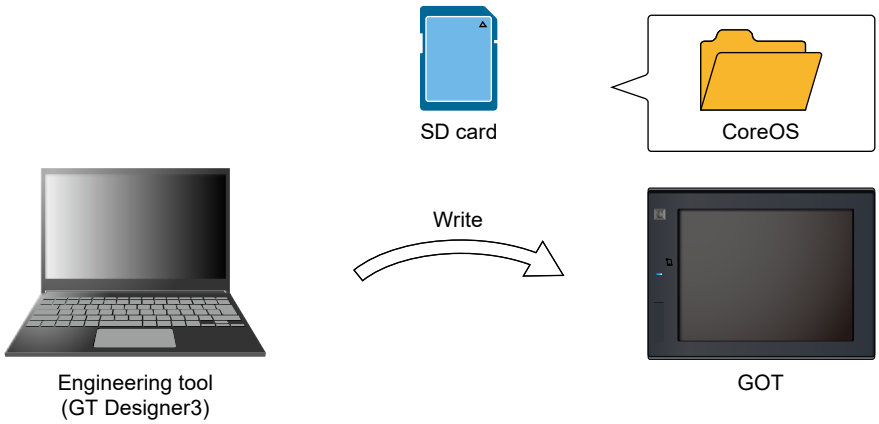


Figure 10 Image of updating CoreOS

2.4.4.2 Updating BootOS

Update BootOS through communication via USB connection from the engineering tool or by using data storage such as USB memory or SD card.

After update is completed, confirm that BootOS has been updated by checking the "GOT information" of the utility function of the GOT.

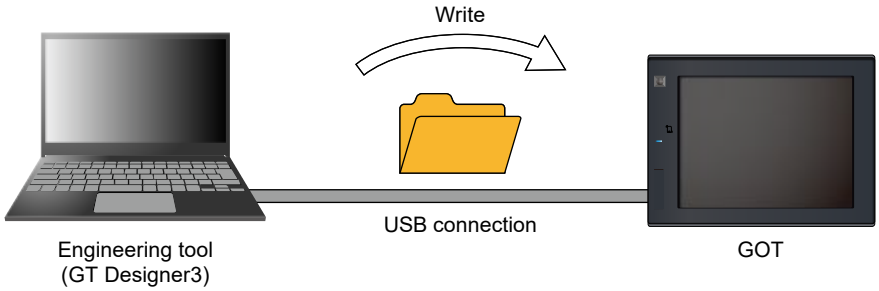


Figure 11 Image of updating BootOS (USB connection)

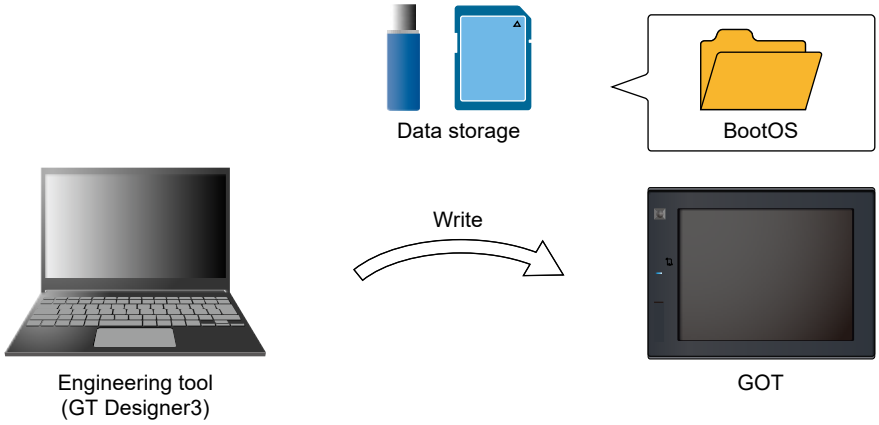


Figure 12 Image of updating BootOS (Using data storage)

2.4.4.3 Updating system applications

Update a system application through communication via USB or by the Ethernet connection from the engineering tool, or by using data storage such as USB memory or SD card.
After update is completed, check the GOT utility function "Package data management" to confirm that the system application has been updated.

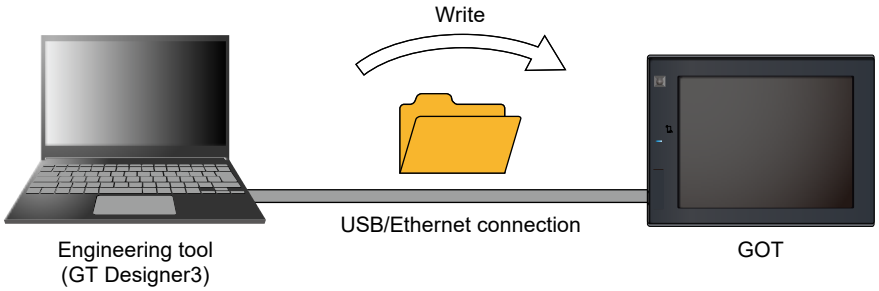


Figure 13 Image of updating system applications (USB or Ethernet connection)

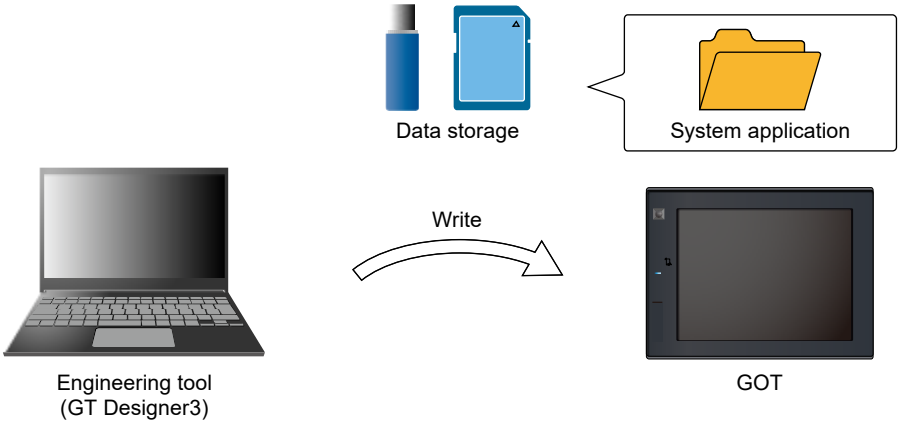


Figure 14 Image of updating system applications (Using data storage)

2.4.4.4 Precautions

The following describes precautions for using this function.

- Obtain the firmware update file by downloading it from the MITSUBISHI ELECTRIC FA Global Website. Do not use files obtained from other sites. (Firmware update files are included in the update file of the engineering tool "GT Designer3".)
- For CoreOS and BootOS, check the CRC value of the OS in [GOT information] of the utility function, and check that it matches the value published on the MITSUBISHI ELECTRIC FA Global Website.
  URL: https://www.mitsubishielectric.com/fa/products/hmi/got/dldb/gt_works3/crc.html
- Check whether firmware update is available periodically, and update the firmware as needed.

2.4.5 Operation setting function

If an error occurs in the GOT3000 series, the operation setting function allows the GOT3000 series to perform specific actions and notify the user of the error with a buzzer.
The operation setting function prevents necessary functions from being stopped by unintended operations of the GOT3000 series.

- The GOT3000 series stops communication with external devices if it operates abnormally due to an error.

2.4.6 Port forced close function

There are two types of port forced close functions as follows.

- Default open port usage setting function
- USB host/device disable function (disables the front USB interface of the GOT)

2.4.6.1 Default open port usage setting function

The default open port usage setting function is used to set whether to use the port numbers that are open by default in the GOT3000 series by opening or closing the port numbers individually.
The default open port usage setting function prevents situations where services that may be subject to attacks due to poor maintenance will become executable.

2.4.6.2 USB host/device disable function (disables the front USB interface of the GOT)

The USB host/device disable function disables communication with external devices via the front USB port on the GOT3000 series and the recognition of devices by disabling the host/device function of the front USB port. The USB host/device disable function is used to restrict the use of the USB port.

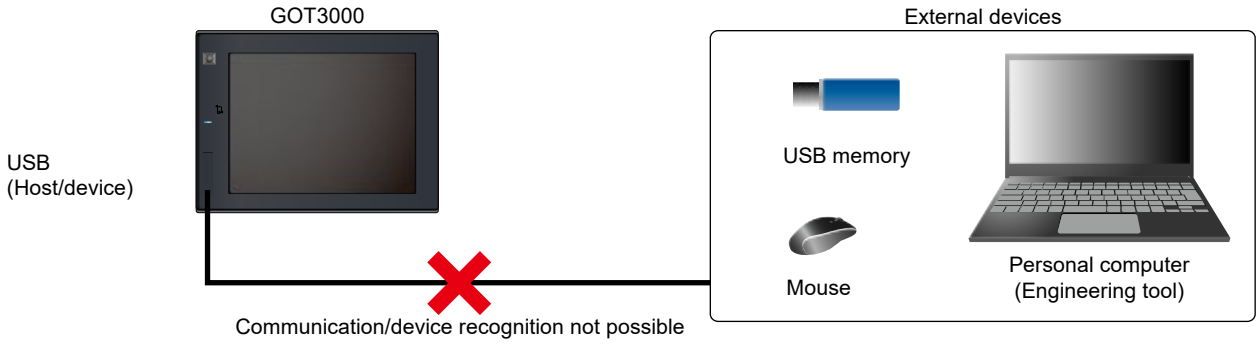


Figure 15 Image of the USB host/device disable function (disables the front USB interface of the GOT)

The USB host/device disable function (disables the front USB interface of the GOT) can be set with the engineering tool or utility of the GOT3000 series.

2.4.6.3 Precautions

Default open port usage setting function

- This function is a method for preventing unauthorized access from external devices. It is not possible to completely prevent unauthorized access only by using this function.
  In addition to this function, use other countermeasures, for example, installing firewalls, configuring a VPN, and installing anti-virus software, to maintain the security of the GOT3000 series against unauthorized access from external devices, DoS attacks, computer viruses, and other cyber-attacks.
- This function can perform the open and close operations of ports that are open by default. Port numbers opened by the customer to use the GOT3000 series functions are not subject to the operation of this function. For a function that requires a port number to be set to open, if the customer does not use it, set the function to not available.

USB host/device disable function (disables the front USB interface of the GOT)

- This function is enabled only for the USB port on the front. Enabling this function does not affect the rear port of the GOT3000 series.
- When the USB host/device is disabled, communication using the USB port on the front becomes unavailable. To enable the USB host/device again, change the settings without using the USB port on the front. (For example, changing the settings with the utility, Ethernet connection, and writing project data by using data storage connected to the USB port on the rear or SD card.)

2.4.7 Input data verification function from external devices

The GOT3000 series verifies whether data input from the outside of the trust boundary is in accordance with the specifications.
The input data verification function from external devices prevents unauthorized data that affects necessary functions from being input due to operational mistakes or other errors.

2.4.8 Security verification function

To use the product in compliance with IEC62443-4-2, the customer is required to periodically check that the security functions of the GOT3000 series operate according to the intended settings.
The security verification function prevents unintended operations from being performed which are caused by unauthorized persons accessing or operating the GOT3000 series due to incorrect settings or others.

For items to be checked, refer to "2.6.2 Periodic maintenance" in this document.

2.4.9 GOT all information initialization function

The GOT all information initialization function deletes all the data in the GOT3000 series. This function is used to discard the GOT3000 series with security ensured.
This function can be executed from the utility of the GOT3000 series.

2.4.9.1 Precautions

- Even when this function is executed, the function cannot initialize data in the SD card mounted to the GOT3000 series and various data storage connected to the USB host.
- Once deleted, the data can no longer be restored.
- Execute this function when disposing of the GOT3000 series.
- Do not turn off the power while all information initialization is in progress.

2.4.10 Information protection function

There are two types of information protection functions as follows.

- File tampering check function
- Confidentiality protection function

2.4.10.1 File tampering check function

The file tampering check function checks that files affecting the control of the GOT3000 series have not been tampered.
The file tampering check function detects unauthorized data changes.

The function targets files that affect the control of the GOT3000 series, and checks that the files have not been tampered.

2.4.10.2 Confidentiality protection function

The confidentiality protection function protects the confidentiality of security information of the GOT3000 series using encryption and operator authentication to control access.
The confidentiality protection function prevents data stored in the GOT3000 series from being disclosed due to operational mistakes or other errors.

Protect the confidentiality of information assets in the GOT3000 series by the following methods.

① Encryption of information assets
② Access control by operator authentication

2.4.10.3 Precautions

- If the password for a file is changed, the new password does not apply to files encrypted with the previous password. As a results, those files can no longer be read.

2.4.11 Encrypted communication function

Encrypted communication is a function that encrypts communication data when the GOT3000 series communicates with target devices across the trust boundary.

The encrypted communication function prevents communication data alteration due to accidental factors, reconnection to sessions that were intended to be disconnected, unintended data disclosure, and access to unintended devices.

To use the GOT3000 series in compliance with IEC62443-4-2, encrypt communication with target devices across the trust boundary.

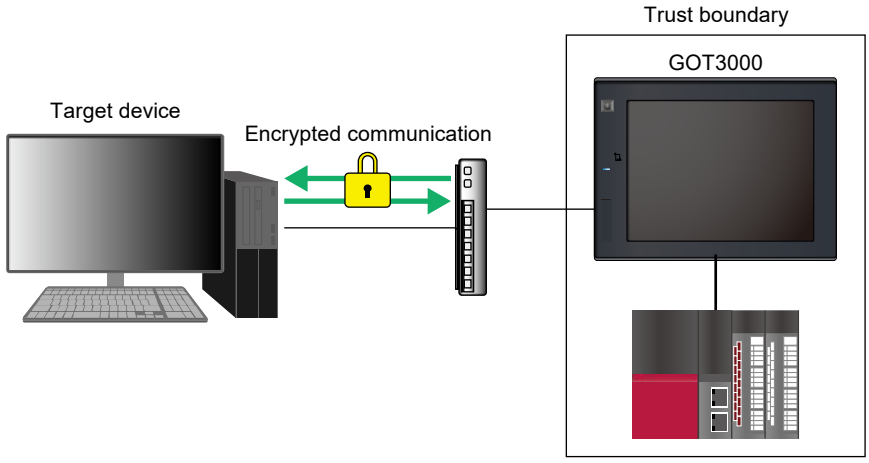


Figure 16 Overview of the encrypted communication function

2.4.11.1 Communication functions with encryption

- Communication with external devices that are directly connected to the GOT3000 series is subject to encrypted communication.
  Encrypted communication via a device, including seamless communication, is not applicable.
- Set whether to enable or disable encrypted communication in the engineering tool.
- Enabling/disabling of encrypted communication can be set for each driver or function.

The following shows the communication functions with encryption in the GOT3000 series.

Table 15 Functions using encrypted communication

No.	Function
1	MX controller (encrypted communication)
2	Communication with the engineering tool
3	VNC server function
4	Web browser function
5	GOT Mobile (Web server) function
6	OPC-UA server function
7	VPN connection function
8	FTP server function
9	File transfer (FTP client) function
10	E-mail send function
11	SoftGOT-GOT link function
12	OPC UA client function
13	Remote personal computer operation (Ethernet) function

*The VPN connection function securely connects the GOT3000 series from a remote terminal via the Internet. Since software VPN is built in the GOT, a secured remote system environment can be created at low cost without the need for a VPN router.

2.4.11.2 Electronic certificates used in encrypted communication

If electronic certificates (hereinafter referred to as "certificates") are not set correctly, encrypted communication with target devices cannot be performed.
Set the certificate setting information in GT Designer3, write it to the GOT3000 series, and create a certificate using the GOT utility function.

- Certificate setting information is required to create or update a certificate for the GOT.
- When there is certificate setting information in the GOT3000 series, the certificate can be created or updated from [Certificate management] of the GOT utility.

2.4.11.3 Precautions for electronic certificates

- For certificates, it is needed to set an expiration date. The expiration date is set to one year by default. To use the product in compliance with IEC 62443-4-2, do not change the expiration date which is one year by default.
- For the GOT3000 series, the internal time can be changed at any timing. Be careful when the time is changed because the expiration date of certificates is checked by referencing the internal time. After the time is changed, the status of a certificate may change from valid to invalid or from invalid to valid when the expiration date is checked.
- When enabling the encrypted communication function, set the local time as well. Otherwise, UTC+0000 is applied for the time.
- A system alarm is issued 90 days before the electronic certificate expires. Update the expiration date of the certificate.
- To configure a system in compliance with IEC 62443-4-2, set the setting information for the initially installed server certificate.

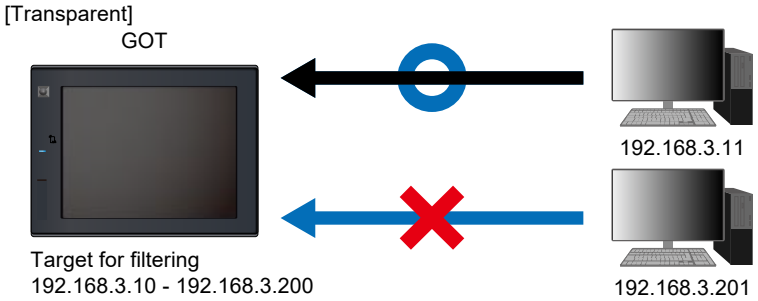
2.4.12 IP filter function

The IP filter function restricts the IP addresses of devices to be connected to the GOT3000 series by Ethernet, thereby preventing access through unauthorized IP addresses and allowing communication only with trusted devices.

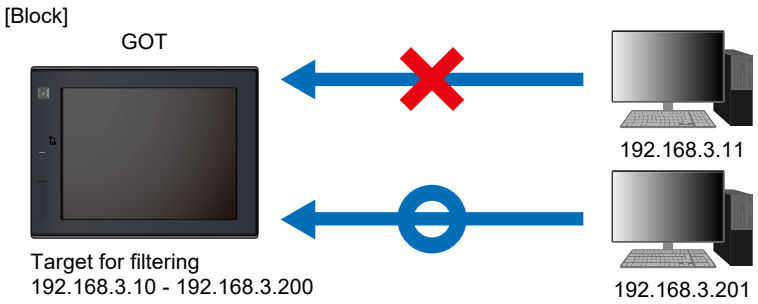
The IP filter function prevents communication traffic from increasing in the network due to operational mistakes or other errors, or necessary communication from being degraded or disabled.

The IP filter function applies to various interfaces accessed with IP addresses.

- Specify whether to use or not the IP filter function for each GOT3000 series product. (Default setting: Not used)
- Specify whether to permit (transmit) or prohibit (block) Ethernet communication with external devices with IP addresses specified in the filter target list for each GOT3000 series product. (Default setting: Transparent)
- Only devices that are directly connected to the GOT3000 series are subject to blocking.



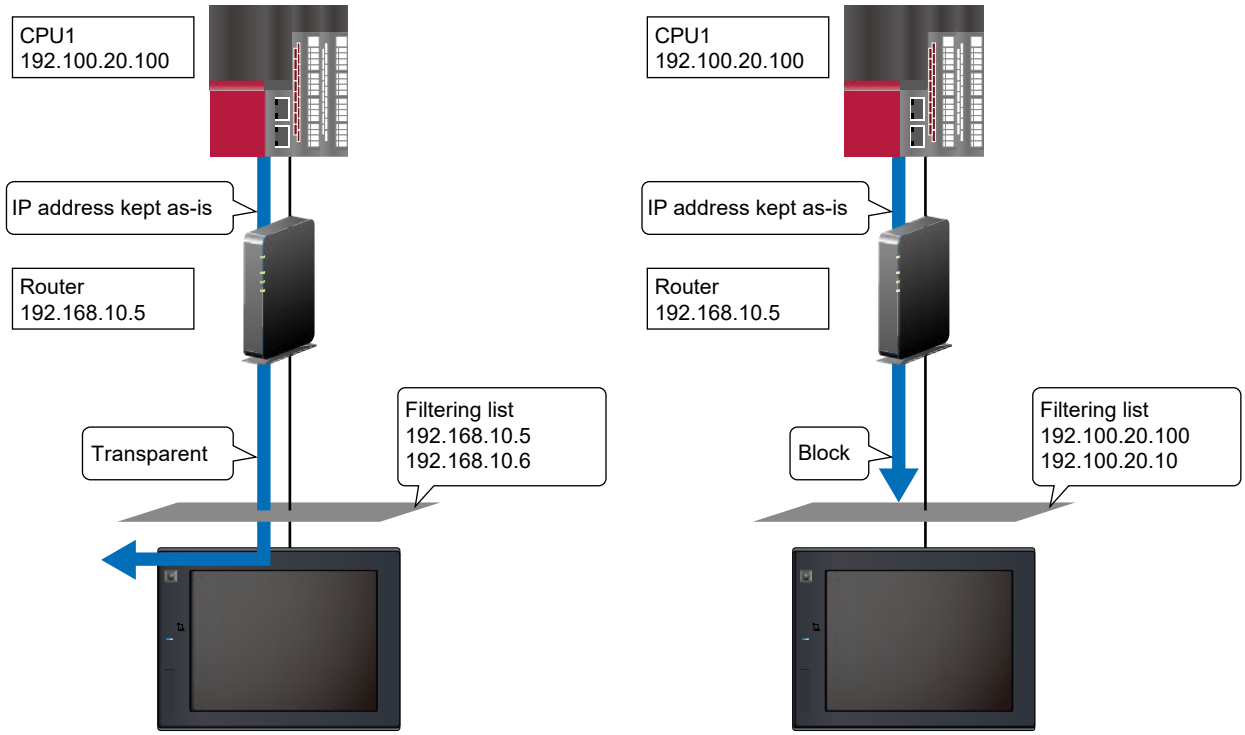
Only communication with devices whose IP addresses meet the filter condition is allowed.



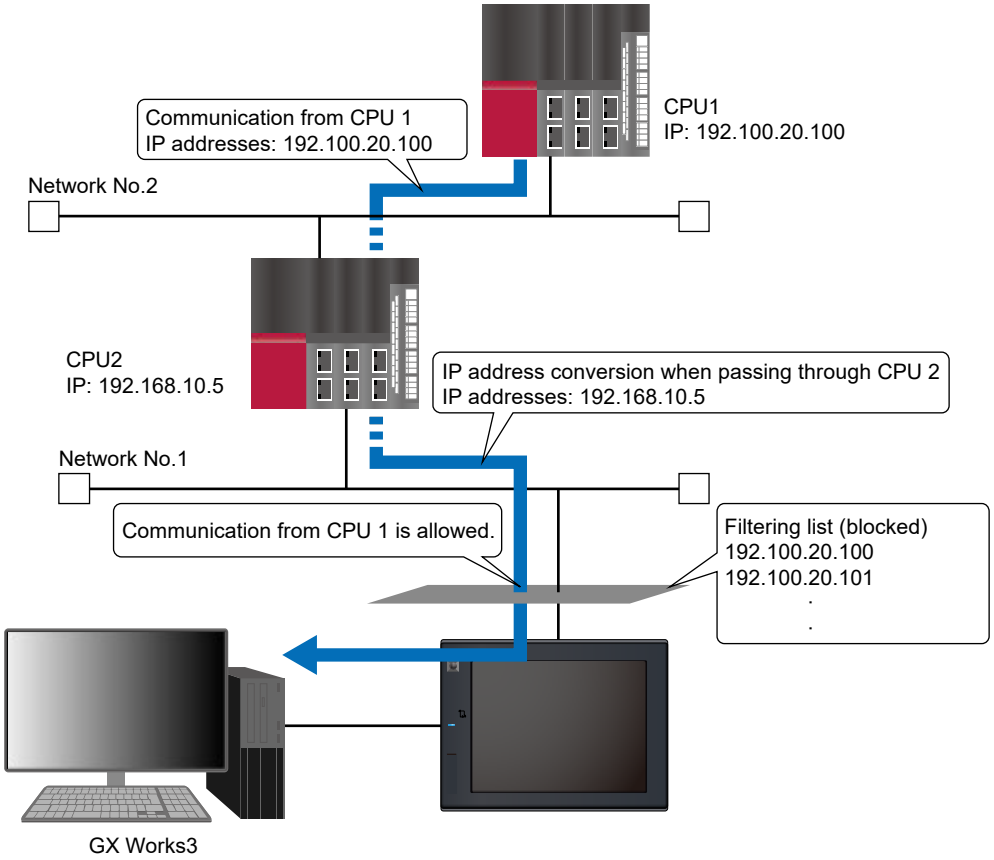
Communication from devices whose IP addresses meet the filter condition is blocked. (Any other communication is allowed.)

2.4.12.1 Precautions

- When using this product in an environment with Ethernet connection, it is recommended to use the IP filter function.
- To use the product in compliance with IEC 62443-4-2, use the IP filter function.
- This function is a method for preventing unauthorized access from external devices. It is not possible to completely prevent unauthorized access only by using this function. In addition to this function, use other countermeasures to ensure the security of the GOT3000 series against unauthorized access from external devices, DoS attacks, computer viruses, and other cyber-attacks.
  The following shows examples of countermeasures against unauthorized access.
  - ➢ Install firewalls and VPNs.
  - ➢ Install a personal computer as a relay station to control the relay of transmission and reception data with an application program.
  - ➢ Install an external device that can control access rights as a relay station. (For external devices that can control access rights, contact your network service provider or device dealers.)
- If a relaying device re-creates only Ethernet frames in the same way as a normal router, filtering is not applicable even if a target of blocking exists in between. If the IP address of the transmission source device is the target of blocking, it is blocked.



- If a relaying device re-creates and relays IP packets, filtering is applicable. In this case, communication is not blocked even if the IP address of the transmission source device is blocked.



- If the IP address range of a filter that overlaps with the range of another filter is set, the filter setting that was set earlier has priority. Therefore, the exception IP address list that was set later may be disabled.

2.4.12.2 At the occurrence of an error

If the IP filter settings become corrupted, they can be restored automatically.

2.4.13 Operation log function

The operation log function records the security functions and system operations of the GOT3000 series chronologically. The operation log function or system alarm observation function is used for recording.
By using the operation log function, recorded information can be checked chronologically, the causes of errors can be investigated, and unauthorized access and operations can be detected.
To use the function, select mode 2 for the security mode.

The following table shows the security functions subject to recording.

Table 16 Security functions and corresponding logging functions

Available: ○, Not available: -

No.	Security function	Operation log	System alarm observation
1	Security function setting function	○	-
2	Operator authentication function	○	-
3	Mobile code execution control function (disables JavaScript)	○	-
4	Firmware update function	○	-
5	Operation setting function	-	○
6	Port forced close function	○	-
7	GOT all information initialization function	○	-
8	Encrypted communication function	○	○
9	IP filter function	○	-
10	DoS attack restriction function	○	-
11	GOT data package acquisition function	○	-
12	Restore function	○	-

2.4.13.1 Saving operation logs and checking recorded logs

- Only the users who are given the operation authority by operator authentication can check the recorded operation logs.
- The details of the operation logs can be checked in [Operation log information] in the GOT utility main menu.
- The operation log file can be saved to the SD card or USB memory.
- If the capacity of storage media is insufficient, the older logs will be overwritten with new logs. You can also configure the setting to stop logging and prevent overwriting of old logs.
- If the total log file size is exceeded, the oldest file is automatically deleted. Therefore, before setting the total log file size, check the file size of the operation log file used in actual operation to ensure that it can be saved for the intended period of time. The total log file size can be checked in [Operation log information] of the GOT3000 series utility.
- If the GOT cannot be started for any reason, restore it using either of the following methods. Restoring the GOT allows you to check the logs in the operation log information in the utility.
  - Transferring the backup data to the GOT using the restore function
  - Write the project data using the same encryption password as the one set for the operation log file from the engineering tool

2.4.14 DoS attack restriction function

The DoS attack restriction function restricts the Ethernet communication function used by the GOT3000 series. The DoS attack restriction function prevents necessary functions from being affected by increased network traffic and CPU loads due to operational mistakes or other errors.

2.4.14.1 Precautions

- This function is a method for preventing unauthorized access from external devices. It is not possible to completely prevent unauthorized access only by using this function. In addition to this function, use other countermeasures to ensure the security of the GOT3000 series against unauthorized access from external devices, DoS attacks, computer viruses, and other cyber-attacks.
  The following shows examples of countermeasures against unauthorized access.
  - Install firewalls and VPNs.
  - Install a personal computer as a relay station to control the relay of transmission and reception data with an application program.
  - Install an external device that can control access rights as a relay station. (For external devices that can control access rights, contact your network service provider or device dealers.)
- To use the product in compliance with IEC 62443-4-2, use this function in combination with the IP filter and the default open port usage setting.

2.4.15 GOT data package acquisition function

The GOT data package acquisition function backs up data in the GOT to data storage such as SD card and USB memory.

Backup data can be restored by using the restore function.

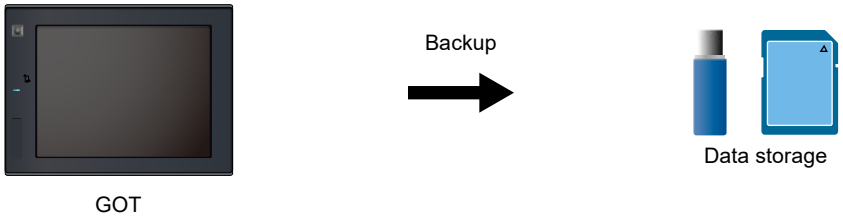


Figure 17 Image of the GOT data package acquisition function

Execute this function by using the utility of the GOT.

2.4.15.1 Precautions

- CoreOS and BootOS cannot be backed up with this function. Before executing the restore function, update the CoreOS and BootOS versions if necessary with the firmware update function.

2.4.16 Restore function

The restore function restores the data that was backed up by the GOT data package acquisition function by transferring the data to the GOT.

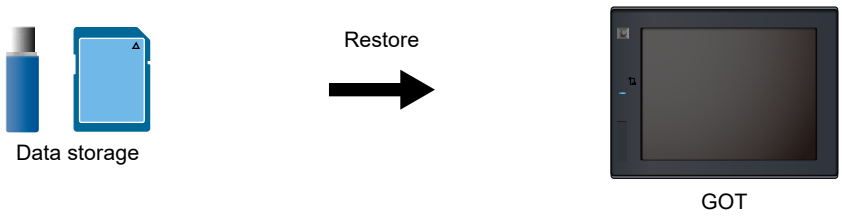


Figure 18 Image of the restore function

The restore function is executed using the package data management of the GOT utility or the system installation mode.

2.4.16.1 Precautions

- If backup data is acquired periodically using the GOT data package acquisition function, perform restoration using the latest backup data.
- After executing the restoration function, check that no error occurs.

2.5 Other security functions

The GOT3000 series also includes security functions other than those compliant with IEC 62443-4-2 as shown below.
Use each security function if needed.

- Screen security function (2.5.1)
- Functional operation security (2.5.2)
- Data transfer security (2.5.3)
- Ethernet security control (2.5.4)
- System screen operation restriction function (2.5.5)
- SD card access control signal (2.5.6)

For the operating procedures of the functions, refer to the following manuals.

- GOT3000 Series User's Manual (Utility Function, Maintenance and Inspection)
- GT Designer3 (GOT3000) User's Manual (Screen Design)

2.5.1 Screen security function

Setting the "security level" can restrict the operation and display of the screens, objects, utilities, and system applications of the GOT to only operators who have authorities with the specified security level or higher.

Security level password authentication

The authentication is performed with the password that has been set for each security level.

The operation and display of the GOT screen and objects can be controlled according to the security level.

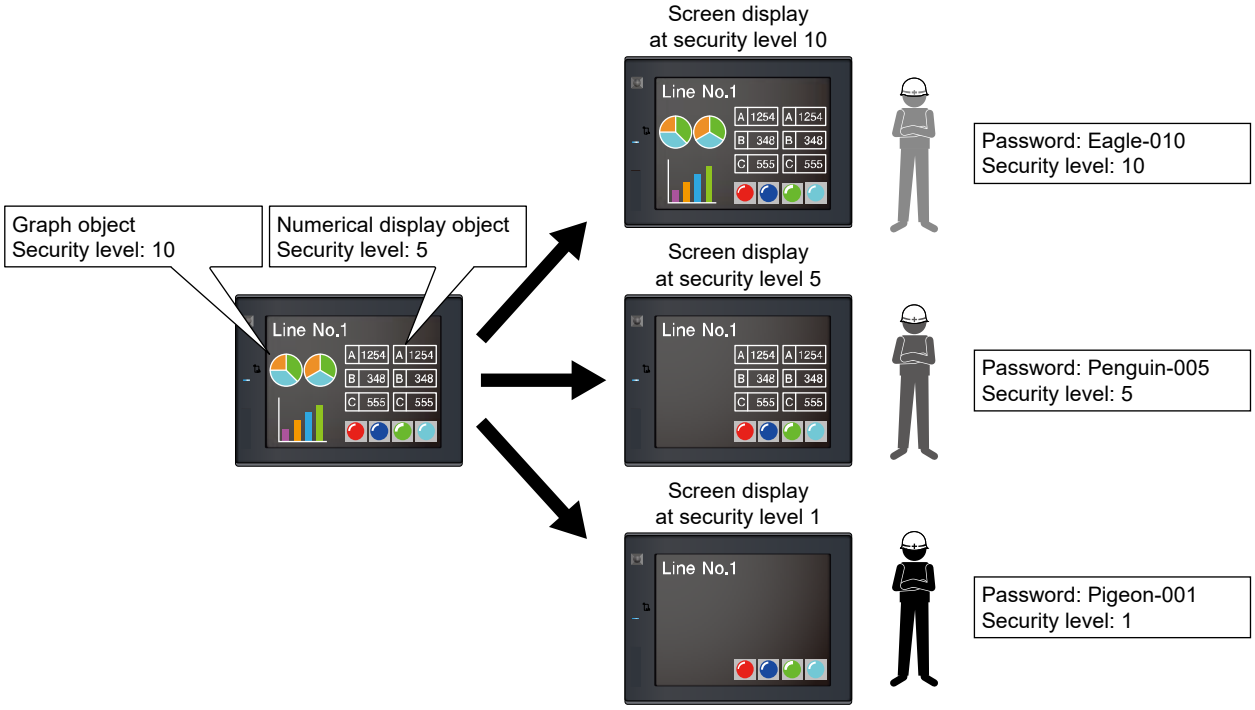


Figure 19 Image of security level password authentication

In security mode 2, security level password authentication is disabled. In that case, perform authentication by operator authentication.

2.5.2 Functional operation security

This function restricts the startup and operation of the GOT3000 series utility and various monitor functions using authentication or a device.
Configure the settings in GT Designer3.

Authentication can be performed using password authentication or operator authentication.
When password authentication is selected, a password can be set for each target operation to restrict which operators can perform it.
When operator authentication is selected, a level can be set for each target operation to restrict which operators can perform it based on their level.

2.5.3 Data transfer security

Data transfer security refers to the security of data operations managed by the GOT.
Unauthorized reading or writing of the package data and project data can be restricted with a password.
When data transfer security is set for project data,
password authentication is required for reading the project data or resource data or for overwriting the project data.
The GOT can be operated even without data transfer security.

In security mode 2, data transfer security is disabled. The restrictions enforced by data transfer security will be managed through the access privileges of operator authentication.

2.5.3.1 Precautions

- Registered passwords cannot be checked later. If the password is forgotten, the package data cannot be written to the GOT and project data and resource data cannot be read from the GOT.
- If the password is forgotten, reinstall BootOS or perform the GOT all information initialization function. If "Do not delete" is selected for GOT files, the data will not be deleted at the time of re-installation. Therefore, select "Delete" before re-installing. After the re-installation, all the data in the GOT including project and resource data is deleted.

2.5.4 Ethernet security control

The following operations can be disabled or enabled via the Ethernet port. In addition, a notification can be sent when a read, write, or installation request is received from the engineering tool via the Ethernet port while these operations are being disabled.

Via Ethernet port 1

- Writing a system package
- Writing or reading project data

Via Ethernet port 2

- Installing a system package
- Writing or reading project data

2.5.5 System screen operation restriction function

The operation of the following screens in the [Data] tab of the utility can be restricted.

- Alarm information, image file management, recipe information, logging information, operation log information, restriction of drive access operation, write operation to restricted GOT drives, and enabling/disabling of drive access on the memory card format screen
- Enabling/disabling of the display of the package management and GOT data package acquisition screens
- Enabling/disabling of the display of non-volatile RAM management screen

2.5.6 SD Card Access Control signal

The on/off state of the SD card access switch can be controlled. When the SD card access switch is on, the SD card inserted into the GOT3000 series can be accessed. When the switch is off, the card cannot be accessed.

2.6 Operation and maintenance of the GOT3000 series

2.6.1 Recommended operation examples of the GOT3000 series

As physical security measures for the GOT3000 series, it is recommended to implement area-based access restrictions in the factory and install the GOT3000 series in a secure and monitored location (e.g., inside of equipment or a locked cabinet) to protect it from unauthorized access and physical destruction. In particular, for a room storing devices for controlling networks and important devices for the continuous operation of the control system, it is recommended to separate the room from other areas and use lock management so that only specific persons can enter and exit from the room.

The GOT3000 series communicates with personal computers for maintenance and production management via networks. You can install the engineering software on the personal computers to manipulate the files stored in the GOT3000 series. To prevent these personal computers from being compromised and files stored in the GOT3000 series from being leaked, or files that cause unintended behavior from being written to the product, the following security measures are recommended for the personal computers connected to the GOT3000 series.

- Antitheft measures for personal computers with wire locks
- Access control for personal computer users
  - Only authorized persons shall be allowed to log in to the personal computers
  - Strict management of information for login
- Installing anti-virus software and other measures

To protect networks within the trust boundary where the GOT3000 series is installed and networks where personal computers are located from unnecessary external access, it is recommended to install network devices such as firewalls and routers between the Internet and networks in the factory or outside the trust boundary.

As part of continuous security operation in a factory where the GOT3000 series is installed, it is recommended to perform the check items for each function as shown in Table 17.

Table 17 Check items recommended for continuous security operations

No.	Function name	Check item
1	Backup	To be prepared for troubles such as product failure, back up the system package and project data to SD cards.
2	Acquired log check	Checking the logs acquired by the operation function is effective to detect suspicious behavior. For example, potential unauthorized access can be checked by reviewing the failed login attempt log. Note that if the capacity of storage media is insufficient, the older logs will be overwritten with new logs.
3	Certificate check	Check that the expiration date of the certificate used for the encrypted communication function. If the certificate expires, communication will not operate properly, so the certificate must be renewed.

When using the GOT3000 series, it is recommended to select an appropriate person as an administrator. In addition, it is recommended to provide sufficient education and training to GOT3000 series users to ensure proper setup, management, and operation of the product. Please use the GOT3000 series appropriately according to user's manuals and this guideline.

The files (customer assets) stored on the SD card may be leaked due to theft or other causes. In addition, if a malicious third party inserts an SD card containing an incorrect file, control of the customer's equipment may be affected. Therefore, it is recommended to avoid using an SD card in unprotected environments, such as control panels where the SD card slot may be subject to unauthorized access.

2.6.2 Periodic maintenance

To keep the system and GOT3000 series secure, perform periodic security maintenance (at least once a year is recommended). Specifically, it is recommended to check that the functions listed in Table 18 operate properly. Table 19 also shows the functions whose settings affect security. Use this information to also periodically check the accuracy of the settings.

Table 18 Operation verification items for security functions

No.	Function name	Check item
1	Operator authentication function	An operator can log on only when the correct combination of the operator name and password is entered.
		An operator is locked out when an incorrect combination of the operator name and password is entered several times.
		An operator can perform operations only within the operation authority range of the group to which the logged-on operator belongs.
2	Mobile code execution control function (disables JavaScript)	Mobile code subject to restriction is not executed.
3	Firmware update function	Updates the firmware version of the GOT3000 series.
4	Port forced close function	The port set as closed cannot be accessed.
5	Encrypted communication function	If a client device does not have the server certificate generated by the GOT3000, an error occurs during encrypted communication, and no communication is performed.
		Sets the internal time of the GOT correctly.
		Checks if the certificate has expired.
6	IP filter function	If Block is selected in the IP filter setting, communication from the set IP addresses is blocked and communication from the other IP addresses is not blocked.
		If Transparent is selected in the IP filter setting, communication from the set IP addresses is not blocked and communication from the other IP addresses is blocked.
7	Operation log function	The event is consistent with the contents of the operation log.
		The occurrence time of the event is consistent with the clock data in the operation log.
8	GOT data package acquisition function	When performing the GOT data package acquisition function with a memory card inserted, backup files are generated in the memory card.
9	Restore function	If the restore function is executed with an SD card containing password-protected backup data inserted, the state at the time of the backup will be restored.
		Acquires the backup periodically.

Table 19 Setting check item of the security function

No.	Function name	Check item
1	Operator authentication function	Check the users. Delete unnecessary operators if they remain.
		Check the privileges granted to the group. If an inappropriate privilege has been granted, delete the privilege.
2	Port forced close function	Check which ports are open. If an unused port is open, close it.
3	IP filter function	Check the IP addresses that are allowed to communicate with the product. If access from an unintended IP address is allowed, block access from that IP address.

2.7 Removal and discard of the GOT3000 series

This product stores data that will cause a problem if it is leaked to other companies when the product is discarded or transferred. To prevent such data from being leaked, make sure to remove and discard the product according to the following procedure when terminating the use of this product.

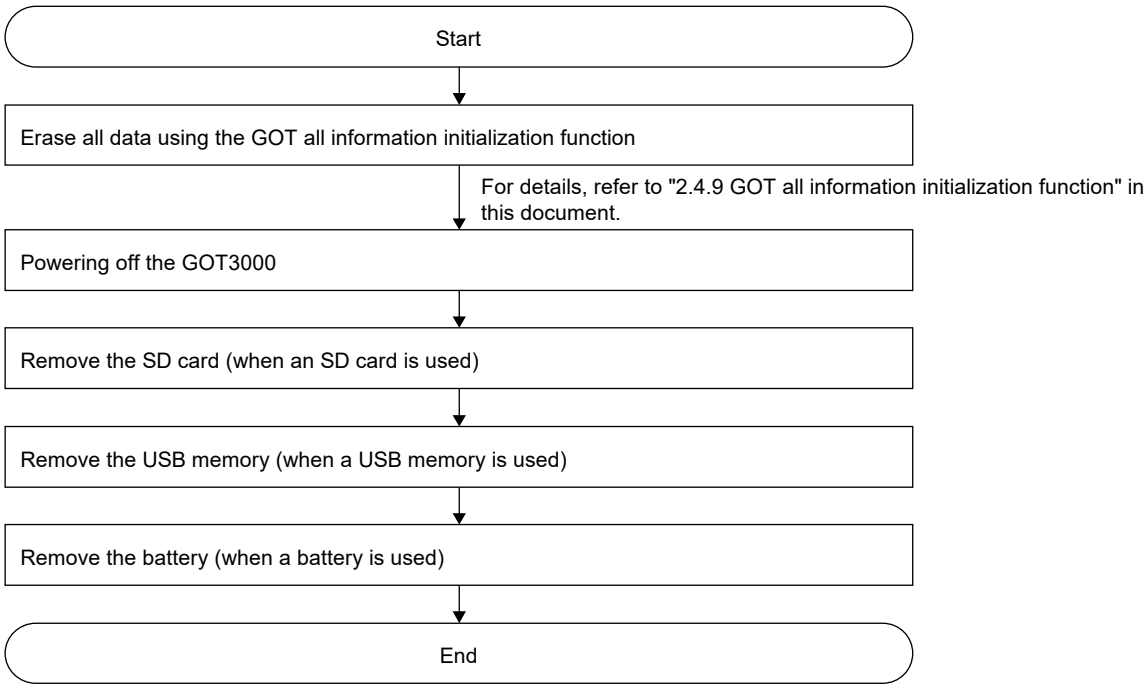


Figure 20 How to remove the product

Note that all information initialization does not delete the contents of the SD card or USB memory. When discarding or transferring the product, make sure to remove the SD card and USB memory and manage them properly. For general precautions concerning disposal, refer to SAFETY PRECAUTIONS in the GOT3000 Series User's Manual (Hardware).
If the GOT all information initialization function cannot be used due to failure or other reasons, it is recommended to dispose of the product in a way that prevents confidential information from being read, such as by crushing the product or destroying the magnetic parts.

To ensure the stability of overall factory control and the preservation of data stored in the system, stop the GOT3000 series after the system has been shut down.

Also, when removing a device connected to the GOT3000 series in the system, note that the device may contain protected assets. Take appropriate measures, such as deleting data, to prevent information from being retrieved before removal.

3. Contact for security-related issues

To improve the information security quality of products, our company collects information related to product vulnerabilities from external security researchers and coordination institutions (e.g., CERT[8] inside and outside Japan). For information on product vulnerabilities, contact coordination institutions or our company from the contact form of our website.

Contact regarding vulnerability of Mitsubishi Electric's products (contact form)
https://www.mitsubishielectric.com/psirt/contact/index.html

In addition, the details of reported vulnerabilities, mitigations, and solutions are disclosed in the following.
https://www.mitsubishielectric.com/psirt/vulnerability/index.html

[8] Computer Emergency Response Team

4. FAQ

[Q1]:

Under what policies does Mitsubishi Electric implement security measures for the GOT3000 series?

[A1]:

Our basic policies are "1. Compliance with laws and regulations", "2. Establishment of organizations and systems to ensure safety and security", "3. Promotion of defense-in-depth in FA systems", "4. Protection of the GOT3000 series throughout the product lifecycle", and "5. Reduction of security risks in the supply chain". For details, refer to Chapter 2 "Mitsubishi Electric's Approach to FA Security" in the FA SYSTEM SECURITY GUIDELINE".

[Q2]:

Does the Mitsubishi Electric GOT3000 series have any security standards?

[A2]:

We strive to provide products compliant with international security standards and regulations (such as IEC 62443) for control systems.

[Q3]:

What cybersecurity measures are implemented for the Mitsubishi Electric GOT3000 series?

[A3]:

As a company providing equipment and services to promote factory automation, we are implementing the following measures based on the concept of the international security standard (IEC 62443) for control systems.

- Building an organization and system for security
- Implementation of security functions and creation of security guidelines for products
- Protection of the GOT3000 series throughout the product lifecycle (planning, design, manufacturing, operation, and disposal)
- Security measures for the supply chain

For details on each item, refer to Chapter 2 "Mitsubishi Electric's Approach to FA Security" in the FA SYSTEM SECURITY GUIDELINE".

[Q4]:

What initiatives does Mitsubishi Electric implement for the GOT3000 series to protect customer systems and data from security threats?

[A4]:

As a general security policy for the GOT3000 series, we are promoting measures based on the four pillars described in [A3]. For the GOT3000 series, we implement the IP filter function, operator authentication, and other functions to reduce security risks for customers. Additionally, we consider security at each phase of the product lifecycle (planning, design, manufacturing, operation, and disposal) to protect the GOT3000 series against evolving attacks.

For information on the security functions of the GOT3000 series, refer to "2.2.4 Security functions of the GOT3000 series" and for the product lifecycle, refer to "2.2.5 Implementing secure product development lifecycle" in the FA SYSTEM SECURITY GUIDELINE.

[Q5]:

How should we consider security measures for the factory?

[A5]:

The items to be secured and the potential threats vary by factory, so the priority of security measures also varies. Refer to Chapter 3 "Construction and Operation of a Secure FA System" and Section 2.2.3 "Threat response policies" in the FA SYSTEM SECURITY GUIDELINE to consider security measures suitable for your factory.

[Q6]:

What should I do with the external storage media (such as an SD card) when disposing of the GOT3000 series?

[A6]:

To prevent logging information, recipe information, and other data from being extracted, it is recommended to initialize or perform similar procedures on unnecessary external storage media, delete the saved information, and then dispose of the media.

[Q7]:

What is Mitsubishi Electric's approach to procuring product parts, equipment used in design, development, and manufacturing, and software (including updates)?

[A7]:

To reduce risks associated with externally-procured hardware and software, we conduct on-site inspections with our suppliers and provide guidelines to raise security awareness, and reduce the intrusion of vulnerabilities through incoming inspections. We also instruct our business partners on countermeasures against leakage of design information and programs related to our products, including security-related information.