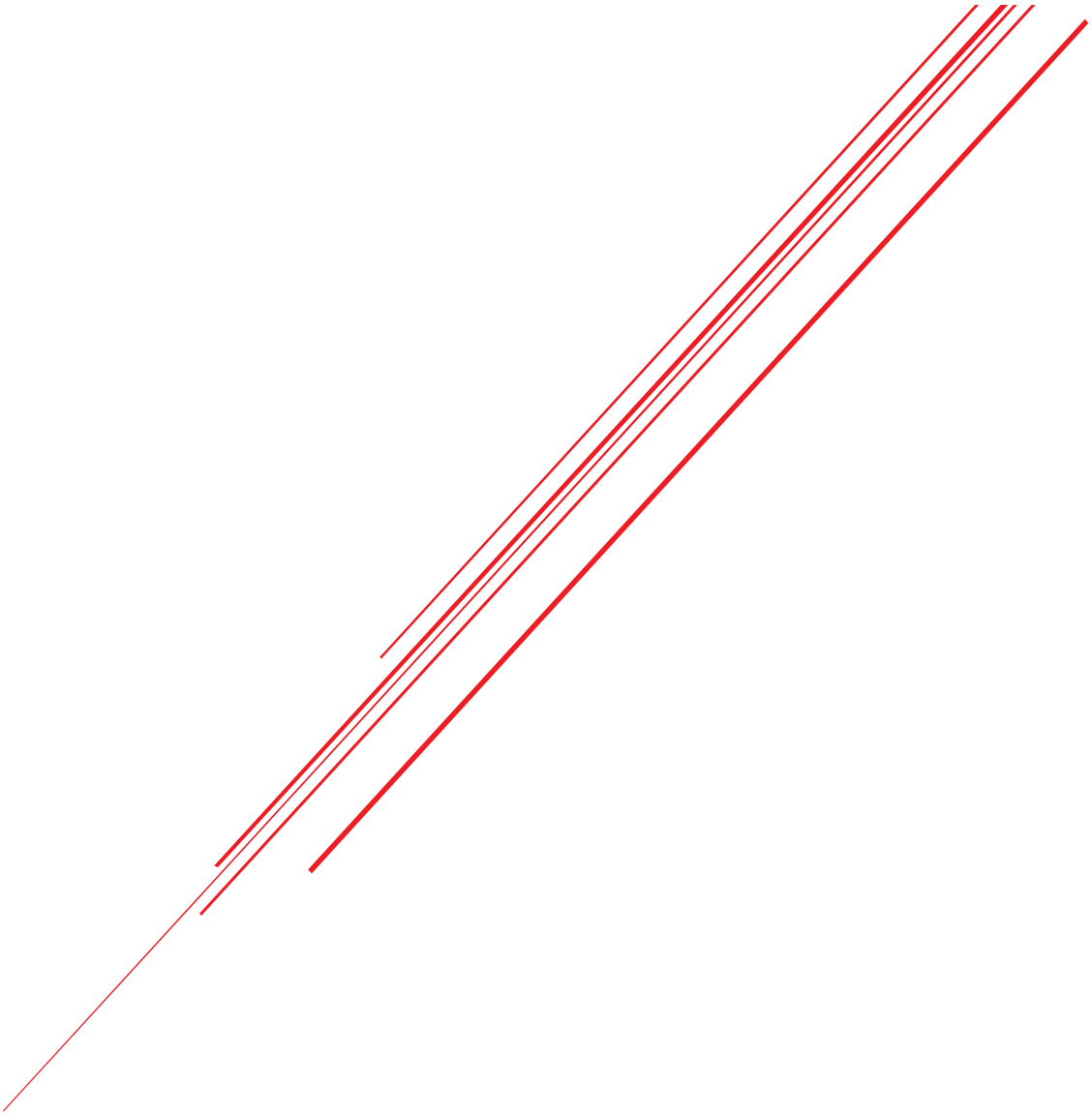
FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [GT SoftGOT3000] -



MITSUBISHI ELECTRIC CORPORATION

BCN- P5999-1861-A

Revision history

Date	Document number	Notes
Dec. 2025	BCN-P5999-1861-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 GT SoftGOT3000. They include GOTs, PLCs, personal computers, and applications that run on the personal computer.
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 the utility or add-on function).
Access	Reading, writing, editing, moving, and deleting data stored in GT SoftGOT3000.
Event	Specific operations and processing that occur in GT SoftGOT3000.
User	A generic term for the people who operate, access, and manage GT SoftGOT3000.
Event history	Logs of events that occurred in GT SoftGOT3000. The event history is recorded with the operation log and system log.
Protected assets	A generic term for package data, resource data, and security function setting information stored in GT SoftGOT3000.
Authentication	An operation in which GT SoftGOT3000 determines whether a login is successful based on the operator name and password entered by the user.
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.
Operation authority	The authority that allows each user to operate GT SoftGOT3000 screens and access GT SoftGOT3000.

[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
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 encrypted communication between GT SoftGOT3000 and external devices.
Certificate setting information	The setting information file required by GT SoftGOT3000 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 malware called WannaCry which targets IT systems gave significant damage by bringing factories to a halt. (Figure 1)

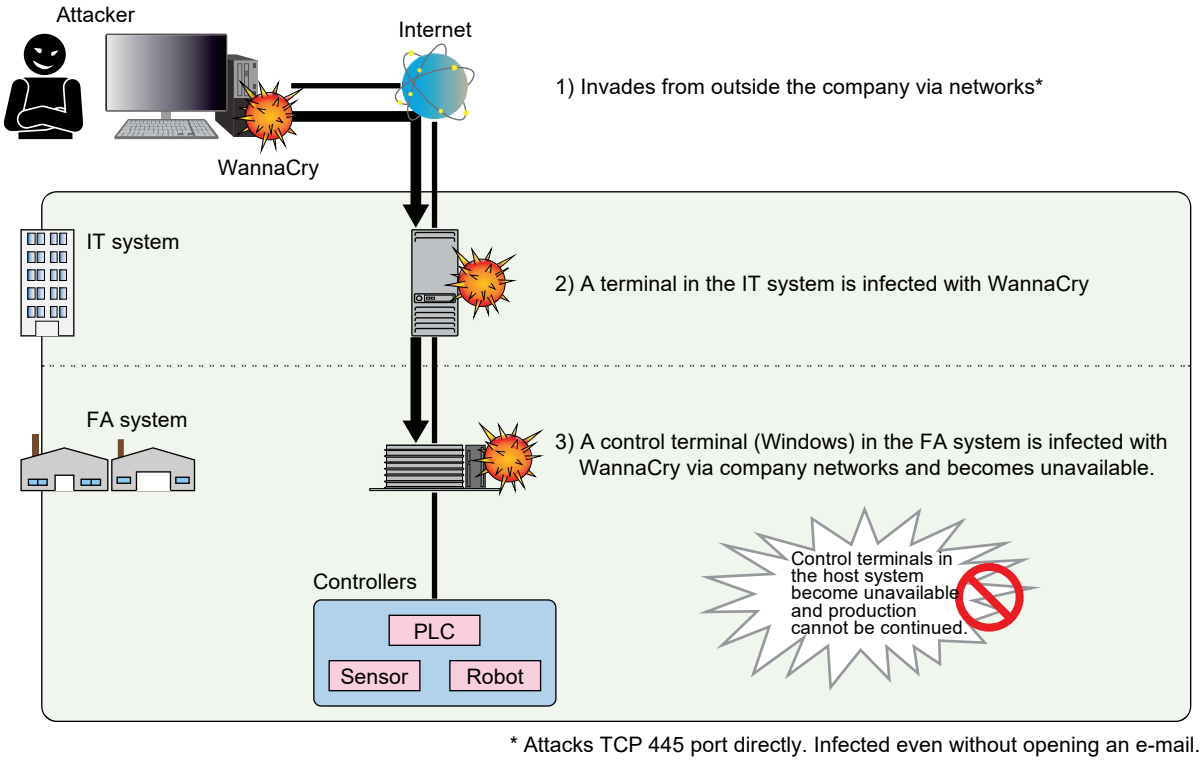


Figure 1 Example of infection routes and damage caused by WannaCry in the FA system

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 and SoftGOTs compliant with IEC 62443 to provide customers with safe and secure FA systems.

[6] For information on IEC 62443, refer to "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.

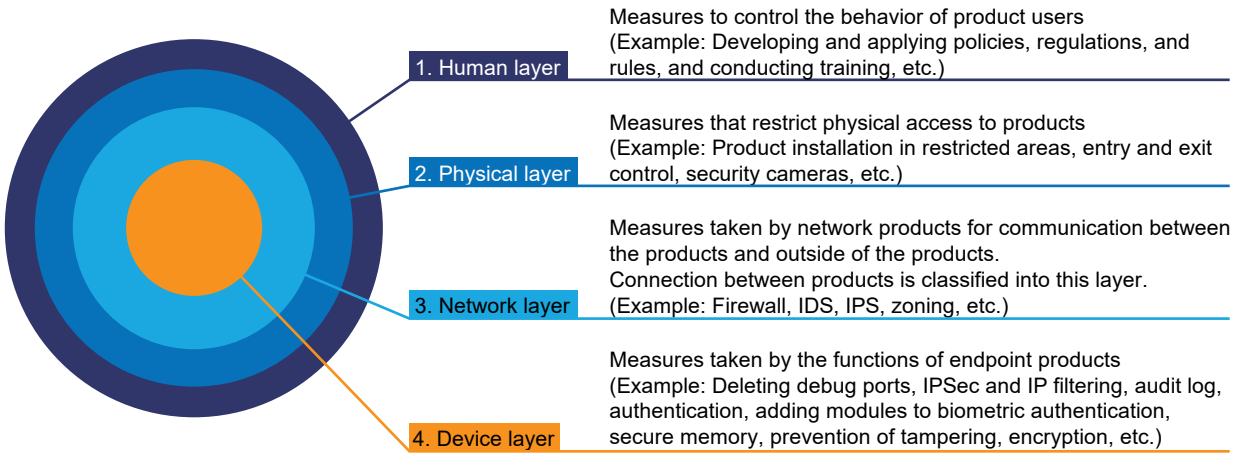


Figure 2 Concept of defense-in-depth

2. Security with GT SoftGOT3000 and Windows

2.1 Positioning of this chapter

The purpose of this guideline is to explain our company's way of thinking about the security of GT SoftGOT3000, and to provide the following information so that GT SoftGOT3000 will be used safely and securely in the customer's FA system.

- Security strategy in GT SoftGOT3000 (2.2):
  Identifies potential threats to GT SoftGOT3000, and explains the security response policies. The response policies include those performed by GT SoftGOT3000 itself and those performed in combination with other products.
- Method for installing GT SoftGOT3000 (2.3, 2.4):
  Explains the security functions of GT SoftGOT3000, how to set the functions, and how to install GT SoftGOT3000 in the FA system.
- Method for operating and maintaining GT SoftGOT3000 (2.6):
  Explains recommendations on managing users and passwords for GT SoftGOT3000 operation.
- Method for removing and disposing of GT SoftGOT3000 (2.7):
  Explains recommended methods (e.g., deletion function of data in the product) when removing and disposing of GT SoftGOT3000.

For the detailed specifications and operation methods of each function of GT SoftGOT3000, refer to the following manuals as needed.

- GT SoftGOT3000 User's Manual
- GT Designer3 (GOT3000) Screen Design Manual
- GOT3000 Series User's Manual (Utility & Maintenance Functions)

Read this guideline and the related manuals described above carefully to fully understand the security of GT SoftGOT3000, and use it to establish and maintain a safe and secure FA system.
For the basic security policies for our FA products, including GT SoftGOT3000, our efforts in product lifecycle, and examples of FA system configuration, refer to the following reference document.

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

2.2 Security response policies for GT SoftGOT3000

This chapter describes the following contents on the security strategy in GT SoftGOT3000.

- Assumed usage environments for GT SoftGOT3000 (installation environment, networks, operation and maintenance methods, user tasks, administrator tasks, etc.)
- Threats to GT SoftGOT3000
- Threat response policies
- Security functions in GT SoftGOT3000
- Security measures to be taken outside this product

2.2.1 Usage environments assumed for GT SoftGOT3000

Figure 3 shows an assumed environment in which GT SoftGOT3000 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.

GT SoftGOT3000 is assumed to be installed on a personal computer in the following environments.

- A control personal computer used as part of the process equipment installed in the production site in an access-controlled factory
- A production monitoring personal computer installed in an access-controlled office
- A personal computer in an access-controlled office in a remote area outside the factory

The inside of the personal computer in the above-mentioned environments is the trust boundary[7].

SD cards and USB memory devices are used for connection to GT SoftGOT3000. They are located outside the trust boundary because they are portable and can be used outside the equipment. GT SoftGOT3000 is not connected directly but connected via a firewall or router to communicate with networks outside the trust boundary.

[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.

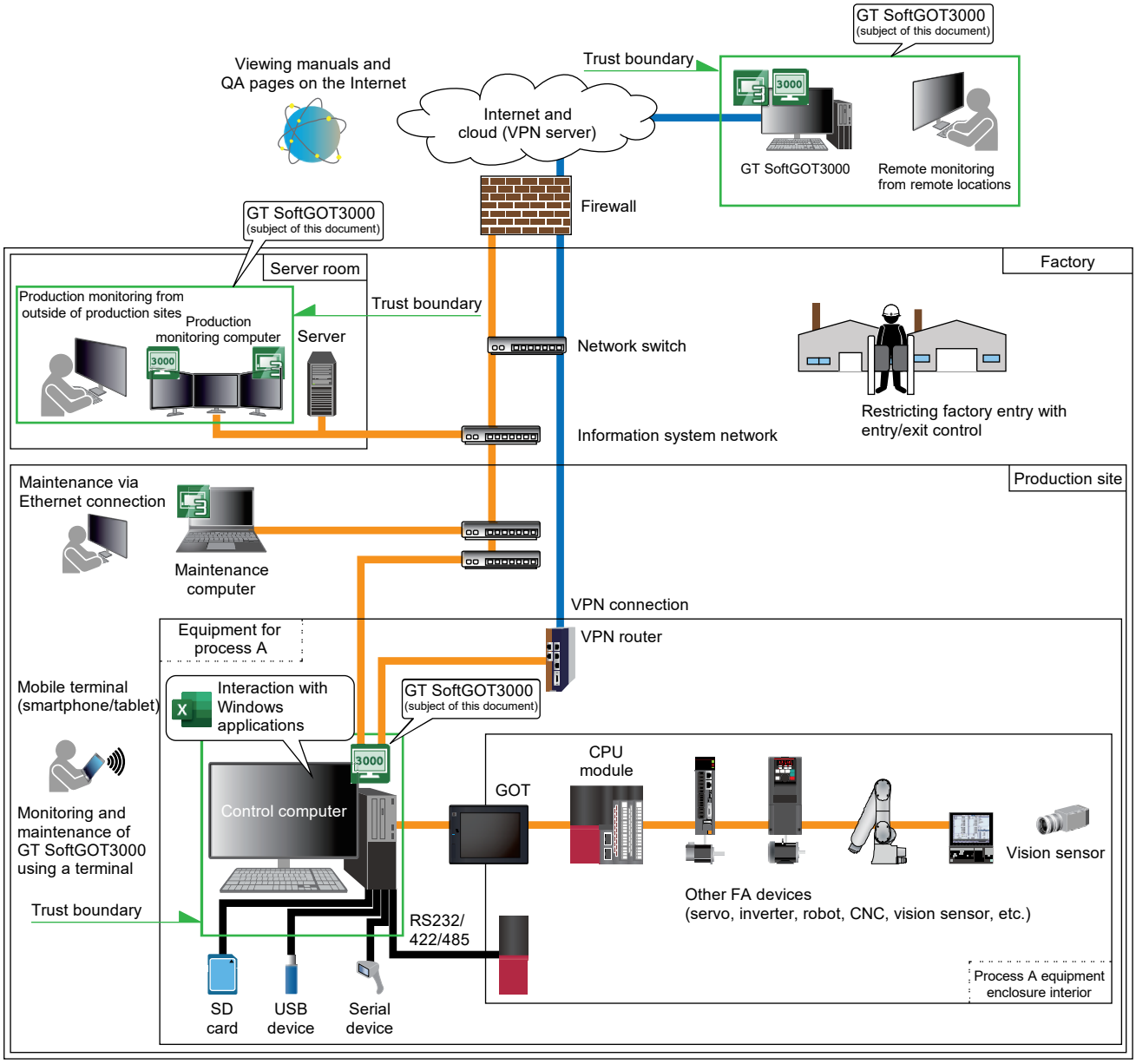


Figure 3 Assumed environment for GT SoftGOT3000 installation

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.
2	Network partitioning	The network to which GT SoftGOT3000 is connected is separated from external networks by devices such as firewalls and virtual private networks (VPNs).
3	Physical protection of the personal computer	Secure the personal computer with GT SoftGOT3000 installed with a wire lock or other means to prevent it from being taken out.
4	Anti-virus protection	By installing anti-virus software or others, the personal computer with GT SoftGOT3000 installed is protected against virus threats.
5	Windows settings compliant with the guidelines	Configure the Windows settings compliant with the guidelines to keep Windows secure. (Example: BitLocker, user management, version control)
6	Storage (SD, USB memory) management	Take appropriate security measures to manage the storage (SD, USB memory) properly.

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	Control personal computer	A device in which software for controlling the FA products in the control line system is installed, such as a CPU module. GT SoftGOT3000 is an example of our software for controlling FA products. Control personal computers include industrial personal computers and panel computers.
3	Production monitoring personal computer	A device in which software for monitoring the status of the control line system is installed. Our status monitoring software includes GENESIS64 (SCADA) and GT SoftGOT3000.
4	Remote monitoring personal computer	A device in which software for monitoring the status of the control line system from a remote office is installed. GT SoftGOT3000 and GENESIS64 are examples of our status monitoring software products. The production site can be accessed from a remote office via a VPN line.
5	Maintenance personal computer	A device in which the engineering tool necessary for maintenance of GT SoftGOT3000 is installed. An example of the engineering tool in our products is GT Works3.
6	Field Network	A network used for communication between the control personal computer and field devices.
7	Information system network	A network that is located inside the firewall and used for communication between the production monitoring personal computer and the control personal computer. Ethernet TCP/IP communication is an example of an information system network.
8	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.
9	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).
10	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.
11	External network (cloud)	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.
12	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.
13	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.

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 GT SoftGOT3000 is used.

Table 3 Area classification and operation methods

No.	Term	Description
1	Office	An area that stores important devices for the continuous operation of the control line system, including network control devices. By using a production monitoring personal computer, the production site is monitored via an information system network. Measures (e.g., locking so that only specific persons can enter and exit from the room) are taken to protect against unauthorized access and destructive actions.
2	Device in each process	Equipment that stores FA products and others. To protect the equipment against unauthorized access and destructive actions, measures are taken to ensure that only specific persons among those who are allowed to enter the production site can perform operations (e.g., locking control).
3	Production site	An area where only control line system users can enter.
4	Factory	An area where only factory users can enter.

A user refers to a control line system operator. Users work with GT SoftGOT3000 installed on the personal computer in the production site or in the office. They are authorized to set and execute some security functions and GT SoftGOT3000 related applications.
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 GT SoftGOT3000 from the administrator.
2	Receive training on security policies from the administrator, and understand procedures.

The administrator refers to the administrator of the control line system. The administrator operates and manages the personal computer with GT SoftGOT3000 installed and GT SoftGOT3000 related data and applications, and 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 GT SoftGOT3000

Our company considers that Figure 3 in 2.2.1 is the usage environment assumed for GT SoftGOT3000. Figure 4 shows threats to GT SoftGOT3000 and Table 6 describes such threats based on our knowledge from the risk assessment of the product and common knowledge of attack cases.

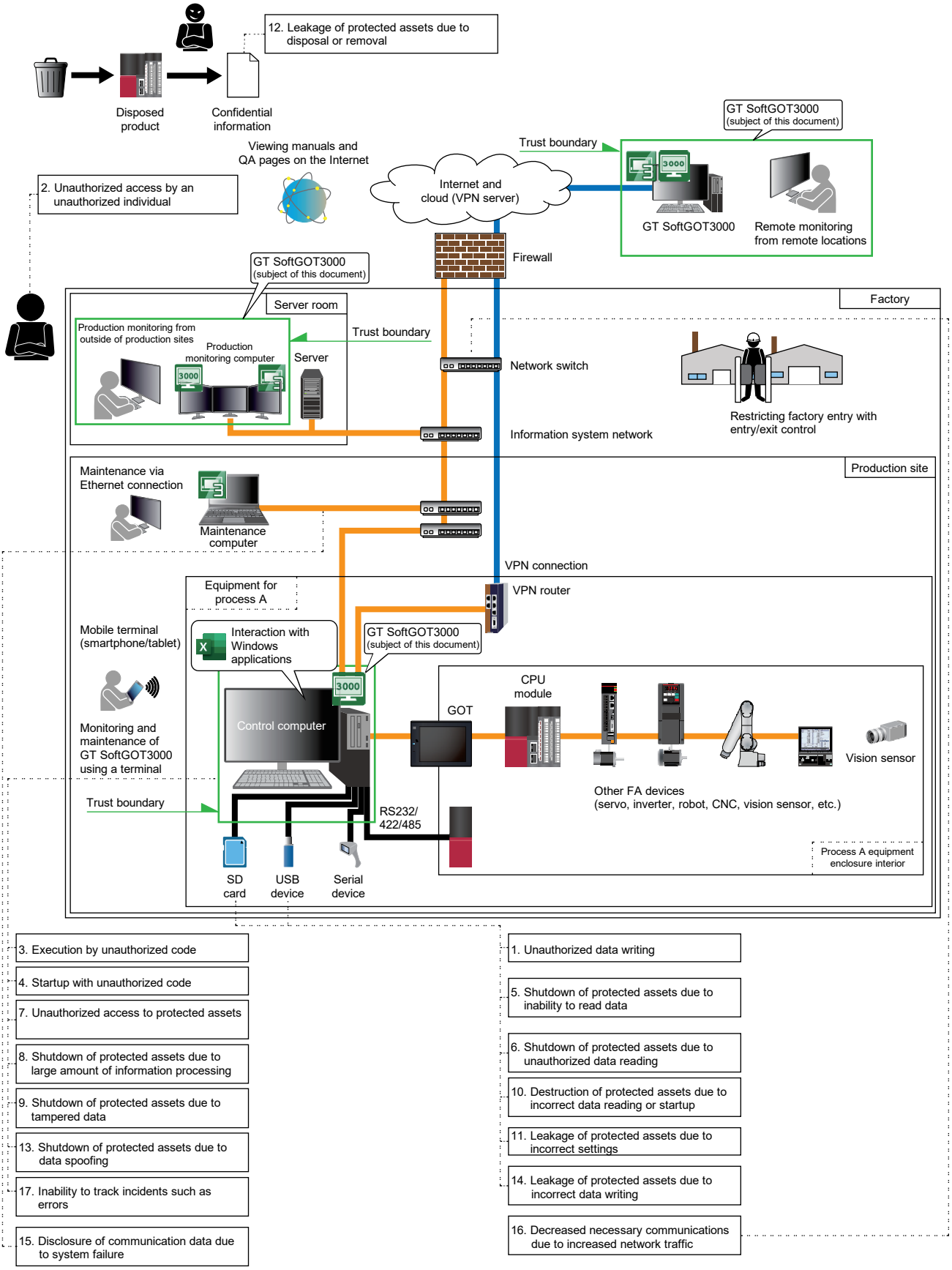


Figure 4 Threats to GT SoftGOT3000

Table 6 Explanation of threats

No.	Threat name	Description
1	Unauthorized data writing	Data may be written to an incorrect external application or controller due to operational mistakes, resulting in information leakage. If data is written to an incorrect application due to operational mistakes, the protected assets may malfunction.
2	Unauthorized access by unauthorized person	An incorrect authority may be granted to an unauthorized operator due to operation mistakes, allowing the operator to access the protected assets.
3	Execution by unauthorized code	Malicious data may be read due to operational mistakes, resulting in the destruction of the protected assets.
4	Startup with unauthorized code	Incorrect external application data may be started due to operational mistakes, resulting in the destruction of the protected assets.
5	Shutdown of the protected assets due to inability to read data	Data cannot be read from external devices due to inadequate maintenance, resulting in the shutdown of the protected assets.
6	Shutdown of the protected assets due to unauthorized data reading	• A large amount of incorrect information may be processed due to operational mistakes, resulting in interrupted or stopped services for the protected assets. • Incorrect application data may be read due to operational mistakes, resulting in the shutdown of the protected assets. • A large amount of incorrect data may be written to an application due to operational mistakes, resulting in interrupted services for the protected assets.
7	Unauthorized access to protected assets	• An incorrect protected asset may be accessed via the RS-232/422 communication function due to operational mistakes. • An incorrect protected asset may be accessed via key input due to operational mistakes.
8	Shutdown of the protected assets due to large amount of information processing	• A large amount of information from an external device may be processed due to operational mistakes, resulting in interrupted services for the protected assets. • A large amount of information from the data store may be processed due to operational mistakes, resulting in the shutdown of the protected assets.
9	Shutdown of the protected assets due to tampered data	• Accidental factors may cause key input data to be tampered with, resulting in the shutdown of the protected assets. • Accidental factors may cause communication data to be tampered with, resulting in the shutdown/malfunction of the protected assets. • Accidental factors may cause the read data to be tampered with, resulting in the shutdown of the protected assets.
10	Destruction of the protected assets due to reading or starting of incorrect data	• Data of an incorrect external application may be read due to operational mistakes, resulting in the destruction of the protected assets. • Data of an incorrect external application may be started due to operational mistakes, resulting in the destruction of the protected assets.
11	Leakage of the protected assets due to setting mistakes	Unauthorized person may be able to access the protected assets due to setting mistakes.
12	Leakage of the protected assets due to disposal/removal	The protected assets stored in the disposed/removed personal computer or external device may be leaked due to inadequate system maintenance.
13	Shutdown of the protected assets due to data spoofing	Accidental factors may data spoofing, resulting in the shutdown of the protected assets.
14	Leakage of the protected assets due to incorrect data writing	Data may be written to an incorrect application due to operational mistakes, resulting in information leakage.
15	Disclosure of communication data due to system failure	Communication data may be disclosed due to system failure.

No.	Threat name	Description
16	Decreased necessary communications due to increased network traffic	Network traffic may increase due to system failure, resulting in the decrease/shutdown of communications necessary for the protected assets.
17	Invalidity to track incidents such as errors	Unauthorized data transmission or errors may be unable to track due to operational mistakes.

2.2.3 Threat response policies

Figure 5 shows the threat response policies for GT SoftGOT3000. The response policies include not only those performed by GT SoftGOT3000, 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 GT SoftGOT3000. Therefore, security measures are necessary for the entire FA system, as well as for GT SoftGOT3000.

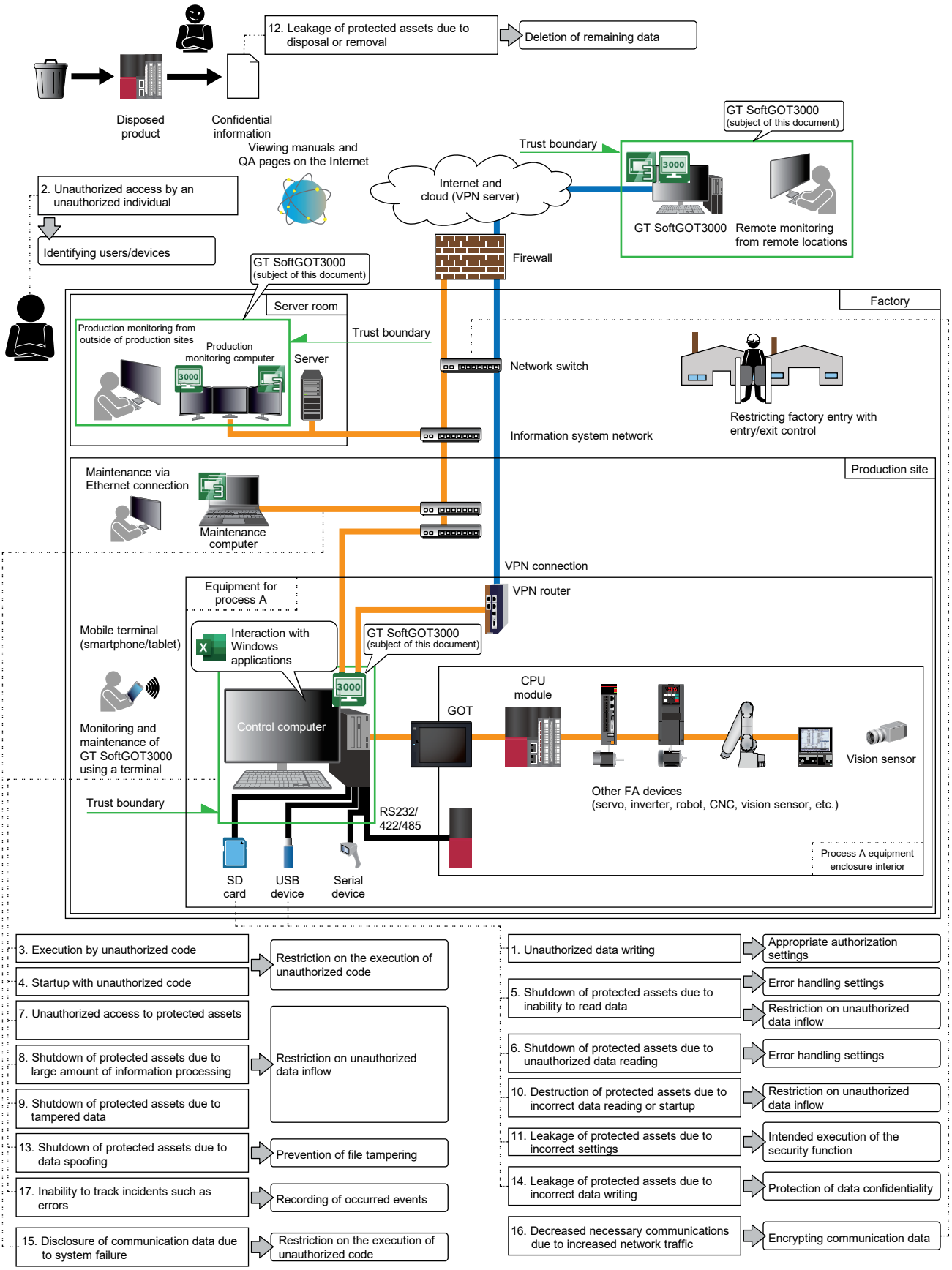


Figure 5 Threat response policies for GT SoftGOT3000

Table 7 Threat response policies for GT SoftGOT3000

No.	Threat name	Response policy	Related function/measures
1	Unauthorized data writing	● Setting appropriate authorities	● Operator authentication
2	Unauthorized access by unauthorized person	● Identifying users/devices	● Operator authentication
3	Execution by unauthorized code	● Restriction on the execution of unauthorized code	● Mobile code execution control function
4	Startup with unauthorized code	● Restriction on the execution of unauthorized code	● Mobile code execution control function
5	Shutdown of the protected assets due to inability to read data	● Settings for operation when an error occurs ● Restriction of unauthorized data inflow	● Operation setting function ● External device input data verification function
6	Shutdown of the protected assets due to unauthorized data reading	● Settings for operation when an error occurs	● Operation setting function
7	Unauthorized access to protected assets	● Restriction of unauthorized data inflow	● External device input data verification function
8	Shutdown of the protected assets due to large amount of information processing	● Restriction of unauthorized data inflow	● External device input data verification function
9	Shutdown of the protected assets due to tampered data	● Restriction of unauthorized data inflow	● External device input data verification function ● Information protection function
10	Destruction of the protected assets due to reading or starting of incorrect data	● Restriction of unauthorized data inflow	● External device input data verification function
11	Leakage of the protected assets due to setting mistakes	● Execution of the security function as intended	● Security verification function
12	Leakage of the protected assets due to disposal/removal	● Deletion of remaining data	● GT SoftGOT3000 all information initialization function
13	Shutdown of the protected assets due to data spoofing	● Prevention of file tampering	● Information protection function
14	Leakage of the protected assets due to incorrect data writing	● Protection of data confidentiality	● Information protection function
15	Disclosure of communication data due to system failure	● Encrypting communication data	● Encrypted communication function
16	Decreased necessary communications due to increased network traffic	● Restricting the IP addresses of controllers ● Restricting the bandwidth of networks used	● IP filter function ● Restriction function against DoS attacks
17	Invalidity to track incidents such as errors	● Recording of events that have occurred	● Operation log function

2.2.4 Security functions of GT SoftGOT3000 and functions of Windows or external environments

GT SoftGOT3000 includes the security functions as shown in Table 8 to implement the threat response policies described in 2.2.3.

The security functions of GT SoftGOT3000 include Windows functions (security measures for external software).

Table 8 Security functions of GT SoftGOT3000

Function name	Description	Threat to be handled
Security function setting function	Specifies the security-related operations of GT SoftGOT3000 for establishing a secure system.	-
Operator authentication function	Restricts users who can access GT SoftGOT3000. There is also a function that displays precautions for using GT SoftGOT3000 to the user before executing this function.	1. Unauthorized data writing 2. Unauthorized access by unauthorized person
External device input data verification function	Verifies the validity of the data when GT SoftGOT3000 receives data beyond the trust boundary.	5. Shutdown of the protected assets due to inability to read data 7. Unauthorized access to protected assets 8. Shutdown of the protected assets due to large amount of information processing 9. Shutdown of the protected assets due to tampered data 10. Destruction of the protected assets due to reading or starting of incorrect data
Security verification function	Allows the user to periodically check whether the security functions of GT SoftGOT3000 operate normally according to intended settings.	11. Leakage of the protected assets due to setting mistakes
GT SoftGOT3000 all information initialization function	Deletes folders and files that are not deleted by uninstallation and uninstalls the application using the uninstaller.	12. Destruction of the protected assets due to disposal/removal
Information protection function	The file tampering check function and the confidentiality protection function are available. The file tampering check function checks that the files affecting the control of GT SoftGOT3000 have not been tampered. The confidentiality protection function protects confidentiality of the information assets of GT SoftGOT3000.	9. Shutdown of the protected assets due to tampered data 13. Shutdown of the protected assets due to data spoofing 14. Leakage of the protected assets due to incorrect data writing
Encrypted communication function	Encrypts communication data between GT SoftGOT3000 and the target devices across the trust boundary.	15. Disclosure of communication data due to system failure

Function name	Description	Threat to be handled
Operation log function	Records logs with the alarm observation function or operation log function.	17. Invalidity to track incidents such as errors
Restore function (import function)	Copies the GT SoftGOT3000 data backed up by the GOT data package acquisition function (export function) to the installation folder or another folder and restores the data.	-
Error display function	If an error occurs, displays the error using the GT SoftGOT3000 or Windows function.	-

Table 9 Windows or external environment function

Function name	Description	Threat to be handled
Mobile code execution control function	Windows function. This function restricts the execution of mobile code that may be executed with the web browser function or application interaction function of GT SoftGOT3000.	3. Execution by unauthorized code 4. Startup with unauthorized code
Operation setting function	Windows function. When an error occurs in GT SoftGOT3000 and it can no longer maintain normal operation, this function notifies the user of the error status in a Windows dialog box.	5. Shutdown of the protected assets due to inability to read data 6. Shutdown of the protected assets due to unauthorized data reading
Error display function	If an error occurs, displays the error using the GT SoftGOT3000 or Windows function.	-
IP filter function	Windows or external environment function. This function restricts the IP addresses of devices connected to GT SoftGOT3000 when Ethernet connection is used, thereby preventing access by incorrect IP address specification and enabling communication only with trusted devices.	16. Decreased necessary communications due to increased network traffic
Operation log function	Records events that occur in GT SoftGOT3000 as a Windows application.	17. Invalidity to track incidents such as errors
Restriction function against DoS attacks	Windows or external environment function. This function prevents DoS attacks by limiting the network bandwidth used by GT SoftGOT3000 or by restricting Ethernet communications.	16. Decreased necessary communications due to increased network traffic
GOT data package acquisition function (export function)	Saves GT SoftGOT3000 data to a folder such as a local folder of a user with administrator privileges.	-
Wireless usage control function	Windows function. When wireless connection is used, this function encrypts communication data using the Windows function.	-

2.2.5 Security measures to be taken outside this product

Figure 6 and Table 10 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 GT SoftGOT3000 and the threat response policies (2.2.3).

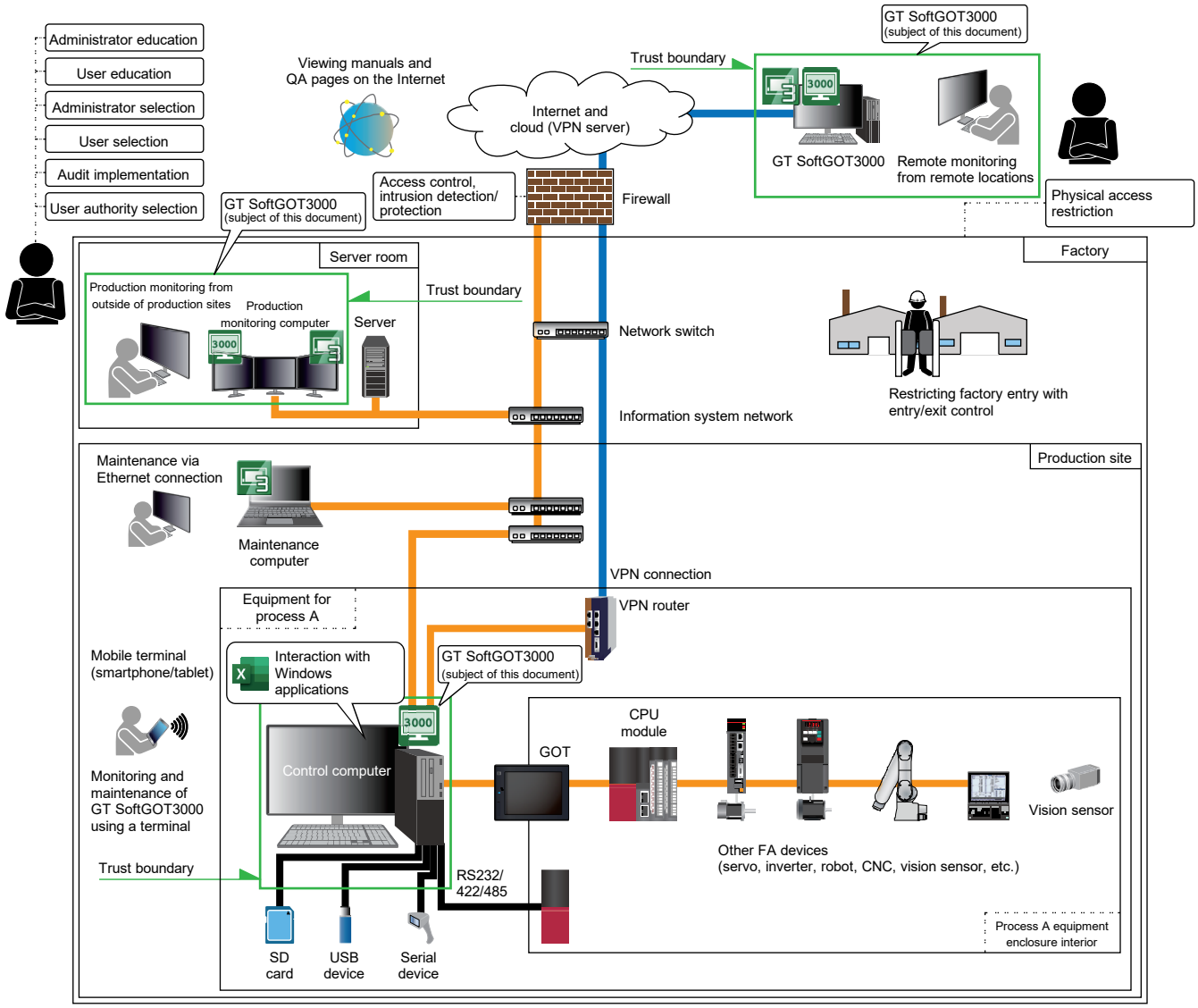


Figure 6 Security measures to be implemented in usage environment

Table 10 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 physical access by unauthorized persons by installing GT SoftGOT3000 in a safe and monitored location.	● Unauthorized access by unauthorized person
Human layer	User selection	GT SoftGOT3000 shall be able to be used only by users who have received permission from the administrator.	● Unauthorized access 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.	● Invalidity to track incidents such as errors
Network layer	Access control, intrusion detection/protection	Prevent attacks by outsiders from external networks by installing devices such as firewalls.	● Decreased necessary communications due to increased network traffic

2.3 Installation of GT SoftGOT3000

This chapter describes how to install GT SoftGOT3000 in a system and how to set and use the security functions of GT SoftGOT3000.

2.3.1 Procedures for installing and setting up GT SoftGOT3000

In a system using GT SoftGOT3000 (Figure 7), it is recommended to operate GT SoftGOT3000 according to the procedure shown in Figure 8 to ensure compliance with IEC 62443-4-2 (with security enhancement settings enabled).

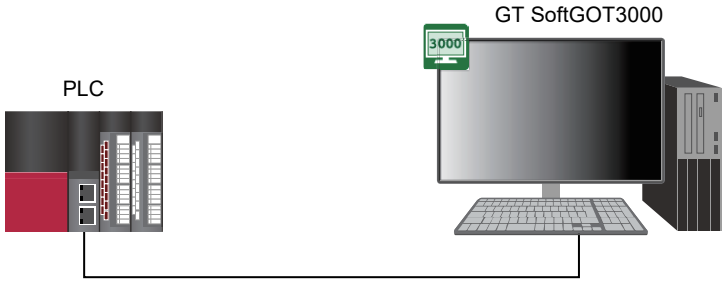


Figure 7 System configuration example

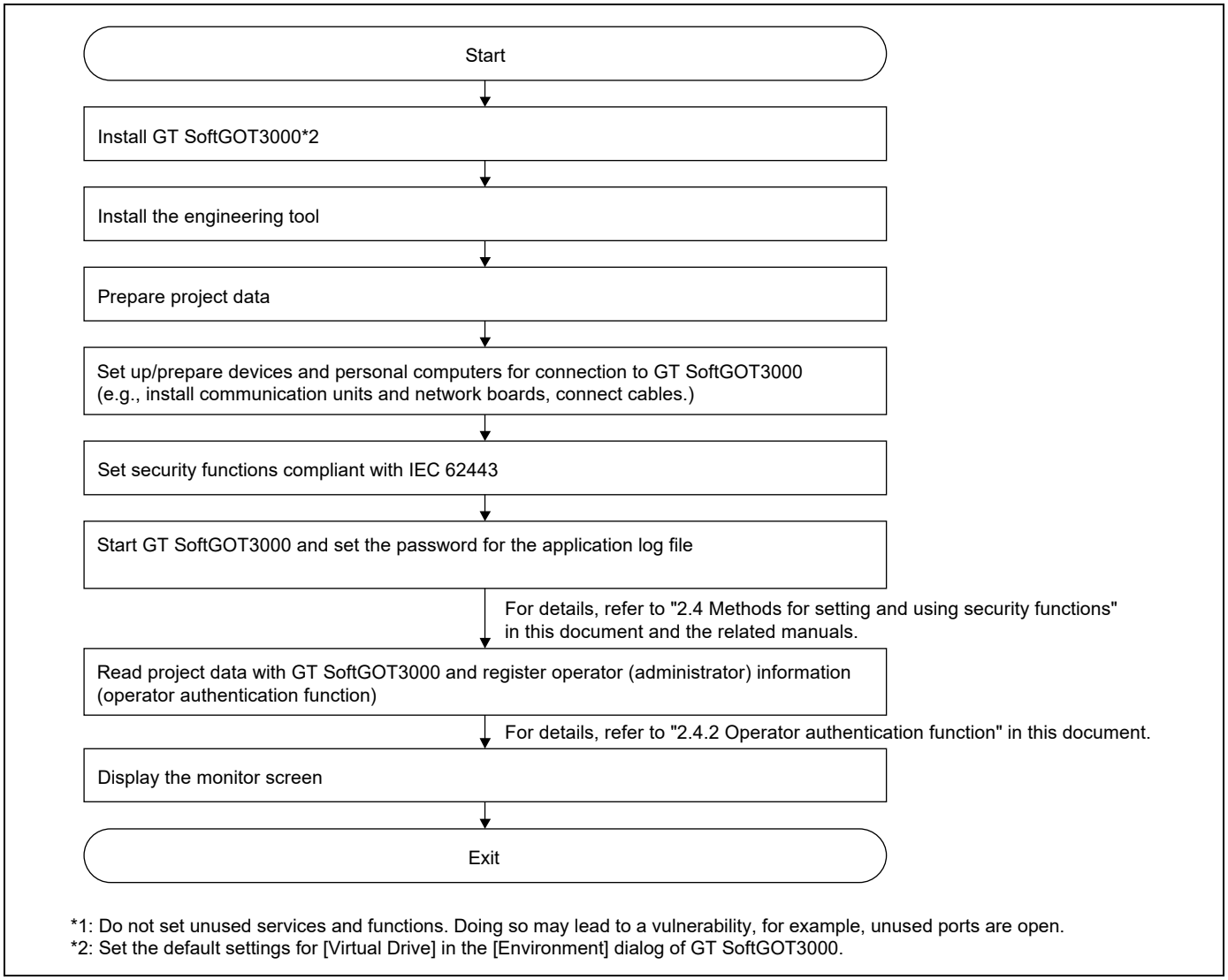


Figure 8 Procedure before operation

• Security function settings compliant with IEC 62443-4-2

Perform the following items (Table 11) as security function settings compliant with IEC 62443-4-2.

Table 11 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
3	Operator authentication function	Set the operation authorities for each group appropriately.	2.4.2
4		Set a password that is not easy to guess.	
5		Change the password periodically.	
6		Set an appropriate message to notify the user at logon.	
7		Perform operator authentication before accessing the protected assets.	
8	Mobile code execution control function	Control execution using the Windows function.	2.4.3
9	Operation setting function	Control execution using the Windows function.	2.4.4
10	Information protection function	Set a password that is not easy to guess.	2.4.8
11	Encrypted communication function	The encrypted communication function is not enabled by default. Enable the encrypted communication function.	2.4.9
12		Encrypt communication with target devices across the trust boundary.	
13		Perform encrypted communication via the built-in Ethernet port of GT SoftGOT3000.	
14		Set the term of validity of the certificate used for encrypted communication to one year (default setting).	
15	IP filter function	Enable this function.	2.4.10
16		Restrict access from the target device with the IP filter.	
17	Restriction function against DoS attacks IP filter function	As countermeasures against DoS attacks, use the IP filter function, DoS attack restriction function, and other additional countermeasures against unauthorized access.	2.4.12
18	Operation log function	Set the correct time so that time stamp will be correctly recorded.	2.4.11
19	Restore function (import function)	Use the encrypted GOT data package acquisition file for restoration.	2.4.14
20	Wireless usage control function	Control execution using the Windows function.	2.4.15
21	Error display function	Use the function of GT SoftGOT3000 or Windows to check.	2.4.16
22	GOT data package acquisition function (export function)	Encrypt the data when performing GOT data package acquisition.	2.4.13
23	GT SoftGOT3000 all information initialization function	When disposing of the computer, completely delete the files related to GT SoftGOT3000 and uninstall the application.	2.4.7

- To use GT SoftGOT3000 in compliance with IEC 62443-4-2, perform necessary security functions at each stage of installation, operation, maintenance, and disposal of GT SoftGOT3000 according to the procedure shown in Figure 8.
- 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.

Table 12 Implementation items related to security policies and the usage environment

No.	Item	Settings for security functions	Reference
1	Precautions for removing/disposing of connected devices	When removing or disposing of a device connected to GT SoftGOT3000, 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 GT Soft3000 series are set and operate as intended.	-
3		When communication with GT SoftGOT3000 is no longer required, end the session immediately.	-
4	Backup implementation and management	The protected assets of GT SoftGOT3000 and connected devices in the system may be lost due to sudden disasters or failures. Perform periodic backups and manage the backup data properly.	2.4.13 2.4.14 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 describes how to set and use security functions of GT SoftGOT3000. 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.

- GT SoftGOT3000 User's Manual
- GT Designer3 (GOT3000) Screen Design Manual
- GOT3000 Series User's Manual (Utility & Maintenance Functions)

This chapter describes the following security functions.

- Security function setting function (2.4.1)
- Operator authentication function (2.4.2)
- Mobile code execution control function (2.4.3)
- Operation setting function (2.4.4)
- Input data verification function from external devices (2.4.5)
- Security verification function (2.4.6)
- GT SoftGOT3000 all data initialization function (2.4.7)
- Information protection function (2.4.8)
- Encrypted communication function (2.4.9)
- IP filter function (2.4.10)
- Operation log function (2.4.11)
- DoS attack restriction function (2.4.12)
- GOT data package acquisition function (export function) (2.4.13)
- Restore function (import function) (2.4.14)
- Wireless usage control function (2.4.15)
- Error display function (2.4.16)

2.4.1 Security function setting function

The security function setting function is used to configure the security-related operation settings of GT SoftGOT3000 to the mode to establish a secure system. The mode can be specified in units of GT SoftGOT3000 project data.

Table 13 Security mode

No.	Security mode	Description
1	Mode 1 (security mode 1)	GT SoftGOT2000 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 14 Differences of functions between the modes

No.	Function	Security mode 1	Security mode 2
1	Operator authentication	Effective for only user-created screens in GT SoftGOT3000	Effective for all the operations in GT SoftGOT3000
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

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	○

The operator authentication function is performed using the GT SoftGOT3000 or Windows function.
This function restricts operation of GT SoftGOT3000 screens and access to the protected assets in GT SoftGOT3000 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 GT SoftGOT3000 by unauthorized persons, unauthorized device behavior caused by a setting change, and other risks can be prevented.
If the user authentication function is not enabled, users who can connect to GT SoftGOT3000 can use all functions of GT SoftGOT3000, which may cause information leakages and other threats such as unauthorized device behavior.
To use GT SoftGOT3000 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 in GT SoftGOT3000 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 15 Group

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 GT SoftGOT3000. 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 GT SoftGOT3000 in compliance with IEC 62443-4-2, set the operator authentication function as follows.

- 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 usage notification messages for the following information to give warnings to log 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
- Perform operator authentication before accessing the protected assets.

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 cannot log in again after logging out 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 forgot 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.
- When using the Windows functions, do so basically with administrator privileges.
- Use the Windows function AppLocker or other functions to control applications executable by specific users.

- 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 (GT SoftGOT), 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 (GT SoftGOT) 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)

○: Use -: Do not use

GT SoftGOT3000 function	-	Windows or external environment function	○

Mobile code execution control is performed using the Windows function. This function restricts the execution of mobile code that may be executed when the web browser function or application interaction function of GT SoftGOT3000 is used. The mobile code execution control function prevents malicious codes from being read.

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 Operation setting function

○: Use -: Do not use

GT SoftGOT3000 function	-	Windows or external environment function	○

The operation setting function is performed using the Windows function. This function notifies the user of an exception in the GT SoftGOT3000 system in a Windows dialog box when an error occurs in GT SoftGOT3000 and it can no longer maintain normal operation.
The operation setting function prevents necessary functions from stopping due to unintended operations executed by GT SoftGOT3000.

2.4.5 External device input data verification function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

Verification of input data from external devices is performed using the GT SoftGOT3000 function. GT SoftGOT3000 verifies whether data input from the outside of the trust boundary is in accordance with the specifications.
The input data verification function for external devices prevents unauthorized data that affects necessary functions from being input due to operational mistakes or other errors.

2.4.6 Security verification function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

Security verification is performed using the GT SoftGOT3000 function. To use the product in compliance with IEC 62443-4-2, the customer is required to periodically check that the security functions of GT SoftGOT3000 operate according to the intended settings.
The security verification function prevents unauthorized persons from accessing or operating GT SoftGOT3000 due to setting mistakes or other errors, thereby ensuring that the security functions run as intended.

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

2.4.7 GT SoftGOT3000 all information initialization function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

GT SoftGOT3000 all information initialization is performed using the GT SoftGOT3000 function. Uninstallation using the uninstaller and the uninstallation exclusion data deletion function are available.

* The uninstallation exclusion data deletion function deletes folders and files that are not deleted by uninstallation.

You can delete all files related to GT SoftGOT3000 by executing the function to delete uninstallation exclusion data, then uninstalling GT SoftGOT3000. Only users with administrator privileges can execute the uninstallation exclusion data deletion function.

This function enables disposal of the personal computer with GT SoftGOT3000 installed securely.

2.4.7.1 Precautions

- If [Virtual Drive] in the [Environment] dialog has been changed from the default, the destination folders and files are not deleted even if this function is executed. To use the product in compliance with IEC 62443-4-2, do not change the default setting of [Virtual Drive].

2.4.8 Information protection function

There are two types of information protection functions as follows.

- File tampering check function
- Confidentiality protection function

2.4.8.1 File tampering check function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

File tampering check is performed using the GT SoftGOT3000 function. This function checks that files affecting the control of GT SoftGOT3000 have not been tampered.
By using the file tampering check function, data is protected from spoofing due to accidental causes that could result in the shutdown of the protected assets.

The function targets files that affect the control of GT SoftGOT3000, and checks that the files have not been tampered.

2.4.8.2 Confidentiality protection function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

Confidentiality protection is performed using the GT SoftGOT3000 function. This function protects the confidentiality of the information assets in GT SoftGOT3000 by encryption and operator authentication to control access.
By using the confidential information protection function, the data stored in GT SoftGOT3000 is protected from being disclosed by writing of incorrect application data due to operational mistakes or other errors.

The confidentiality of information assets in GT SoftGOT3000 is protected by the following methods.

① Encryption of information assets
② Access control by operator authentication
③ Application execution control using Windows AppLocker

2.4.8.3 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.

2.4.9 Encrypted communication function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

Encrypted communication is performed using the GT SoftGOT3000 function. This function encrypts communication data for communications with target devices across the trust boundary. By using the encrypted communication function, communication data is protected from disclosure due to system failure.

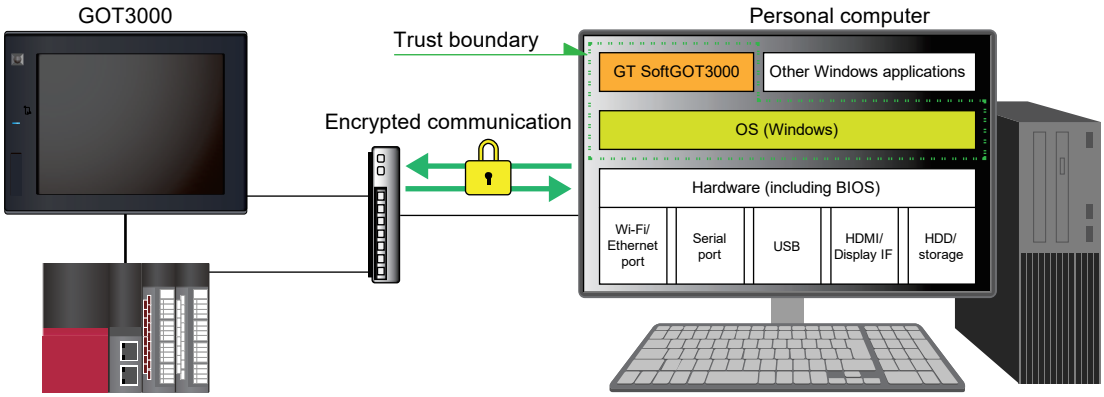


Figure 9 Image of the system configuration for encrypted communication

The target of encrypted communications is the information system network that communicates with the outside of the trust boundary, which is subjected to network attacks.
To use the GOT in compliance with IEC 62443-4-2, encrypt communication with target devices across the trust boundary.

2.4.9.1 Communication functions with encryption

- 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 GT SoftGOT3000.

Table 16 Functions using encrypted communication

No.	Function
1	MX controller (encrypted communication)
2	GOT Mobile (Web server) function
3	OPC UA server function
4	E-mail send function
5	OPC UA client function
6	SoftGOT-GOT link function

2.4.9.2 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 GT SoftGOT3000, and create a certificate using the utility function.

2.4.9.3 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.
- GT SoftGOT3000 allows you to change the time of the operating environment (personal computer time) at any timing. Be careful when changing the time because the expiration date of the certificate refers to the time of the environment in which GT SoftGOT3000 is running (personal computer time). After changing the time, the certificate may be valid or invalid when you check the expiration date.
- A system alarm is issued 90 days before the electronic certificate expires. Update the expiration date of the certificate.
- When the GOT Mobile function is used, the expiration date of the certificate is not notified by the system alarm.

2.4.10 IP filter function

○: Use -: Do not use

GT SoftGOT3000 function	-	Windows or external environment function	○

IP filtering is performed using the Windows or external environment function.
This function restricts the IP addresses of devices connected to GT SoftGOT3000 when Ethernet connection is used, thereby preventing access by incorrect IP address specification and enabling 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.

To specify whether to apply the IP filter function, use the Windows function.

- When applying the IP filer, block the communications from the specific IP addresses using the Windows Firewall function. If not applying the IP filter, you will not configure the settings with the Windows Firewall function.
- Specify whether to permit (transmit) or prohibit (block) Ethernet communication with external devices with IP addresses specified in the filter target list*. (Default setting: Transmit) This function is controlled by the Windows Firewall.

* List of IP addresses of the filtered external devices The list is created in Windows Firewall.

2.4.10.1 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. Also use other countermeasures to ensure the security of GT SoftGOT3000 and the system against unauthorized access from external devices, DoS attacks, computer viruses, and other cyber-attacks.
  The following shows examples of countermeasures against unauthorized access.
  - Installing firewalls and VPNs

2.4.11 Operation log function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	○

The operation log function includes the alarm monitoring and operation log functions of the GOT3000, the application log function that records logs related to the operation and actions of GT SoftGOT3000, and the Windows event management function as a Windows application.
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.

- By setting the security mode to "Mode 2", the operation log function records logs compliant with IEC 62443-4-2.
- The event history as a Windows application is obtained through the Windows Event Viewer.

The following functions are subject to system log recording.

Table 17 Security functions and corresponding logging functions (GT SoftGOT3000)

○: Use -: Do not use

No.	Security function	Operation log	System alarm observation
1	Operator authentication function	○	-
2	Operation setting function	-	○
3	GT SoftGOT3000 all information initialization function	○	-
4	Encrypted communication function	○	○
5	GOT data package acquisition function (export function)	○	-
6	Restore function (import function)	○	-

Table 18 Security functions and corresponding logging functions (Windows)

○: Use -: Do not use

No.	Security function	Event output by Windows
1	IP filter function	○
2	Restriction function against DoS attacks	○

2.4.11.1 Checking the recorded logs

- The recorded logs can be checked by converting them to CSV or Unicode text files using the resource data conversion function of GT Designer3.
- Only the users who are given the operation authority by operator authentication can check the recorded operation logs.
- When converting application logs, the password set at the GT SoftGOT3000 startup is required.
- 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 GT SoftGOT utility.
- If GT SoftGOT cannot be started for any reason, restore it using the following method. Restoring GT SoftGOT allows you to check the logs in the operation information in the utility.
  - Write the project data using the same encryption password as the one set for the operation log file from the engineering tool

2.4.11.2 Precautions for the execution of the uninstallation exclusion data deletion function

- When executing the uninstallation exclusion data deletion function, obtain the operation log file from the save destination, and delete the save destination folder and operation log file.

2.4.11.3 Precautions

- When the log file created by the application log function is encrypted, a password information file is created to record the application log password required for encryption. If the application log password is not set, a password edit dialog appears when GT SoftGOT3000 starts, prompting you to set a password.
- If Windows event logs are retained indefinitely, they may occupy storage space and affect the operation of GT SoftGOT3000. Please change the retention period from the Windows Event Viewer to avoid affecting the operation of your computer.

2.4.12 Restriction function against DoS attacks

○: Use -: Do not use

GT SoftGOT3000 function	-	Windows or external environment function	○

DoS attack restrictions are performed using the Windows or external environment function.
The following controls are applied when the occurrence of a DoS event is determined. This prevents increased network traffic that could result in the shutdown of the protected assets.

① Blocking unauthorized access by Windows Firewall
② Restricting the bandwidth of networks used by GT SoftGOT3000

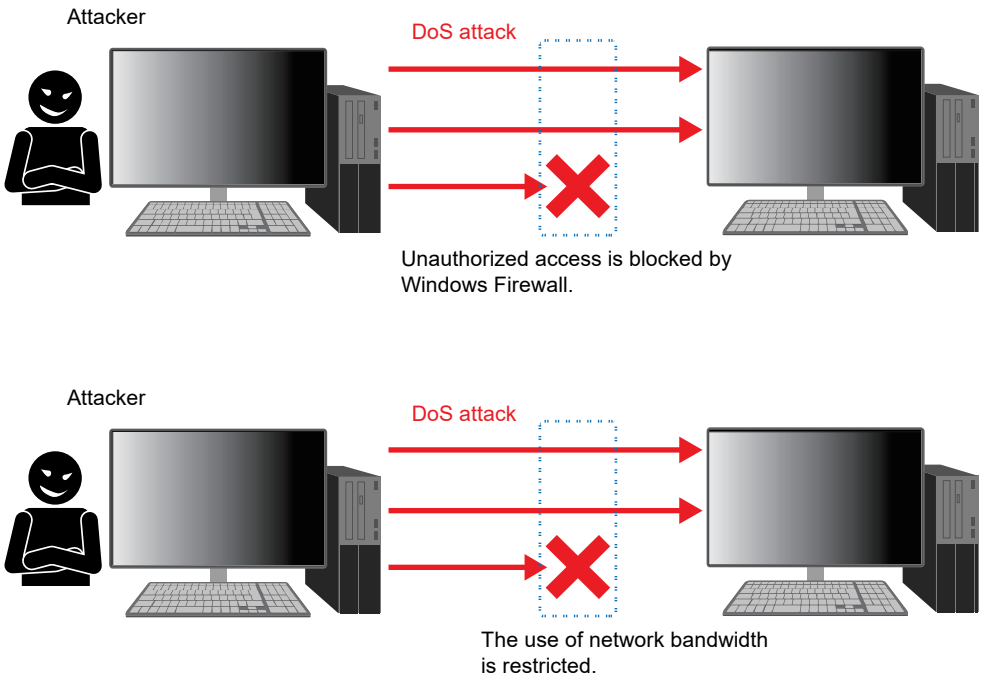


Figure 10 Overview of the DoS attack restriction function

2.4.12.1 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. Also use other countermeasures to ensure the security of GT SoftGOT3000 and the system against unauthorized access from external devices, DoS attacks, computer viruses, and other cyber-attacks.
  The following shows examples of countermeasures against unauthorized access.
  - Installing firewalls and VPNs
  - Installing antivirus software on the personal computer
- To use the product in compliance with IEC 62443-4-2, use this function in combination with measures against unauthorized access, such as the IP filter function.
- When this function is in operation, screen interactions and application performance may slow down.

2.4.13 GOT data package acquisition function (export function)

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

This function backs up GT SoftGOT3000 configuration data to the user's local folder or another folder using the export function of GT SoftGOT3000.

The backed-up data can be restored using the restore function (import function).

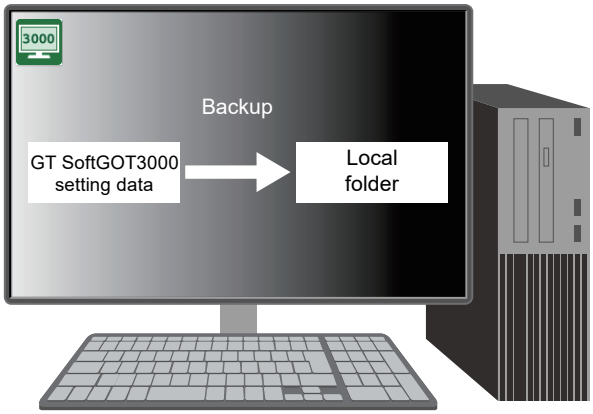


Figure 11 Image of the GOT data package acquisition function

2.4.13.1 Precautions

- To protect the confidentiality of the batch-acquired data, encrypt the data using the confidentiality protection function.
- The target data for GT SoftGOT3000's GOT data package acquisition function (export function) is only the GT SoftGOT3000 setting information. Therefore, the following data must be managed by the user.
  - User files: Resource data, backup data, log data
  - Project data
  - Operator authentication setting information
  - Server certificate

2.4.14 Restore function (import function)

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	-

The restore is performed using the import function of GT SoftGOT3000. This function imports and restores the GT SoftGOT3000 setting information backed up by the GOT data package acquisition function.

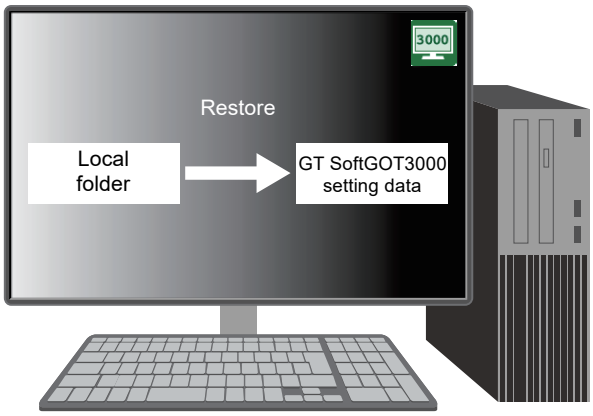


Figure 12 Image of the restore function

2.4.14.1 Precautions

- Encrypt the data backed up by the GOT data package acquisition function (export function) using the confidentiality protection function. To decrypt the data, enter the password set for encryption.
- The server certificate is not covered by backup and thus cannot be restored.
- If backup data is acquired periodically using the GOT data package acquisition function (export function), perform restoration using the latest backup data.

2.4.15 Wireless usage control function

○: Use -: Do not use

GT SoftGOT3000 function	-	Windows or external environment function	○

Wireless usage control is performed using the Windows function. For wireless connection, the connection is controlled using the Windows function.

Figure 13 Image of wireless connection between a personal computer with GT SoftGOT3000 installed and a target device

2.4.16 Error display function

○: Use -: Do not use

GT SoftGOT3000 function	○	Windows or external environment function	○

Errors are displayed using the GT SoftGOT3000 or Windows or external environment function. If an error occurs, this function displays the error using the GT SoftGOT3000 or Windows function.

The following table shows the security functions subject to notification of error information if an error occurs.

Table 19 Error display target functions

○: Applicable, -: Not applicable, ×: No security function

No.	Security function	GT SoftGOT3000	Windows
1	Security function setting function	×	-
2	Operator authentication function	○	○
3	Mobile code execution control function	-	×
4	Operation setting function	×	-
5	Error display function	×	×
6	External input data verification function	○	-
7	Security verification function	×	×
8	GT SoftGOT3000 all information initialization function	×	-
9	Information protection function	×	×
10	Encrypted communication function	×	-
11	IP filter function	-	×
12	Operation log function	×	×
13	Restriction function against DoS attacks	-	×
14	GOT data package acquisition function (export function)	×	-
15	Restore function (import function)	×	-
16	Wireless usage control function	-	×

2.5 Other security functions

GT SoftGOT3000 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
- Functional operation security
- Data transfer security
- Project security

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

- GT SoftGOT3000 User's Manual
- GT Designer3 (GOT3000) Screen Design Manual
- GOT3000 Series User's Manual (Utility & Maintenance Functions)

2.5.1 Screen security function

Setting the "security level" can restrict the operation and display of GT SoftGOT3000 screens, objects, utilities, and system applications 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 GT SoftGOT3000 screens and objects can be controlled according to the security level.

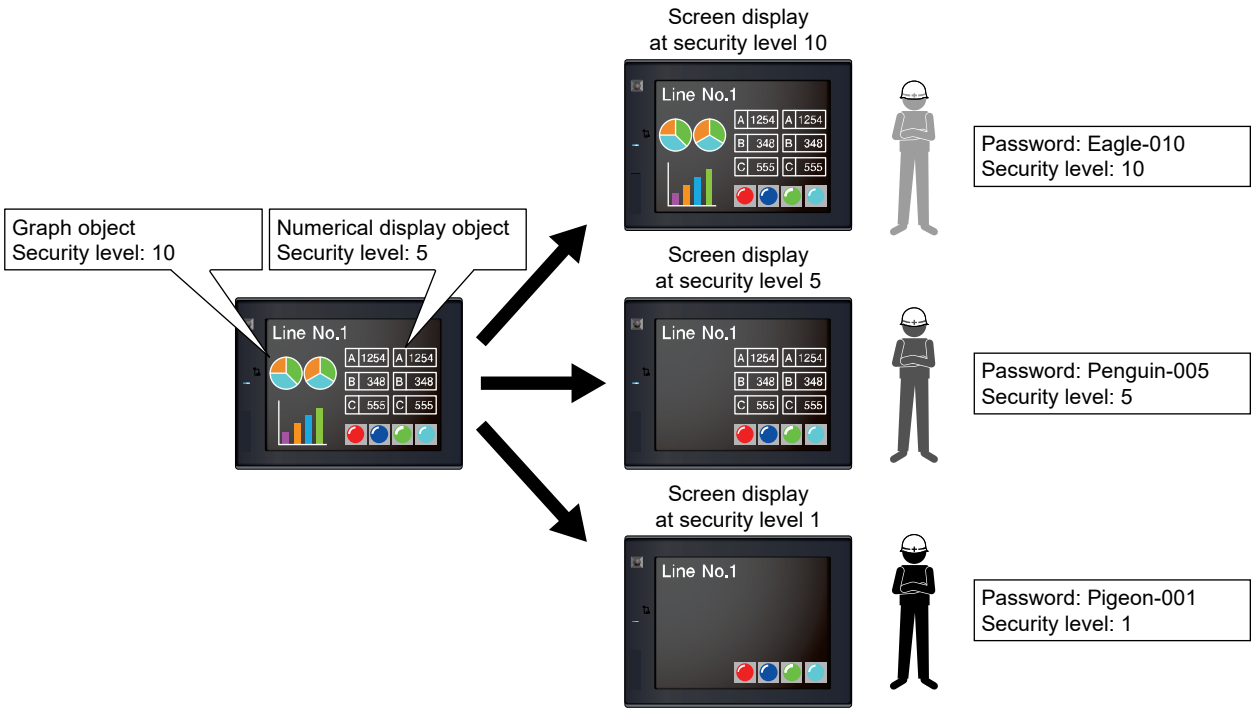


Figure 14 Image of security level password authentication

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

2.5.2 Functional operation security

When the main menu of the GT SoftGOT3000 utility is displayed, authentication with a password can be performed to restrict the operators who are granted operations on the utility screen.
Passwords are set in the engineering tool.

In security mode 2, information operation security is disabled. The restrictions implement by the functional operation security will be implemented by the access privilege of the operator authentication.

2.5.3 Data transfer security

Data transfer security refers to the security of data operations managed by GT SoftGOT3000.
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 project data or resource data, and for overwriting project data.
GT SoftGOT3000 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 GT SoftGOT3000 and project data and resource cannot be read from GT SoftGOT3000.
- If the password is forgotten, reinstall BootOS or perform the GT SoftGOT3000 all information initialization function.

2.5.4 Project security

Displaying and editing of project data can be restricted according to the user.
The setting is performed with the engineering tool.

2.6 Operation and maintenance of GT SoftGOT3000

2.6.1 Recommended GT SoftGOT3000 operation examples

As physical security measures for GT SoftGOT3000, it is recommended to implement area-based access restrictions in the factory and install GT SoftGOT3000 in a secure and monitored location to prevent unauthorized access and destructive actions. 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.

GT SoftGOT3000 is to be installed on a personal computer. Install the engineering software on a personal computer with GT SoftGOT3000 installed and personal computers that communicate with the computer to manipulate the files stored in GT SoftGOT3000. To prevent these personal computers from being compromised and files stored in GT SoftGOT3000 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 GT SoftGOT3000.

- 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
- Applying publicly available security updates
- Implementing security tools provided by Microsoft

To protect the network within the trust boundary of GT SoftGOT3000 and the network where personal computers are located from unwanted external access, network devices such as firewalls and routers at the boundary are recommended between the Internet and the factory network.

As part of continuous security operation in a factory where GT SoftGOT3000 is installed, it is recommended to perform the check items for each function as shown in the table.

Table 20 Items recommended to be checked as continuous security operation

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 an SD memory card.
2	Acquired log check	To detect suspicious behavior, checking the logs acquired using the operation log function is effective. For example, potential unauthorized access can be checked by reviewing the failed login attempt log.
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 GT SoftGOT3000, it is recommended to select an appropriate person as an administrator. Sufficient education and training are also recommended to GT SoftGOT3000 users to ensure proper setup, management, and operation of the product. Use GT SoftGOT3000 appropriately according to user's manuals and this guideline.

2.6.2 Periodic maintenance

To keep the system and GT SoftGOT3000 secure, perform periodic security maintenance (at least once a year is recommended). Specifically, it is recommended to check that the functions listed in Table 21 operate properly. Table 22 also shows the functions whose settings affect security. Use this information to also periodically check the accuracy of the settings.

Table 21 Operation verification items for security functions

No.	Function name	Check item
1	Operator authentication function	An operator can log on only when the correct operator name and password are entered in combination.
		An operator is locked out when an incorrect operator name or 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	Mobile code subject to restriction is not executed.
3	Encrypted communication function	If a client device does not have the server certificate generated by the GT SoftGOT3000 series, an error occurs and no communication is performed when encrypted communication is performed with the client device.
		Checks if the certificate has expired.
4	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.
5	Operation log function	The event is consistent with the contents of the system log.
		The occurrence time of the event is consistent with the clock data in the system log.
6	GOT data package acquisition function (export function)	When the GOT data package acquisition function is executed, encrypted backup data is generated in the user's local folder.
7	Restore function (import function)	When the restore function is executed, the state of GT SoftGOT3000 can be restored to the state before backup using the backup data.
		Before executing the restore function, make sure that the encrypted backup data can be restored correctly.
8	Wireless usage control function	Wireless connection can be established by entering the set password.
		If an incorrect password is entered, wireless connection is not established.

- Apply the publicly available security updates.
- Use the latest version of GT SoftGOT3000.

Table 22 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	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 Discarding GT SoftGOT3000

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 discard the product according to the following procedure when terminating the use of this product.

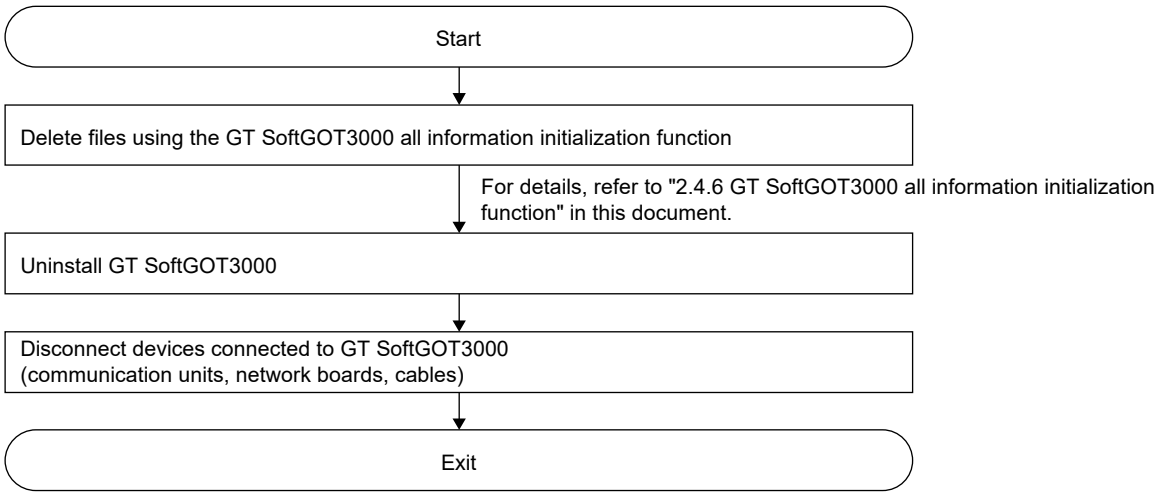


Figure 15 How dispose of the product

Note that the all information initialization function 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 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 storage on which GT SoftGOT3000 is installed or destroying the magnetic parts.

To ensure the stability of overall factory control and the preservation of data stored in the system, stop the GT SoftGOT3000 series after the system has been shut down.

Also, when removing a device connected to the GT SoftGOT3000 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.

2.7.1 Precautions

- The uninstallation exclusion data deletion function of GT SoftGOT3000 does not uninstall applications.
- To dispose of GT SoftGOT3000 in compliance with IEC 62443-4-2 after use, be sure to execute the GT SoftGOT3000 all information initialization function. If the application is uninstalled without all information initialization processing, the uninstallation exclusion data deletion function is not executed, and some files remain in the personal computer even after uninstallation.

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 GT SoftGOT3000?

[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 GT SoftGOT3000 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 GT SoftGOT3000 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 GT SoftGOT3000?

[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 GT SoftGOT3000 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 GT SoftGOT3000 to protect customer systems and data from security threats?

[A4]:

As a general security policy for GT SoftGOT3000, we are promoting measures based on the four pillars described in [A3]. For GT SoftGOT3000, we implement the IP filter function, operator authentication function, 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 GT SoftGOT3000 against evolving attacks.

For information on the security functions of GT SoftGOT3000, refer to "2.2.4 Security functions of GT SoftGOT3000" 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 GT SoftGOT3000?

[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.