FA SYSTEM SECURITY GUIDELINE

- SEPARATE VOLUME [NC (M8/M8V SERIES)] -

MITSUBISHI ELECTRIC CORPORATION

IB-1501811(ENG)-A

Revision History

Date	Document number	Notes
Aug. 2025	IB-1501811(ENG)-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	International standards related to security of control systems developed by IEC (International Electrotechnical Commission) TC 65/WG 10 and ISA (The International Society of Automation) ISA99 Committee[2].
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [3].
NC	Numerical Control A program control method that uses numerical signal commands and a numerical control device that calculates these commands. This function commands and controls the tool position, feedrate, etc.
AP	Access Point A device to provide a network interface where wireless clients access the wired network. The AP as a wireless LAN function provided by NC provides a network interface where the wireless clients can access NC only.
STA	Station mode One of the operation modes for wireless devices. A mode to connect to the access point (AP) as a terminal (station).
SSID	Service Set Identifier An identification name for the access point (AP) in wireless LAN. A name given to a terminal to identify and specify the destination network.
BSSID	Basic Service Set Identifier One of the identifiers of a wireless access point and a wireless network in the wireless LAN. Usually the MAC address of the access point is used as is.
IPS	Intrusion Prevention System Intrusion prevention system. A system that detects unauthorized intrusions via a network and blocks the network in question. While the IDS only notifies of the detection of an intrusion, the IPS automatically blocks communications when an intrusion is detected, preventing the intrusion.
IDS	Intrusion Detection System Intrusion detection system. A system that detects unauthorized intrusions via a network and notifies users of them.
VPN	Virtual Private Network A technology that ensures the security on communication paths by establishing a virtual dedicated line over the Internet or public lines for communications using technology such as encryption.
FW	Firewall A device equipped with filtering functions such as packet filtering, communication restriction functions such as bandwidth limitation, and address translation functions such as NAT (Network Address Translation) and NAPT (Network Address Port Translation).
RIO communication	Communication in which NC communicates with remote I/O unit and operation panel I/O unit.
Field unit	A unit, such as remote I/O unit, operation panel I/O unit, etc., to create signals to be input in the NC unit and output signals created by the NC unit.

[1] Mitsubishi Electric FA Terminology Dictionary
https://www.mitsubishielectric.com/fa/service-support/global/fa_reference/index.html

[2] International Society of Automation (ISA), https://www.isa.org/intech/201810standards

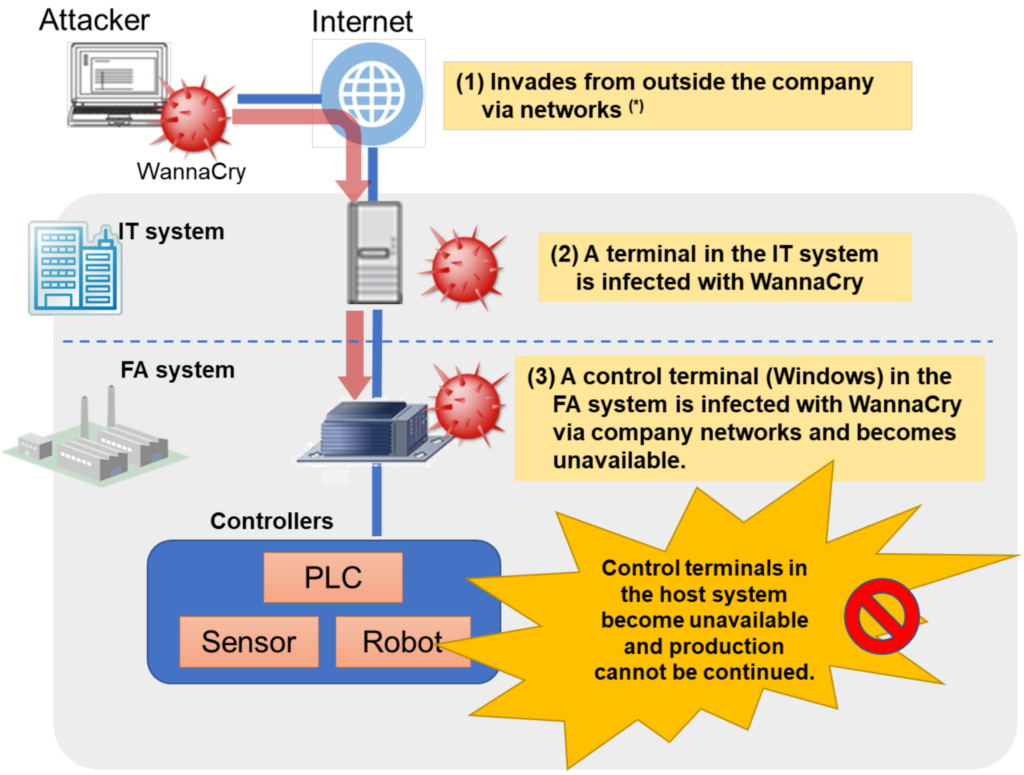
[3] NIST CSRC Glossary, https://csrc.nist.gov/glossary/term/integrity

Term	Description
Field network communication	A network used for communication between the NC unit and field devices. Example of field network communication: CC-Link IE TSN, EtherNet/IP, etc.
Field device	A device connected with the NC unit by field network communication. Example of field device: PLC, robot, I/O unit, etc.
RGU	Remote Service Gateway Unit A unit used for remote service function.

1 Introduction

1.1 Background

With the rapid development of the Internet and IT/IoT technologies, IT utilization in FA systems is increasing to improve the productivity of factories. As the IT utilization in FA systems advances, conventional thinking that FA systems cannot be infected by malware or exposed to cyberattacks because they are "dedicated systems" or "closed" is no longer valid, and the security risks on FA systems are increasing. In fact, in 2017, a malware called WannaCry, which targeted IT systems, caused significant damage, including the shutdown of factories. (Figure 1)


Attacker
Internet
WannaCry
(1) Invades from outside the company via networks (*)
IT system
(2) A terminal in the IT system is infected with WannaCry
FA system
(3) A control terminal (Windows) in the FA system is infected with WannaCry via company networks and becomes unavailable.
Controllers
PLC
Sensor
Robot
Control terminals in the host system become unavailable and production cannot be continued.

(*) Attacks TCP 445 port directly. Infected even without opening an e-mail.

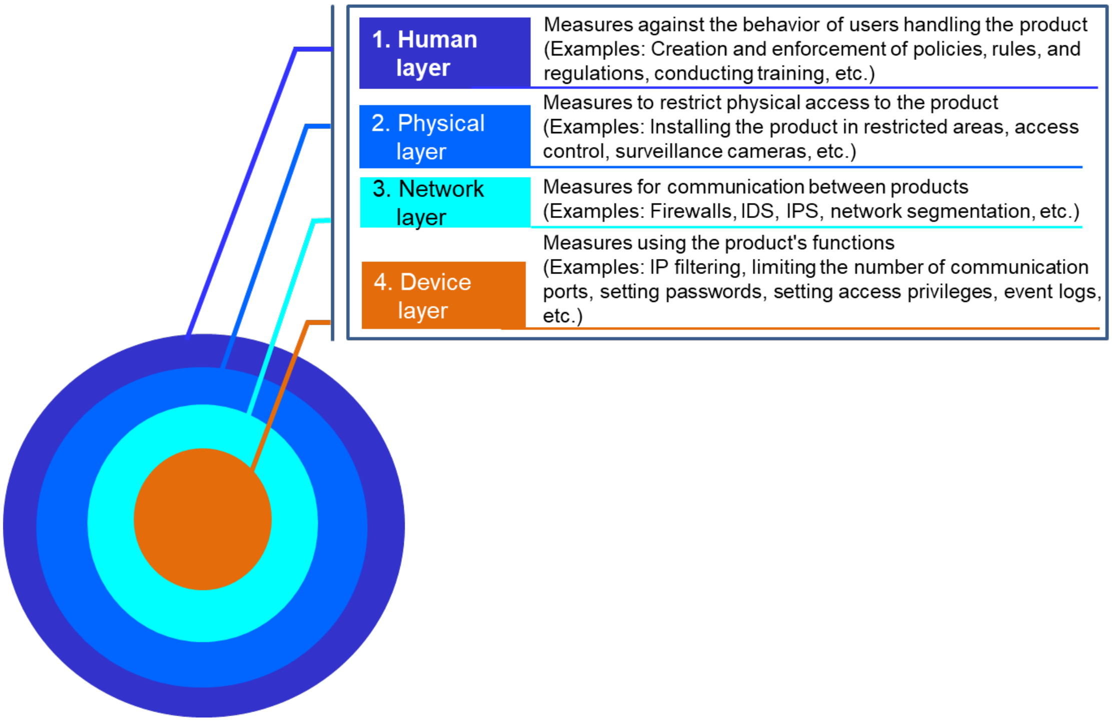
Figure 1 Example of WannaCry infection route and damage to FA system

To protect FA systems from such threats, it is important to combine multiple security measures hierarchically, ranging from physical security measures for factories such as access control, human security measures such as rules and education applied to users who handle products, to security measures on networks and FA devices in factories. This improves security and reduces the impact of attacks by "raising the costs of attacks for the attacker and raising the bar to attack" and "enhancing detection and prevention capabilities in the event of an attack". Such a concept of security measures is called "defense in depth" and is recommended in the international standard IEC 62443. As a manufacturer and seller of FA devices, Mitsubishi Electric Corporation (hereinafter referred to as "Mitsubishi Electric") is developing the NC that is compliant with IEC 62443 for realizing and maintaining safe and secure FA systems for our customers.

1.2 Defense-in-depth strategy for protecting FA products

Defense in depth in security measures refers to the concept of taking countermeasures from different perspectives, such as "human operations", "use of device and facility", "network access", "data access", and "application execution". Mitsubishi Electric divides this perspective into two defense-in-depth measures, one related to the environment (outside the product), and the other related to inside the product, and defines them as the "human layer", "physical layer", "network layer", and "device layer" (Figure 2). Defense in depth reduces the impact of attacks by raising the costs of attacks for the attacker and enhancing detection and prevention capabilities in the event of an attack.

The security function of Mitsubishi Electric products is one of the defense-in-depth measures in the device layer or network layer. To protect the FA system from cyberattacks, measures need to be taken in each of the human layer, physical layer, network layer, and device layer. For example, typical measures include the installation of a firewall to protect against cyberattacks, installation of anti-virus software on personal computers, and access control in the factory.



1. Human layer	Measures against the behavior of users handling the product (Examples: Creation and enforcement of policies, rules, and regulations, conducting training, etc.)
2. Physical layer	Measures to restrict physical access to the product (Examples: Installing the product in restricted areas, access control, surveillance cameras, etc.)
3. Network layer	Measures for communication between products (Examples: Firewalls, IDS, IPS, network segmentation, etc.)
4. Device layer	Measures using the product's functions (Examples: IP filtering, limiting the number of communication ports, setting passwords, setting access privileges, event logs, etc.)

Figure 2 Concept of defense in depth

2 Security of the NC unit

2.1 Purpose of this chapter

This chapter provides the following information to explain Mitsubishi Electric's approach to the security of the NC unit so that it can be used safely and securely in customers' FA systems.

- Security strategy for the NC unit (Section 2.2)
  This section describes the policy on security measures against threats by identifying possible threats to the NC unit. Some countermeasures are performed by the NC unit alone while others are performed in combination with other products.
- Installation method of the NC unit (Section 2.3)
  This section describes how to install the NC unit in an FA system.
- Security functions in the NC unit (Section 2.4)
  This section describes the security functions of the NC unit and how to set them.
- Functions that affect the security risk of the NC unit (Section 2.5)
  This section describes the functions that affect the security risk of the NC unit and how to set them.
- Operation and maintenance method of the NC unit (Section 2.6)
  This section describes the management methods that require attention to operate the NC unit.
- Removal and disposal method of the NC unit (Section 2.7)
  This section describes the recommended methods (e.g., product data deletion functions) for removing and disposing of the NC unit.

Read this guideline and the above related manual carefully to fully understand the security of the NC unit, and use it to realize and maintain safe and secure FA systems.
In addition, refer to the following document for the basic security policy for Mitsubishi Electric FA products including the NC unit, product life cycle initiatives, and examples of FA system construction.

- FA SYSTEM SECURITY GUIDELINE

2.2 Security strategy for the NC unit

This section describes the following items about the security functions of the NC unit.

- Expected usage environment of the NC unit (Product installation environment, network, operation and maintenance methods, etc.)
- Threats to the NC unit
- Policy on countermeasures against threats
- Security functions in the NC unit
- Security measures to be taken outside the product

2.2.1 Expected usage environment of the NC unit

Figure 3 shows the environment where the NC unit is expected to be installed.

Table 1 shows the prerequisites for ensuring security in the installation environment shown in Figure 3. In addition, Figure 3 assumes that an integrated system is installed in which the control unit and display unit are integrated. NC unit refers to a combination of control unit and display unit. These installation environment and usage environment including prerequisites are the premise for the security strategies described in the subsequent sections.

The NC unit is intended for use in equipment to be installed on a production site in a factory. The machine tool contains multiple machines, including the NC unit. External storage and maintenance personal computers are connected to the NC unit for use, however, they are located outside the machine tool because they are portable and used outside the equipment. In addition, there is a server room in the factory, where personal computers for production management and various servers are installed. It is assumed that the NC unit is connected to the network in the factory and has a network configuration to communicate with the external network such as Internet via firewalls or routers.

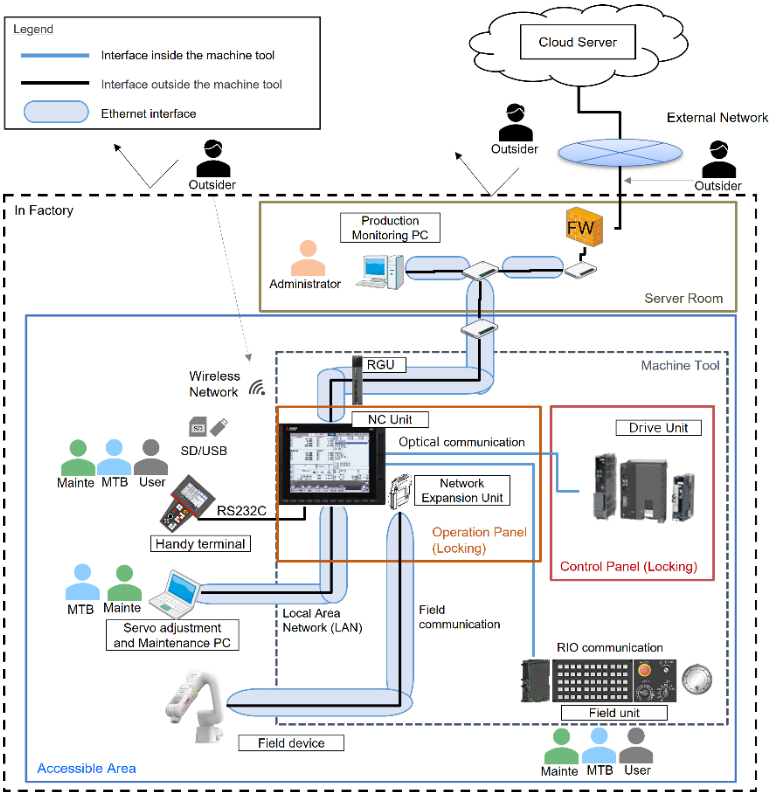


Figure 3 Environment where the NC unit is expected to be installed (Integrated type)

Figure 4 shows a separate-type connection example in which the control unit and display unit are separate. Excluding the NC unit type, the environment is the same as the system configuration for the integrated NC unit shown in Figure 3.

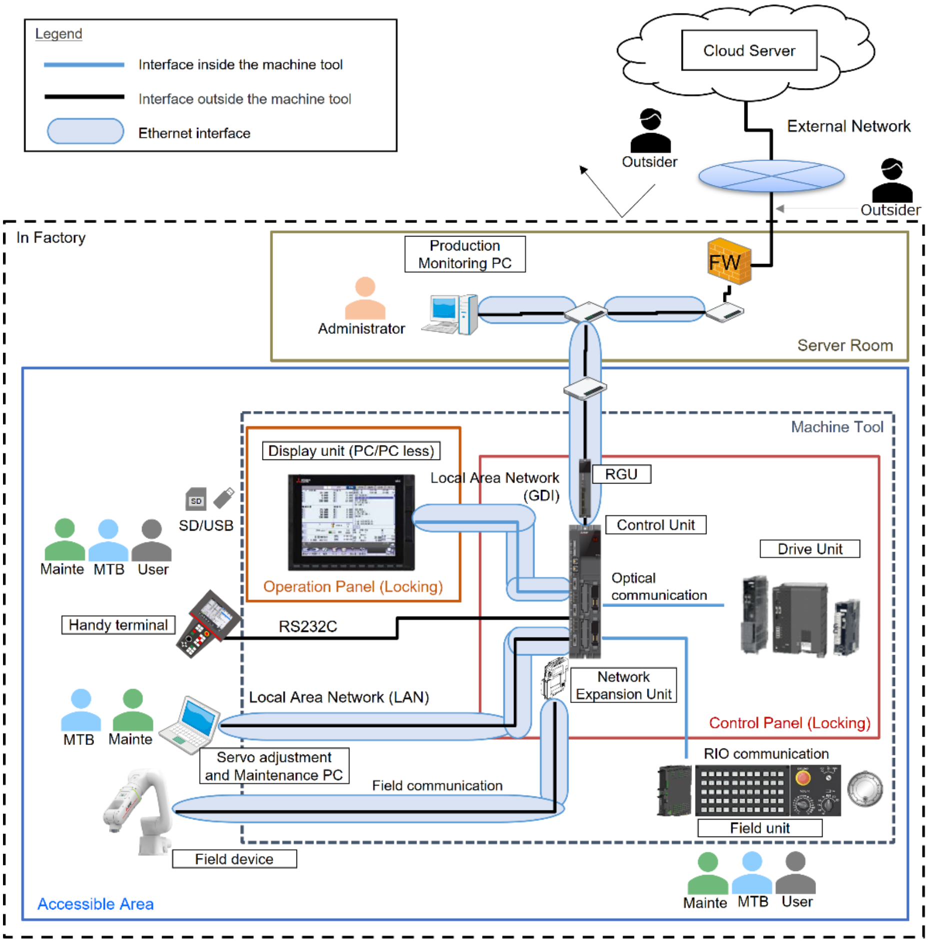


Figure 4 Environment where the NC unit is expected to be installed (Separate type)

Table 1 Prerequisite in the installation environment

No.	Prerequisite	Description
1	Access control	Access control is used to restrict who can enter the factory.
2	Equipment in which the NC unit is installed is locked	The operation panel in which the NC unit is installed is locked, and the devices in the equipment cannot be operated or changed without the permission of the administrator.
3	Management of storage media	Storage media such as SD cards and USB flash drives, which are stored in the locked location, cannot be taken out or input/output without the administrator's permission.
4	Education for users	Users are adequately educated and trained to correctly set, manage, and operate the NC unit.
5	Selection of an appropriate administrator	A person who will carry out the administration appropriately without malicious intent is selected as the administrator.
6	Installation of a firewall	Network switches and firewalls are installed between the network to which the NC unit is connected and the external network, blocking unnecessary communications from the external network.
7	Security on the personal computer that communicates with the NC unit	The personal computers that communicate with the NC unit (personal computer for maintenance and personal computer for production monitoring) have anti-virus software to ensure security.
8	Appropriate password management	Passwords are managed in accordance with internationally recognized and proven password guidelines[4].

[4] One example of password guidelines provides NIST SP 800-63B issued by the National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology (NIST), NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management

https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final

Table 2 describes the devices and networks in Figure 3.

Table 2 Devices, applications, and networks in the environment

No.	Term	Description
1	Personal computer for production management	A device with software for monitoring the status of the control system installed.
2	Personal computer for maintenance	A device with an engineering tool necessary for maintaining the NC unit installed.
3	Cloud server	This server has a web service that collects the operation conditions of machine tools sent from the NC unit or RGU and allows users to view the collected operation conditions of machine tools.
4	Field communication, RIO communication	A network used for communication between the NC unit and field devices.
5	Firewall	A device equipped with filtering functions such as packet filtering, communication restriction functions such as bandwidth limitation, and address translation functions such as NAT (Network Address Translation) and NAPT (Network Address Port Translation).
6	Network switch	A device that uses network layer information in the OSI reference protocol to separate networks with a virtual router or VLAN (Virtual Local Area Network). The network switch can also be used together with the network router.
7	External network	A network that is outside the firewall and beyond the factory's authority to manage the network. Example of external network: Internet
8	Wireless network	A network that exchanges data using radio waves without using cables. An example of a wireless network is a wireless LAN.
9	Field device	A device connected with the NC unit by field network communication. Example of field device: PLC, robot, I/O unit, etc.

Access to devices can be physically controlled by restricting entry to individual areas of the factory or by applying physical locks to the device storage areas. These physical access controls are also important security elements. For the use of the NC unit, the area classification shown in Table 3 is assumed from a security perspective.

Table 3 Area classification and operation method

No.	Term	Description
1	Server room	A room that stores devices critical to continue the operation of the control line system, such as a device that manages the network. To protect against unauthorized access and vandalism, measures are taken so that only specific people can enter and exit the room (e.g., entry and exit management).
2	Machine tool	A machine to perform machining of metallic workpieces by cutting, grinding, etc. It contains the control panel and the operation panel.
3	Control panel	Devices such as control unit and drive unit are stored. To protect against unauthorized access and vandalism, measures (e.g., entry and exit management) are taken to ensure that only specific people who are allowed to enter the production site can operate the equipment.
4	Operation panel	Devices such as display unit and operation panel I/O unit are stored. To protect against unauthorized access and vandalism, which are other than display operations on the front, measures (e.g., fastening the panel using screws) are taken to ensure that only specific people who are allowed to enter the production site can operate the equipment.
5	Accessible area (Production site)	An area where only the users of the machine tool or control line system can enter.
6	Factory	An area with both an accessible area and a server room.

Table 4 shows the users who use the NC system.

Table 4 Definition of users

No.	User	Details	Definition	Malicious or not	Remarks
1	End user (User)	Administrator (Administrator)	Responsible for managing local servers such as personal computers for production management. The administrator can enter and exit the information security areas or accessible areas. Assuming that the administrator is an employee of the user or an affiliated company, they shall undergo an identity check and training. They will also not intentionally take any actions that pose a threat.	Not malicious	👤
2		Asset owner Operator Maintenance worker	A designer who uses machine tools to design machines. This user enters the accessible areas and operates control devices via the NC display. Assuming that the asset owner, operator and maintenance worker are an employee of the user or an affiliated company, they shall undergo an identity check and training. They will also not intentionally take any actions that pose a threat.	Not malicious	👤
3	Machine tool builder (MTB)	Designer Maintenance worker	Responsible for the design or maintenance of machine tools. This user enters the accessible areas and maintains control devices via a personal computer or NC display. Assuming that the designer and maintenance worker are an employee of the machine tool builder or its affiliated company, they shall undergo an identity check and training. They will also not intentionally take any actions that pose a threat.	Not malicious	👤
4	Mitsubishi Electric people concerned (Mainte)	Maintenance worker	Responsible for the maintenance of NC unit. This user enters the accessible areas and maintains control devices via a personal computer or NC display. Assuming that the designer and maintenance worker are an employee of the Mitsubishi Electric Corporation or an affiliated company such as Mitsubishi Electric Mechatronics Engineering Corporation (hereinafter referred to as "MMEG"), they shall undergo an identity check and training. They will also not intentionally take any actions that pose a threat.	Not malicious	👤
5	Third party (Outsider)	-	An unspecified number of people on the Internet. They attempt to gain unauthorized access to services and local networks that can be accessed from the Internet by exploiting vulnerabilities.	Malicious	👤

2.2.2 Threats to the NC unit

Mitsubishi Electric assumes the threats shown in Figure 5 and Table 5 in the usage environment of the NC unit shown in Figure 3 of 2.1.1 based on the risk assessment of the module and knowledge of publicly known attack cases.

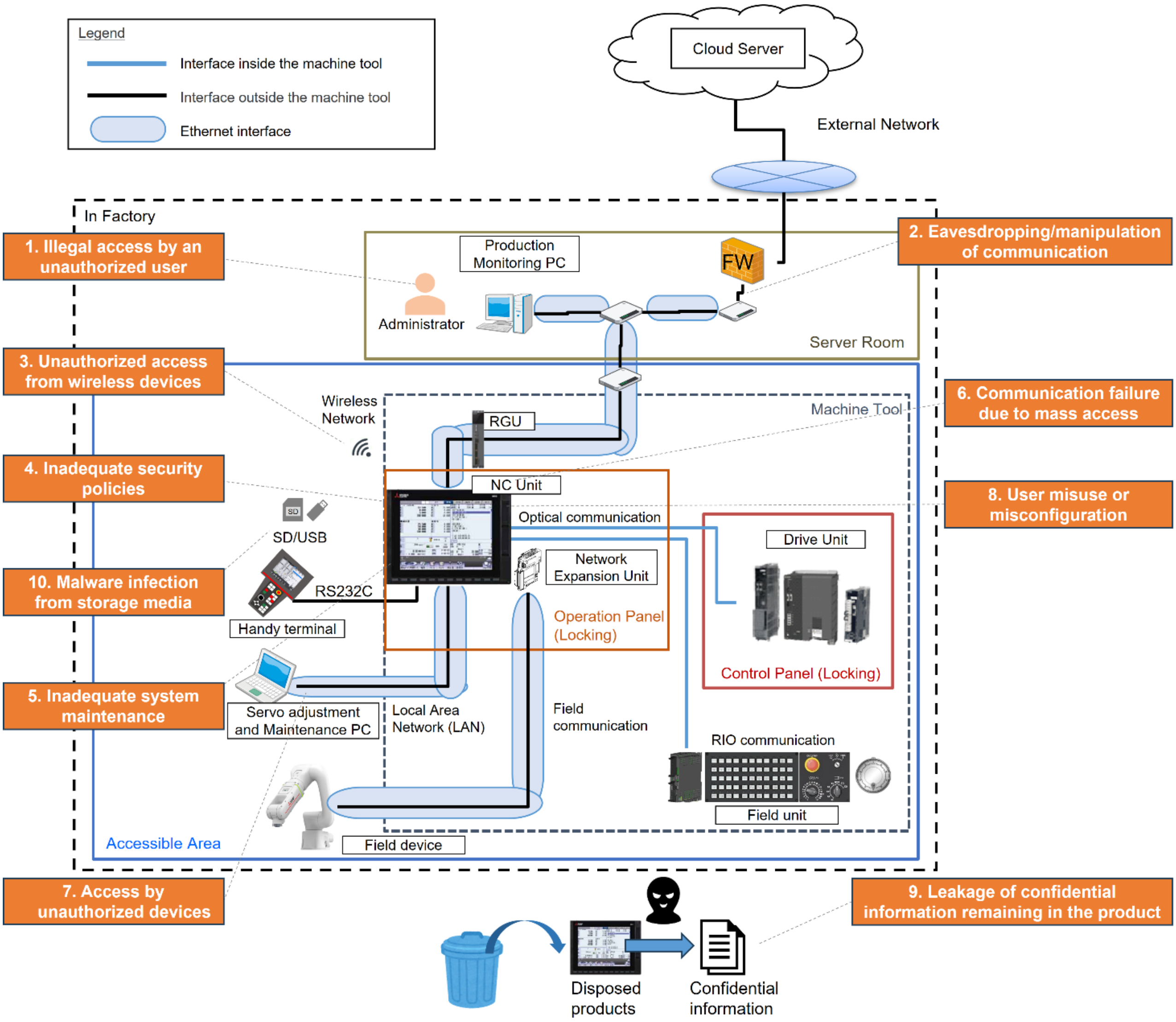

Legend
Interface inside the machine tool
Interface outside the machine tool
Ethernet interface
Cloud Server
External Network
In Factory
1. Illegal access by an unauthorized user
2. Eavesdropping/manipulation of communication
Production Monitoring PC
FW
Administrator
Server Room
3. Unauthorized access from wireless devices
Wireless Network
RGU
Machine Tool
6. Communication failure due to mass access
4. Inadequate security policies
NC Unit
Optical communication
8. User misuse or misconfiguration
SD/USB
Drive Unit
Network Expansion Unit
10. Malware infection from storage media
RS232C
Operation Panel (Locking)
Handy terminal
Control Panel (Locking)
5. Inadequate system maintenance
Servo adjustment and Maintenance PC
Local Area Network (LAN)
Field communication
RIO communication
Field unit
Accessible Area
Field device
7. Access by unauthorized devices
9. Leakage of confidential information remaining in the product
Disposed products
Confidential information

Figure 5 Threats to the NC unit

Table 5 Description of threats

No.	Threat name	Description
1	Illegal access by an unauthorized user	Illegal access is made by a user unauthorized by the administrator.
2	Eavesdropping/manipulation of communication	Communication between the NC unit and an external device is eavesdropped or manipulated.
3	Unauthorized access from wireless devices	Illegal access is made from wireless devices unauthorized by the wireless communication function.
4	Inadequate security policies	The security functions related to the communication function have not been reviewed, so the system is in an incorrect configuration.
5	Inadequate system maintenance	System maintenance has not been performed, so the system is operated in an environment where vulnerabilities are left unattended or communication data changes accidentally.
6	Communication failure due to mass access	Increased communication traffic in the network prevents necessary communication.
7	Access by unauthorized devices	Illegal access is made from unauthorized devices.
8	User misuse or misconfiguration	Illegal access is made by an unexpected user.
9	Leakage of confidential information remaining in the product	Information leakage occurs through the extraction of confidential information remaining in the discarded products or others.
10	Malware infection from storage media	The device is infected by malware through a SD card or USB flash drive, and does not work normally.

2.2.3 Policy on countermeasures against threats

Figure 6 shows the policy on countermeasures against threats to the NC unit. The policy includes not only the countermeasures to be taken in the NC unit, but also the ones to be taken in the customer's environment.

To realize the defense in depth described in 1.2, security measures need to be taken in the human, physical, and network layers, which are difficult to take for the NC unit. Therefore, it is necessary to maintain security measures not only for the NC unit but also for the entire FA system.

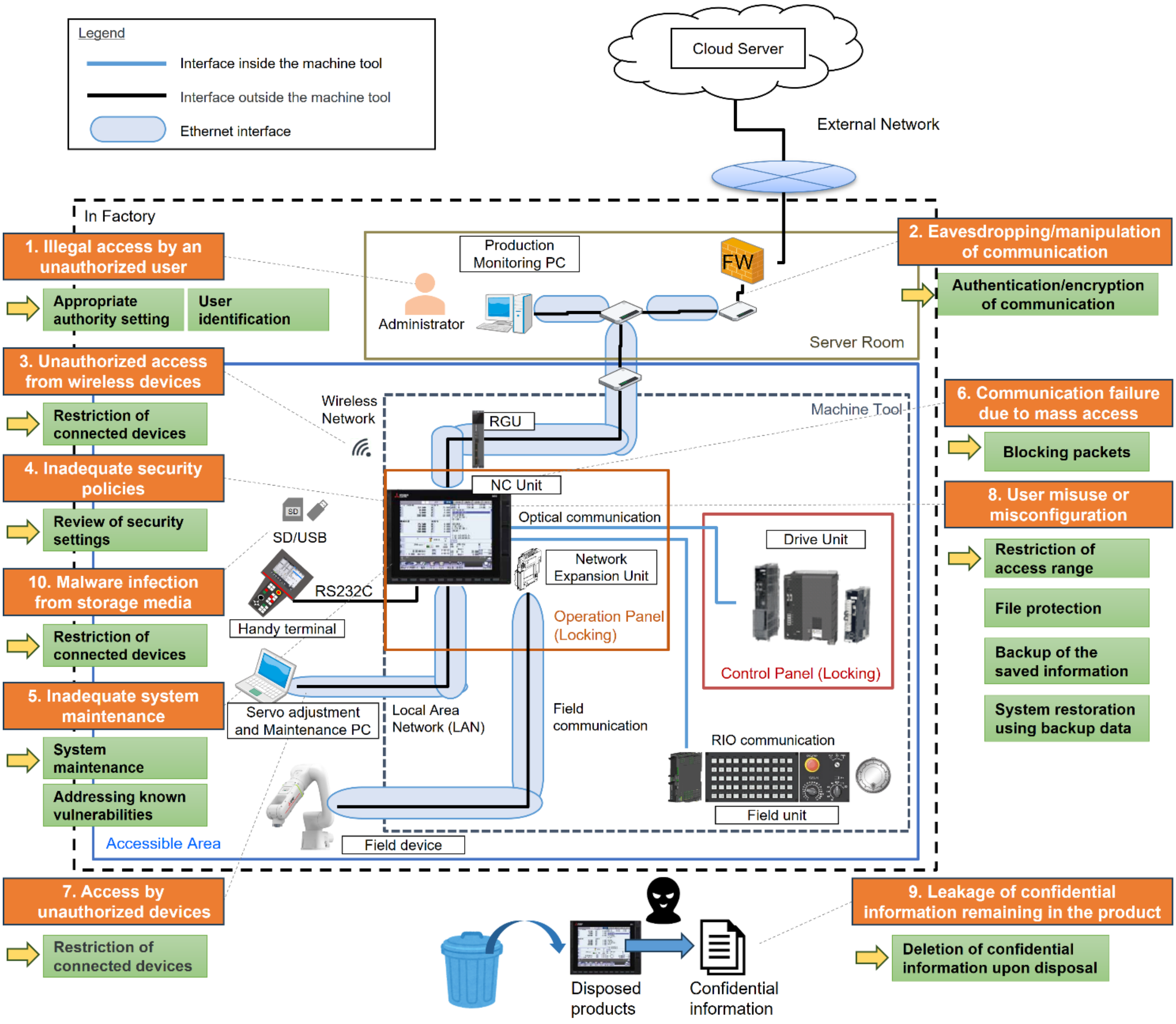

Legend
Interface inside the machine tool
Interface outside the machine tool
Ethernet interface
Cloud Server
External Network
In Factory
1. Illegal access by an unauthorized user
Appropriate authority setting
User identification
Production Monitoring PC
Administrator
FW
Server Room
2. Eavesdropping/manipulation of communication
Authentication/encryption of communication
3. Unauthorized access from wireless devices
Restriction of connected devices
Wireless Network
RGU
Machine Tool
6. Communication failure due to mass access
Blocking packets
4. Inadequate security policies
Review of security settings
SD
SD/USB
NC Unit
Optical communication
8. User misuse or misconfiguration
Restriction of access range
File protection
Backup of the saved information
System restoration using backup data
Drive Unit
Network Expansion Unit
10. Malware infection from storage media
Restriction of connected devices
RS232C
Handy terminal
Operation Panel (Locking)
Control Panel (Locking)
5. Inadequate system maintenance
System maintenance
Addressing known vulnerabilities
Servo adjustment and Maintenance PC
Local Area Network (LAN)
Field communication
RIO communication
Field unit
Accessible Area
Field device
7. Access by unauthorized devices
Restriction of connected devices
9. Leakage of confidential information remaining in the product
Deletion of confidential information upon disposal
Disposed products
Confidential information

Figure 6 Policy on countermeasures against threats to the NC unit

Table 6 Policy on countermeasures against threats to the NC unit

No.	Threat name	Policy on countermeasures	Related functions/measures
1	Illegal access by an unauthorized user	● Appropriate authority setting ● User identification	◆ User authentication ◆ Access restriction ◆ Equipment locking ◆ Selection of the administrator ◆ Installation of a firewall ◆ Installation of IDS/IPS ◆ Security on the personal computer
2	Eavesdropping/manipulation of communication	● Authentication/encryption of communication	◆ Access restriction ◆ Equipment locking ◆ Installation of a firewall ◆ Installation of IDS/IPS ◆ Security on the personal computer ★ Encrypted communication
3	Unauthorized access from wireless devices	● Restriction of connected devices	◆ Removal of unauthorized devices ★ IP filter setting ★ Security function of wireless LAN
4	Inadequate security policies	● Review of security settings	◆ Periodic maintenance
5	Inadequate system maintenance	● System maintenance ● Addressing known vulnerabilities	◆ Periodic maintenance ◆ Firmware update
6	Communication failure due to mass access	● Blocking packets	◆ Installation of IDS/IPS ★ IP filter setting
7	Access by unauthorized devices	● Restriction of connected devices	◆ Removal of unauthorized devices ◆ Access restriction ◆ Equipment locking ★ IP filter setting
8	User misuse or misconfiguration	● File protection ● Backup of the saved information ● System restoration using backup data	◆ Education for users ★ Protection settings ★ Data backup/restoration ★ Operation history
9	Leakage of confidential information remaining in the product	● Deletion of confidential information upon disposal	★ User data deletion
10	Malware infection from storage media	● Restriction of connected devices	◆ Elimination of unauthorized devices

◆ Measures in the operating environment

★ NC security functions

2.2.4 Security functions in the NC unit

The NC unit implements the security functions as described in Table 7 to realize the policy on countermeasures against threats described in 2.2.3.

Table 7 Security functions in the NC unit

Function name		Description	Representative threats to be addressed
Protection settings	Protection settings screen	Restricts accesses to each data item held by NC.	8. User misuse or misconfiguration
	Machine tool builder macro protection	Provides restrictions on viewing machine tool builder macro.	8. User misuse or misconfiguration
	PLC program protection	Provides restrictions on viewing the PLC program.	8. User misuse or misconfiguration
IP filter setting		Identifies the IP address of external devices to allow or deny a connection only from specific IP addresses.	7. Access by unauthorized devices
Security function of wireless LAN		Enables the wireless communication function to provide restrictions on accesses from wireless devices.	3. Unauthorized access from wireless devices
Operation history		Saves NC operation information and history as a data file.	8. User misuse or misconfiguration
Data backup/restoration		Backs up and restores NC data.	8. User misuse or misconfiguration
Encrypted communication		Prevents eavesdropping by encrypted communications. Prevents impersonation by using a certificate.	2. Eavesdropping/manipulation of communication
User data deletion		Deletes the data memory saved in the NC.	9. Leakage of confidential information remaining in a product

2.2.5 Security measures to be taken outside the product

Figure 7 and Table 8 show the security measures to be taken in the usage environment of the customer with the prerequisites (Table 1) in the usage environment (Figure 3) of the NC unit and policy on countermeasures against threat (2.2.3).

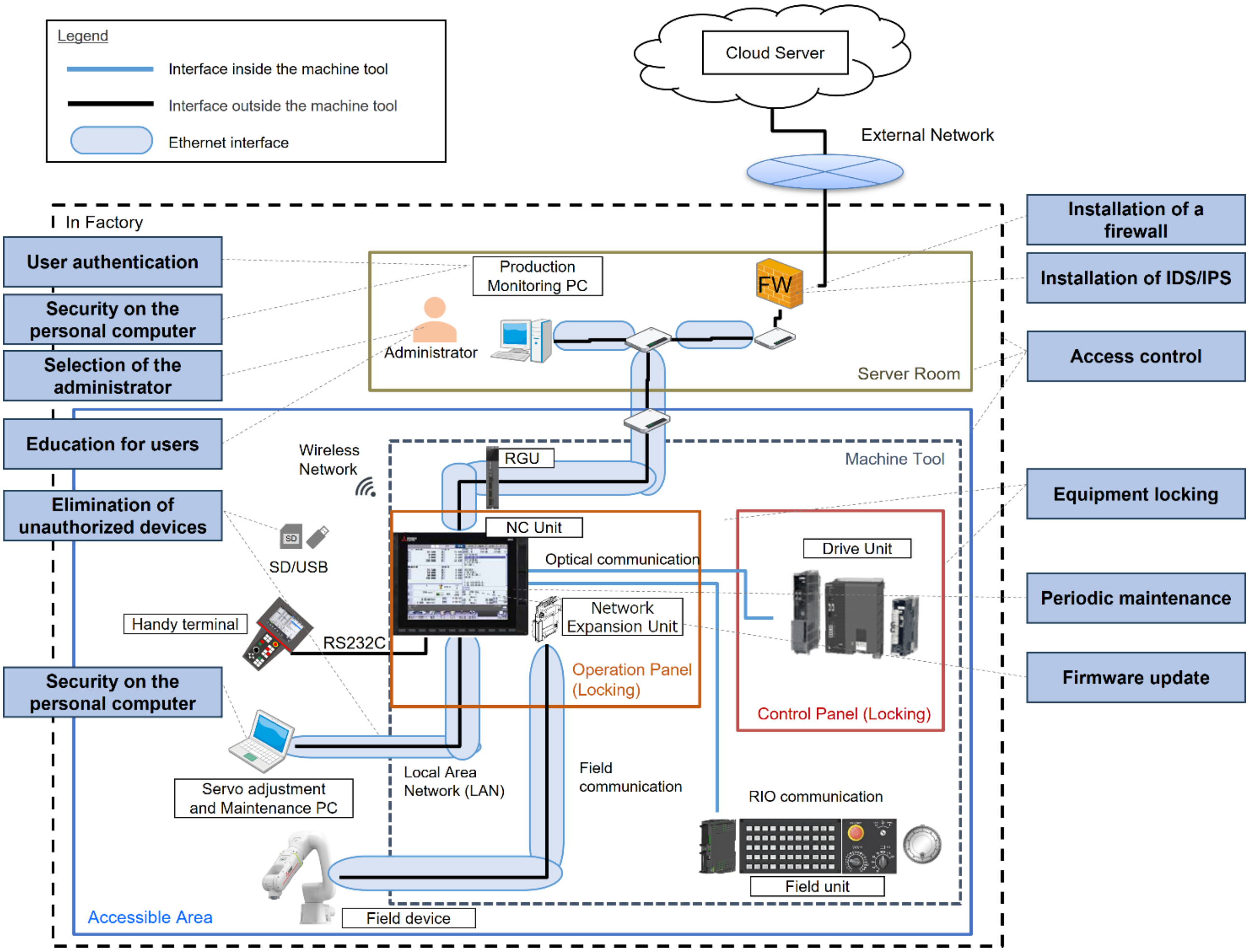


Figure 7 Security measures to be taken in the usage environment

Table 8 Description of the security measures in the usage environment

Layer of defense in depth	Measure name	Description	Corresponding threat
Human layer	User authentication	Set appropriate permissions for using personal computers and management apps. Manage the set passwords appropriately.	1. Illegal access by an unauthorized user
	Selection of the administrator	For the administrator, an appropriate person who will not abuse his/her authority shall be selected.	1. Illegal access by an unauthorized user
	Education for users	Users are educated so that they use the NC unit securely.	8. User misuse or misconfiguration
	Periodic maintenance	Regularly check security settings and vulnerabilities to prevent the NC unit from being operated in an unauthorized environment. For details on maintenance of NC unit functions, refer to 2.6.2.	4. Inadequate security policies 5. Inadequate system maintenance
	Firmware update	Update the system to a version that addresses the newly discovered vulnerabilities to deal with vulnerabilities. For how to update the NC unit firmware, refer to 3.1.	5. Inadequate system maintenance
Physical layer	Removal of unauthorized devices	If any suspicious USB data terminals or cables are connected, remove them to prevent communication eavesdropping and unauthorized access. Take measures, such as virus check, against malware on storage media to be connected with the NC unit.	2. Eavesdropping/manipulation of communication 3. Unauthorized access from wireless devices 7. Access by unauthorized devices 10. Malware infection from storage media
	Access control	Access control of the factory and server room to prevent entry by unauthorized individuals.	1. Illegal access by an unauthorized user 2. Eavesdropping/manipulation of communication 7. Access by unauthorized devices
	Equipment locking	Restrict physical accesses to the NC unit by using it in a locked equipment to prevent unauthorized individuals from touching it. Restrict physical accesses to unused LAN, SD card interface, and USB flash drive interface by locking them up to prevent them from being connected to unnecessary devices.	1. Illegal access by an unauthorized user 2. Eavesdropping/manipulation of communication 7. Access by unauthorized devices
Network layer	Installation of a firewall	Install a firewall to block unauthorized accesses from external networks, and obtain access logs from external networks.	1. Illegal access by an unauthorized user 2. Eavesdropping/manipulation of communication
	Installation of IDS/IPS	Install IDS/IPS to monitor unauthorized accesses from external networks, and obtain access logs from external networks.	1. Illegal access by an unauthorized user 2. Eavesdropping/manipulation of communication 7. Communication failure due to mass access
Device layer	Security on the personal computer	Take appropriate security measures such as installing anti-virus software on the personal computers that communicate with the NC unit.	1. Illegal access by an unauthorized user 2. Eavesdropping/manipulation of communication

2.3 Introduction of the NC unit

Table 9 shows the items to be set when using the NC system in order to use the NC unit securely.

For details of each function, refer to the "Specifications Manual (Function)" and the "Alarm/Parameter Manual".

For the NC unit installation procedure, refer to the section "Flow of Initial Setup" in the "Connection and Setup Manual".

Table 9 Setting for the security function

No.	Function name	Setting	Reference
1	IP filter setting	Identify the IP addresses of connected devices in order to only allow connection from specific IP addresses.	2.4.4
2	Operation history	Enable a collection of the diagnostic data on the diagnosis data collection setting screen.	2.4.6.1
3		Periodically output files and make backups since the oldest entries will be overwritten when the storage size is exceeded.	2.4.6
4		Set the correct time so that the time stamps are recorded correctly.	2.4.6
5	Data backup/restoration	Periodically output backup data and store it in a safe location.	2.4.7

2.3.1 Precautions

- There are two LAN interfaces for M800S/M80 Series and M800VS/M80V Series; however, no device must be connected to LAN2. Refer to "General Specifications" in "Connection and Setup Manual" for the LAN2 position.

2.4 How to set and use security functions and options

This section describes how to set and use the NC security functions. It also describes important security items and precautions regarding setting and using each function.

This section describes the following security functions.

- Protection settings screen (Section 2.4.1)
- Machine tool builder macro protection (Section 2.4.2)
- PLC program protection (Section 2.4.3)
- IP filter setting (Section 2.4.4)
- Wireless LAN (Section 2.4.5)
- Operation history (Section 2.4.6)
- Data backup/restoration (Section 2.4.7)
- Encrypted communication (Section 2.4.8)
- User data deletion (Section 2.4.9)

Table 10 shows the NC support status by model for the security functions described above. For details of each function, refer to the "Specifications Manual (Function)".

Table 10 Security Function Support Status by Model

Function name	M8V Series				M8 Series					
	800VW	800VS	M80V	M80VW	800W	800S	M80	M80W	E80	C80
Protection settings screen (Machine tool builder password)	○	○	○	○	○	○	○	○	○	○
Protection settings screen (Data protection by user's level)	△	△	○	○	△	△	○	○	○	△
Machine tool builder macro protection	○	○	○	○	○	○	○	○	○	○
PLC program protection	○	○	○	○	○	○	○	○	○	△ *1
IP filter setting	○	○	○	○	○	○	○	○	○	-
Wireless LAN*3	-	○	○*2	-	-	-	-	-	-	-
Operation history	○	○	○	○	○	○	○	○	○	○
Data backup/restoration	○	○	○	○	○	○	○	○	○	○
Encrypted communication	○	○	○	○	○	○	○	○	○	○
User data deletion	○	○	○	○	○	○	○	○	○	○

○: Standard function, △: Optional function, -: No function

*1 Depends on the MELSEC specifications.

*2 M80V TypeLA does not have the wireless LAN function.

*3 Includes the security function of wireless LAN.

2.4.1 Protection settings screen

This function restricts accesses to each data item held by the NC.

Users who want to access each data item need to be authenticated by setting and entering a password.

By restricting access with a password, you can prevent unauthorized operation of the device due to misuse or misconfiguration.

This function cannot be disabled or changed to a state in which the password is not set.

For details of this function, refer to the "Data Protection by User's Level" section in the "Specifications Manual (Function)".

2.4.1.1 Entering and canceling the password

By entering a password, you can change or output each access-restricted data.

Access-restricted protection data includes data such as machine parameters and setup parameters.

To return to the state where the password is not entered, restart the NC or select "0-3 opn level" in the "Protect Setting" on the maintenance (Mainte) screen.

2.4.1.2 Data protection by user's level

You can reduce the number of data changes due to operation mistakes by enabling the seven-level operation restrictions for operations on the maintenance screen. For details of this function, refer to the section "Protection Setting" in the "Connection and Setup Manual".

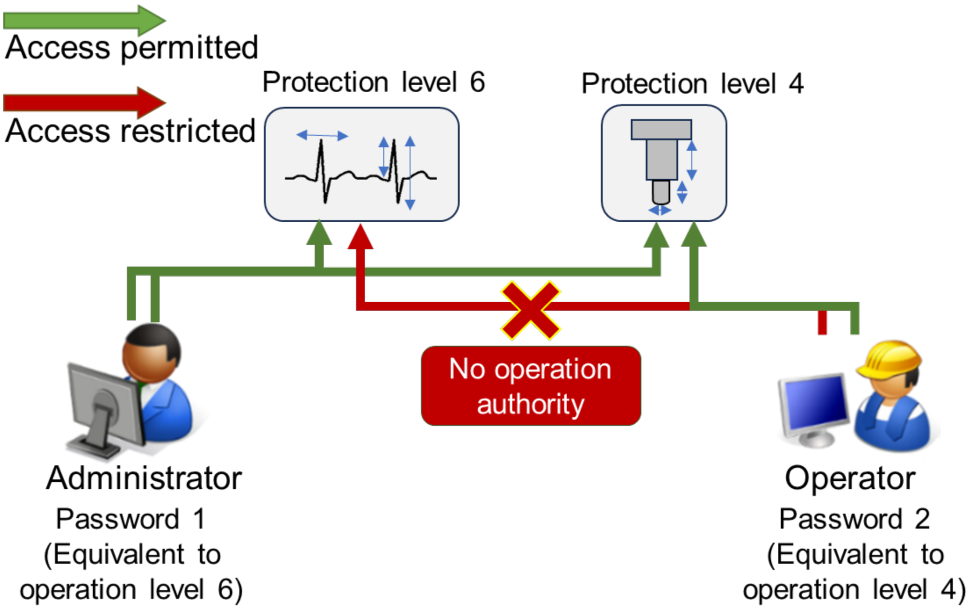


Figure 8 Data protection by user's level

Enabling this function allows you to only access data at operation levels equal to or higher than the protection level you have set. To change the operation level, you need to enter the password for each level. The protected data with settable access restrictions includes tool data, user parameter data, and machine parameter data, each for which access restrictions can be set individually for changes and output.

2.4.1.3 Secure setting method

Table 11 shows the items to be set in order to use this function.

Table 11 Settings for securely using the protection settings screen

Item	Setting	Description
[Base Common Parameters] #11018 (Machine user password held.)	0: Disable	When this parameter is enabled (set to "1"), the machine user (operation level 6) password is held even if the NC is restarted.

2.4.1.4 Precautions

The below describes precautions regarding using this function.

- After canceling the access restriction by entering a password, be sure to restart the NC to return to a state where no password is entered. If the device is operated with a password entered, it is not possible to prevent unauthorized individuals from accessing data or changing operation due to misuse or misconfiguration.
- The default password is set for operation levels 4 to 6. Change the password before use.
- If the data protection by user's level function is disabled, only the machine tool builder password (operation level 6) can be changed. To check if this function is disabled, refer to "Option" screen in the diagnosis screen and the setting of the base common parameter "#1391 User level protect".

2.4.2 Machine tool builder macro protection

The machine tool builder macro is a function that registers dedicated macro programs created by the machine tool builder to the NC.

By setting a password for a registered macro program, you can restrict the display, editing, and input/output of the program. This prevents unauthorized people from improperly viewing the program and also prevents programs and production know-how from being leaked.

If this function is disabled, the machine tool builder cannot register dedicated macro programs.

For details of this function, refer to the "Machine Tool Builder Macro" section in the "Specifications Manual (Function)".

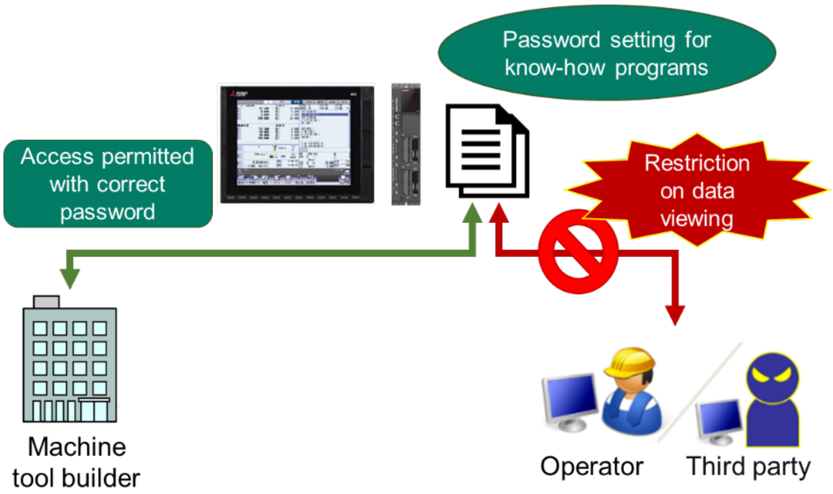

Password setting for know-how programs
Access permitted with correct password
Restriction on data viewing
Machine tool builder
Operator
Third party

Figure 9 Machine tool builder macro protection

2.4.2.1 Secure setting method

Table 12 shows the items to be set in order to use this function.

Table 12 Settings for securely using the machine tool builder macros

Item	Setting	Description
[Base Common Parameters] #1761 (cfgPR11) bit6	1: Machine tool builder macro PIN management method type 2	This parameter sets the machine tool builder macro PIN management method type. ➢ PIN management method type 1: Set the PIN using the numbers "2" to "99999999". ➢ PIN management method type 2: Set the PIN using one to eight alphanumeric characters. There are many character types available, so Type 2 is a more secure PIN management method. It is recommended that you use type 2.
[Base Common Parameters] #11796 (Machine tool builder macro password)	One to eight alphanumeric characters	Register a password to enable editing of machine tool builder macro programs. * This parameter can be set only when the PIN management method type 2 is selected.
R354,355	Numbers "2" to "99999999"	Register a password to enable editing of machine tool builder macro programs. * This R register must be set when the PIN management method type 1 is selected.

2.4.2.2 Precautions

The below describes precautions regarding registering machine tool builder macros.

- The protection release status set by the PIN remains effective until the power is turned OFF.
  - ➢ After entering the PIN, release the protection release status before operating the NC.

2.4.3 PLC program protection

To protect PLC data, you can set a password for each PLC data file.

By preventing unauthorized reading/writing to PLC data files, you can prevent device malfunctions and production stoppages due to writing unauthorized programs, and the leakage of programs and production know-how due to unauthorized reading.

If you do not set a file password, the PLC data can be viewed by the operator without being protected.

For details on this function, refer to the "File password" section in the "MELSEC Development Tool (GX Works2) Specifications Manual".

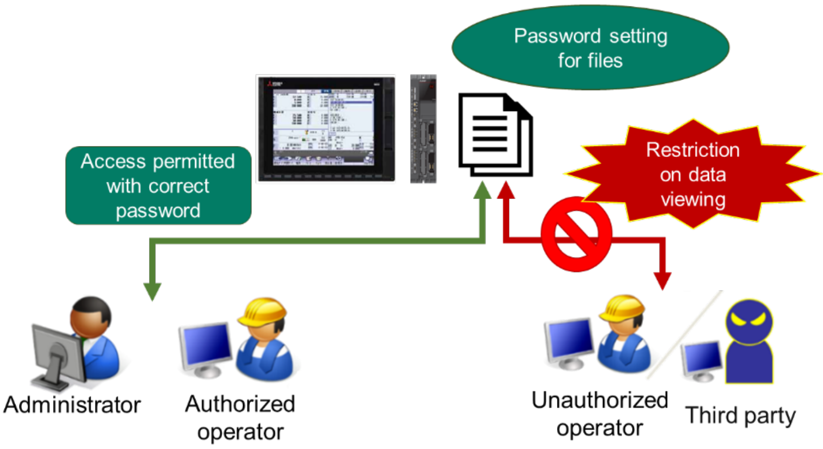

Password setting for files
Access permitted with correct password
Restriction on data viewing
Administrator
Authorized operator
Unauthorized operator
Third party

Figure 10 Program file protection

2.4.3.1 Secure setting method

Table 13 shows the items to be set in order to use this function.

Table 13 Settings for securely using the PLC program protection

Item	Setting	Description
GX Works2	[Online] → [Password/Keyword] → [Register/Change]	You can restrict viewing of PLC data files by setting a file password from GX Works2.

2.4.3.2 Precautions

The below describes precautions regarding using the file password.

- To register/change or cancel the file password, use GX Works2 or GX Developer.
- With the PLC on-board, you cannot register/change or cancel a file password, but can only temporarily cancel it. If the file password cancel status is disabled after the file password is temporarily canceled, the file returns to the file password protection status again.
  - ➢ The file password cancel status remains enabled until you perform the operation to return to the password no-entry status, restart the PLC on-board, or change the connected project.

2.4.4 IP filter setting

This function prevents unauthorized access from external devices by filtering the IP address of the access source when the NC is being connected to Ethernet. By setting IP addresses to be allowed or blocked, it is possible to restrict accesses from external devices to the NC, thereby preventing unauthorized program rewriting and leakage of internal data from unauthorized connected external devices.

If this function is disabled, there is a risk of unintended operation or internal data leakage due to connecting to an unauthorized device.

For details of this function, refer to the "IP Filter Setting" section in the "Specifications Manual (Function)".

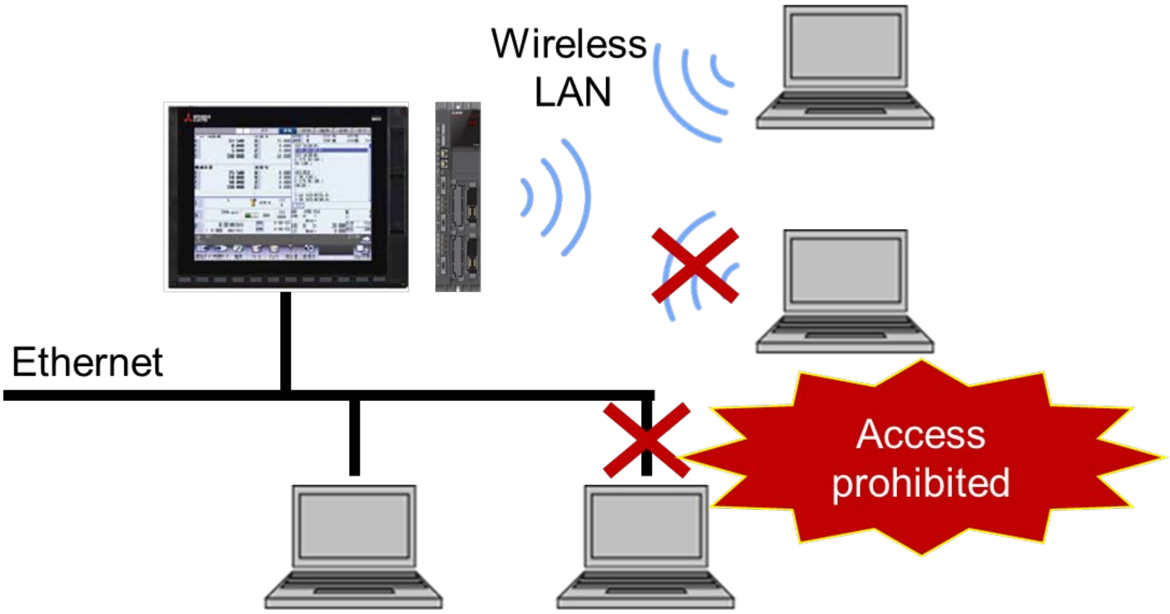


Figure 11 IP filter setting

2.4.4.1 Secure setting method

Table 14 shows the items to be set in order to use this function.

Table 14 Settings for securely using the IP filter setting

Item	Setting	Description
[User Parameters] #9810 (IP Filter for LAN1)	1: Allow	Set the processing for the specified range of IP addresses in the network connected to LAN1. Basically, we recommend that you set the IP addresses of only the external devices with which you want to permit a communication to be "Allow". 0: Disable IP filter setting 1: Allow 2: Block LAN2, LAN3, and WLAN provide parameters with the same setting.
[User Parameters] #9811 (StartFiltIP LAN1-1) #9812 (EndFilterIP LAN1-1)	0.0.0.0 to 255.255.255.255	Set the specified range of IP addresses in the network connected to LAN1. By setting the following parameters, you can specify up to eight IP address ranges. The IP addresses you set are allowed or blocked according to the parameter #9810. LAN2, LAN3, and WLAN provide parameters with the same setting.

2.4.4.2 Precautions

The below describes precautions regarding using the IP filter setting.

- When using the device in an environment where it is connected to a LAN line, use the IP filter setting function.
- If a proxy server exists on the LAN, block the IP address of the proxy server. If the IP address is allowed, access from a personal computer that has access to the proxy server cannot be prevented.
- There are two ways to restrict accesses. Basically, we recommend that you set the IP addresses of only the external devices with which you want to permit a communication to be "Allow".
  - Allow

    If you set a range of IP addresses of the access source to allow a communication, accesses from within that IP address range are permitted, and accesses from other IP addresses are prohibited.
  - Block

    If you set a range of IP addresses of the access source to prohibit a communication, accesses from within that IP address range are prohibited and accesses from other IP addresses are allowed.

2.4.5 Wireless LAN

This function enables the NC to exchange data with devices compliant with wireless LAN standards using wireless communication through the built-in wireless LAN card.

The NC unit can be operated in two modes for wireless LAN: access point (AP) mode, where it operates as an access point, and station (STA) mode, where it operates as a station. The access point (AP) mode enables a communication between the NC unit and wireless LAN devices even in an environment without a wireless LAN router. The station (STA) mode enables a communication between the NC unit and wireless LAN devices in an environment where the wireless LAN is already available.

When this function is enabled, LAN connection is possible freely within range of the radio waves. On the other hand, if a malicious attacker exploits vulnerabilities, the content of communications could be stolen or malformed packets could be inserted, for example.

For details of this function, refer to the "Wireless LAN Function" section in the "Instruction Manual".

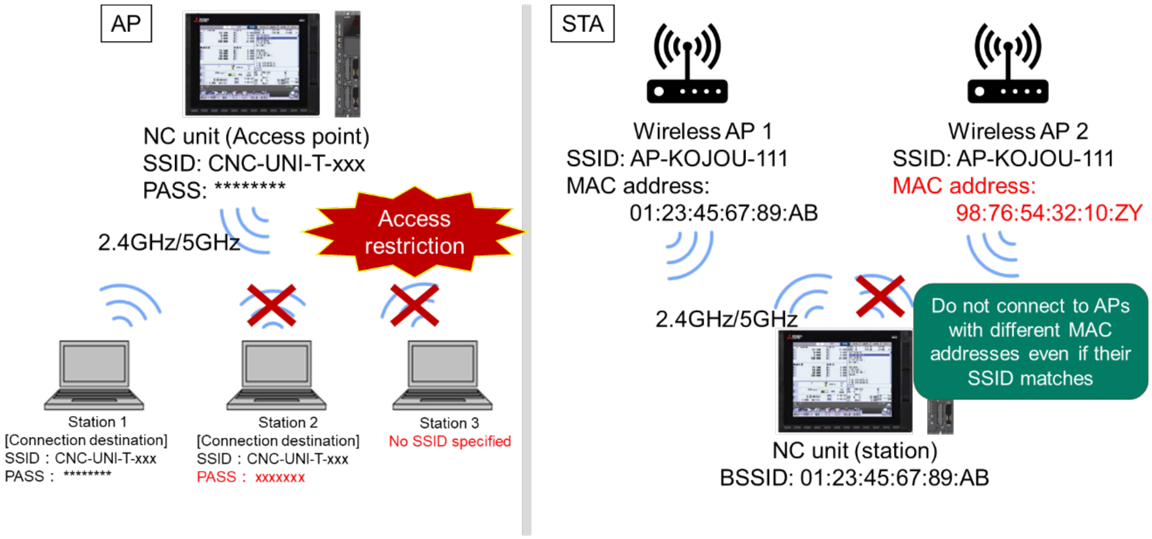


Figure 12 Wireless LAN

2.4.5.1 Enabling conditions

Table 15 shows the conditions to enable the wireless LAN function.

Table 15 Wireless LAN enabling conditions

Item	Setting	Description
[Wireless LAN Parameters] #75000 (WLAN STA/AP mode)	1 or 2	Specify the operation mode of wireless LAN. When this parameter is set to "1" or "2", the wireless LAN function is enabled. 0: No mode (Wireless LAN function invalid) 1: Station (STA) mode 2: Access point (AP) mode

2.4.5.2 Wireless LAN specifications

The below describes the wireless LAN specifications.

Table 16 Common specifications for access point (AP) and station (STA) modes

Item		Specifications
Communication standard	5 GHz	IEEE802.11a IEEE802.11n (HT40) 0
	2.4 GHz	IEEE802.11b IEEE802.11g IEEE802.11n (HT40) 0
Communication mode		Infrastructure mode
Security		WPA-PSK TKIP 0 WPA2-PSK AES
Other functions		IP filter setting

*1: Automatically switched to HT20 when a radio interference occurs.
*2: Works with IEEE802.11a/b/g when WPA-PSK TKIP is used.

Table 17 Access point (AP) mode specifications

Item		Specifications
Frequency range (Channels)	5 GHz	W52, W58
	2.4 GHz	1 to 13
Security		ANY connection rejection ESSID stealth AP isolation
Maximum number of simultaneously connected devices		5 devices
Other functions		DHCP server Channel selection function abg mode

Table 18 Station (STA) mode specifications

Item		Specifications
Frequency range (Channels)	5 GHz	W52, W53, W56, W58
	2.4 GHz	1 to 13
Other functions		DHCP client Roaming

2.4.5.3 Security functions

The below describes the security settings for the wireless LAN functions.

- ANY connection rejection
  - When the NC unit is used as an access point (AP), this function does not allow connections from stations with the SSID set to "ANY" or no setting. This function rejects accesses from stations with no SSID specified, preventing accesses from unauthorized devices that do not specify a connection target. This function is always enabled in access point (AP) mode.
- ESSID stealth
  - This function prevents unidentified stations from accessing the NC unit operating as an access point (AP). When the ESSID stealth function is disabled, the ESSID of the NC unit is made public to wireless devices within the range of the beacon emitted by the NC unit. When the ESSID stealth function is enabled, no beacon is emitted and the ESSID is not made public to surrounding wireless devices.
- AP isolation
  - This function prohibits communications between stations when the NC unit is used as an access point (AP). This function may also be referred to as the privacy separator function. When this function is enabled, communication between stations via the NC unit is not permitted, preventing unauthorized stations from accessing other stations.
- IP filter setting
  - This function identifies the IP address of the access source and restricts connections. (Refer to Section 2.4.4.)

2.4.5.4 Secure setting method

Table 19 shows the items to be set in order to use this function.

Table 19 Settings for securely using the wireless LAN function

Item	Setting	Description
[Wireless LAN Parameters] #75006 (Encryption mode)	1: WPA2-PSK AES	For access point (AP) mode only Specify the data encryption and authentication method for the wireless communications. 0: WPA-PSK TKIP 1: WPA2-PSK AES
[Wireless LAN Parameters] #75010 (ESSID stealth)	1: Enable	For access point (AP) mode only Specify whether to enable ESSID stealth. 0: Disable 1: Enable
[Wireless LAN Parameters] #75011 (AP isolation OFF)	0: Enable	For access point (AP) mode only Specify whether to disable AP isolation. 0: Enable 1: Disable
[Wireless LAN Parameters] #75100 (IP Filter for WLAN)	1: Allow	Set the processing for the specified range of IP addresses in the network connected to wireless LAN. Basically, we recommend that you set the IP addresses of only the external devices with which you want to permit a communication to be "Allow". 0: Disable IP filter setting 1: Allow 2: Block
[Wireless LAN Parameters] #75101 (StartFiltIP WLAN-1) #75102 (EndFiltIP WLAN-1)	0.0.0.0 to 255.255.255.255	Set the processing for the specified range of IP addresses in the network connected to WLAN. By setting the following parameters, you can specify up to eight IP address ranges. The IP addresses you set are allowed or blocked according to the parameter #75101.

2.4.5.5 Precautions

The below describes precautions regarding using the wireless LAN function.

- To enable the wireless LAN function, ensure the following:
  - For the security authentication mode in the wireless LAN settings, use WPA2-PSK AES. WPA-PSK TKIP has weak encryption strength, so network communications may be intercepted or accessed illegally by third parties. Do not use this function if security measures are required.
  - Restrict the IP addresses to allow access using the IP filter setting function.
- When using the NC in access point (AP) mode, ensure the following:
  - Enable the security settings (refer to Section 2.4.5.3).
- When using the NC in station (STA) mode, ensure the following in the wireless LAN router settings:
  - To prevent unauthorized access from the Internet, take measures such as disabling PING response to avoid being identified on the Internet.
- When using a device such as a PC or a tablet in the same network, ensure the following:
  - Keep the OS, software and anti-virus software updated to the latest version.
  - Be careful not to open attached files and hyperlinks from unreliable or unknown sources.
- The NC unit has a wired LAN function that uses an Ethernet cable, but the NC unit handles wireless communication and priority communication independently, so it cannot relay each other's communications.

2.4.6 Operation history

This function is useful for analyzing problems by tracing NC operation information and history.

The history data described below is recorded in chronological order as a data file, thereby enabling this information to be displayed on the screen or output to a file. The history data file allows you to check the date and time when a problem occurred as well as related details.

If this function is disabled, NC history data will not be recorded.

For details of this function, refer to the "Diagnosis Data Collection Setting" section in the "Maintenance Manual".

Table 20 Types of history data

History data	Description
Key history	Keystroke history information on the NC operation board [Entry time, display screen number, screen name, detailed screen number, key code, key name]
Touchscreen history	Touchscreen entry history information on the touchscreen display [Entry time, display screen number, screen name, detailed screen number, coordinates, status (press/release)]
Alarm/warning history	Alarm and warning history information when an alarm or warning occurs on the NC * Including PLC alarm messages [Alarm occurrence time, part system, alarm number, parameter 1, parameter 2]
PLC signal history	Change history information for input/output signals (X device, Y device) between the machine, PLC ladder, and NC [Change time, device name, status (1: OFF → ON, 0: ON → OFF)]
Tool offset change history	Tool change history information when the tool offset value is changed [Change time, type, offset number, change source, offset before change, offset after change]
Workpiece offset change history	Change history information when the workpiece offset value is changed [Change time, type, part system number, axis number, offset before change, offset after change]
AC input power history	History information when the NC power is turned ON/OFF [Occurrence time, NC power ON/OFF]
Detailed alarm information history	Detailed alarm history information when an alarm occurs on the NC * Warnings are not included. [Alarm information, modal information, coordinate information]
Parameter change history*1	Change history information when the value set in the parameter is changed * The PLC switch change history is not output. [Change date and time, change method, parameter number, part system number, axis name, parameter value before change, parameter value after change]
Common variable change history*1	Change history information when the common variable value is changed [Change date and time, change method, variable number, part system number, variable value before change, variable value after change]

*1: Displayed on the setting change history screen in the M8V A0 version, but is not output to the all history output file (ALLLOG.LOG).

In addition, models prior to the M8 do not support displaying on the history screen or outputting to a file.

2.4.6.1 Secure setting method

Table 21 shows the items to be set in order to use this function.

Table 21 Settings for securely using the operation history

Item	Setting	Description
[Mainte] → [Collect set] → Collecting data select	0: Collect	Collects the history data of the items set in the Collecting data select. 0: Collect 1: Does not collect In order to check for unauthorized operations, we recommend that you set this option to collect all history data.
[Mainte] → [Collect set] → [Start]	Status: History collecting	If the status of the history data is set to "History collecting" by pressing the [Start] menu, the history data is being collected. During "History collecting", data collection automatically starts when the NC is turned on, depending on the contents of "Collecting data select".

2.4.6.2 Precautions

The below describes precautions regarding using the operation history.

- If you stop the diagnosis data collection using the [Stop] or [Data Clear] menu on the diagnosis data collection setting screen (the status of the history data is "History stop"), data collection does not start even if the NC power is turned on again.
  In this case, press the [Start] menu on the diagnosis data collection setting screen.
- Pressing the [Data Clear] menu stops the collection of history data and clears the collected data.
- The history data that can be stored is limited. Since it is needed for investigation of causes when an incident occurs, output the history data periodically (1 time/month is recommended) and store it in a safe location.

2.4.7 Data backup/restoration

You can save and restore the status by backing up NC data to a DS, HD, SD memory card, or USB flash drive and restoring the backup data.

By storing the normal backup data, you can use it to restore to the normal status when an abnormality occurs and to identify the cause of the abnormality by comparing the status.

Backup can be performed manually, or you can set parameters to have backups run automatically on a specified date each month. The most recent three automatic backups are saved, and others are overwritten from older files.

For details of this function, refer to the "Data Backup and Restoration" section in the "Maintenance Manual".

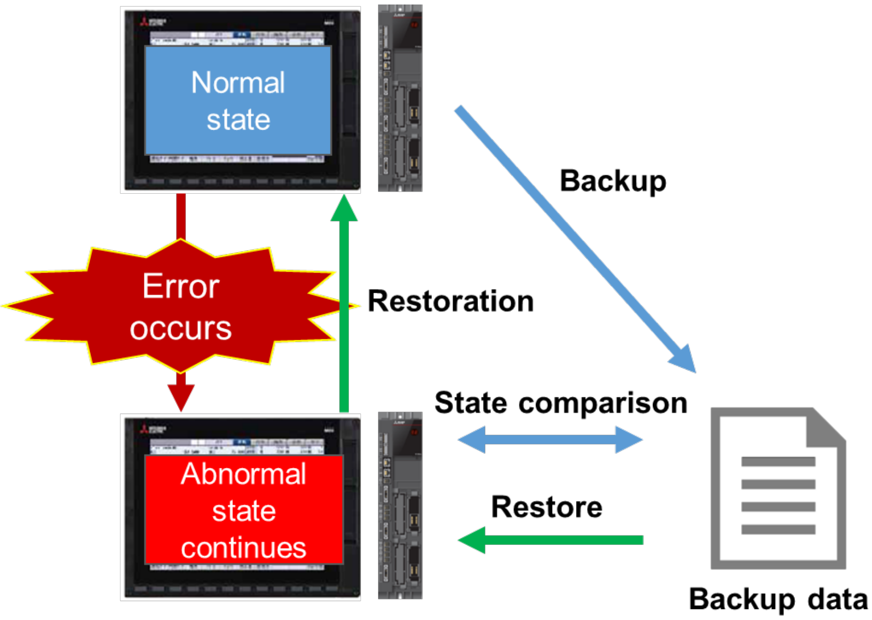


Figure 13 Data backup/restoration

2.4.7.1 Data to be backed up

Table 22 shows the data and their types that are output by bulk backup.

Table 22 Data output by backup

No.	Output data	Typical data type
1	System data	• SRAM data • Parameter • System configuration • Program batch file • Tool length data • Variable data • Machine tool builder macro file
2	Ladder	• User PLC program • EtherNet/IP configuration file
3	Safety parameters	• Safety parameters
4	Safety ladder 1	• Safety PLC program 1
5	Safety ladder 2	• Safety PLC program 2
6	APLC data	• C language module created by user
7	Custom data	• Custom screen data • Motion control release file
8	NCAID data	• NCAID data

2.4.7.2 Automatic backup settings

When setting the automatic backup, set the parameters shown in Table 23 to specify the schedule for performing the automatic backup.

Table 23 Parameters to be set by automatic backup

Item	Setting	Description
[Operation Parameters] #8915 (Auto backup day 1)	-1 to 31 (Select the appropriate one according to your automatic backup settings.)	The automatic backup is executed when the NC power is turned ON for the first time after the designated date of the month. When "-1" is set in this parameter, the automatic backup is executed every time the CNC power is turned ON. (Maximum once a day) ■ Setting range -1: Everyday 0: Disable 1 to 31: Designated date
[Operation Parameters] #8916 to #8918 (Auto backup day 2 to 4)	0 to 31 (Select the appropriate one according to your automatic backup settings.)	The automatic backup is executed when the CNC power is turned ON for the first time after the designated date of the month. ■ Setting range 0: Disable 1 to 31: Designated date
[Operation Parameters] #8919 (Auto backup device)	0 to 3 (Select the appropriate one according to your automatic backup environment.)	Set the device for automatic backup. When setting the automatic backup, select the automatic backup target to suit your environment. ■ M800VW/M80VW terminal with PC 0: DS 1: HD 2: Memory card 3: USB flash drive ■ M800VS/M80V 0: DS 2: Memory card 3: USB flash drive

2.4.7.3 Precautions

The below describes precautions regarding using the data backup/restoration function.

- Output the backup data periodically and store it in a safe location.
- The user data included in the output backup data is not encrypted. When saving user data to storage media such as external storage device, encrypt data for protection as necessary.

2.4.8 Encrypted communication

Encrypted communication is a function that encrypts communication data when the NC device communicates with the cloud server.

Note that a communication with the NC device through any one other than this function is generally not encrypted, as there is a prerequisite that it is carried out within the access-controlled factory.

This function cannot be disabled.

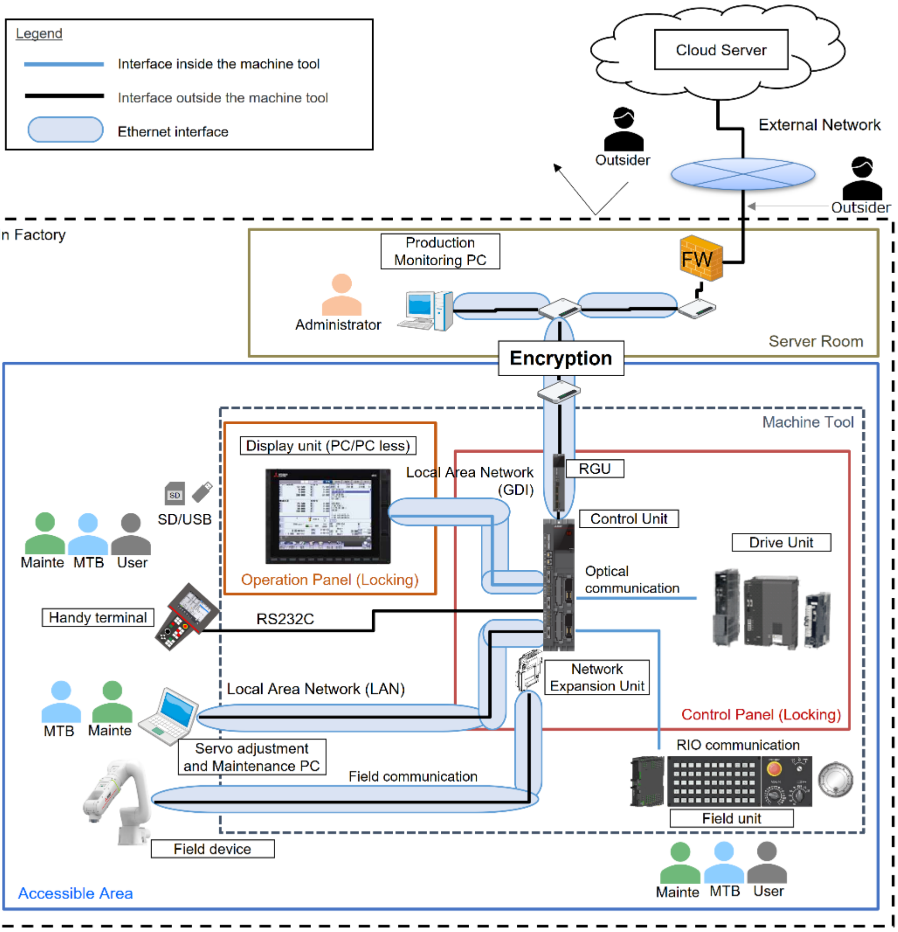


Figure 14 Encrypted communication function

2.4.8.1 Communication function to be encrypted

Table 24 shows the communication functions to be encrypted by this function.

Table 24 Communication function to be encrypted

No.	Communication function
1	Remote service function
2	VNC server*

* This data is only encrypted when the password is sent for connection, so other communication data is not encrypted.

2.4.8.2 Precautions

The below describes precautions regarding using the encrypted communication function.

- This function is only effective for the functions shown in Table 24.
- The encrypted communication function prevents data from being read if it is intercepted. To prevent data interception itself and intrusion from external networks, install a firewall or router to prevent a direct connection between the external network and the factory network.

2.4.9 User data deletion

This function deletes user data.
You can delete data when disposing of the device, preventing an information leakage.

Figure 15 User data deletion

User data is stored in multiple areas, so there are also multiple related deletion functions.
Referring to Table 25 that lists each data area to be deleted, use the function that corresponds to the user data you want to delete.

Table 25 User data deletion types

User data deletion function	Description
SRAM Clear*1	Initializes the entire SRAM. * This function cannot delete data and PLC programs in NC memory 2.
Memory format*2	Deletes machining programs in NC memory/NC memory 2. * This function must be used to delete machining programs in NC memory 2.
PLC program deletion*3	Deletes PLC programs registered in NC. * This function must be used to delete ladders.
Email address deletion (Email notification to operator function)	Deletes email addresses, their user IDs, and passwords registered in NC. For details on how to delete data, refer to Section 2.5.1.2. * This function must be used to delete email addresses, their user IDs, and passwords.

*1: Execute the function, referring to the section "Initializing the NC Internal Data (SRAM)" in the "Connection and Setup Manual".

*2: Execute format by the menu [Format] in the maintenance (Mainte) screen, referring to the section "Setting the Parameters for the System Specifications" in the "Connection and Setup Manual".

*3: Format the PC memory to delete the PLC program, referring to "PLC Development Manual".

2.4.9.1 Precautions

The below describes precautions regarding using the user data deletion function.

- If SRAM Clear is executed, the parameters set by the machine tool builder are also deleted. After SRAM Clear is executed, the machine operation is not possible, so be careful not to run this function unless you are disposing of the machine.

2.5 Functions that affect the security risk of the NC unit

This section describes how to use and set the NC functions that affect security risks. It also describes important security items and precautions regarding setting and using each function.

This section describes the following functions.

- Email notification to operator (Section 2.5.1)
- Remote connection function (Section 2.5.2)
- Server connection function (Section 2.5.3)

Table 26 shows the NC support status by model for the functions described above. For details of each function, refer to the "Specifications Manual (Function)".

Table 26 List of functions that affect security risks by model

Function name	M8V Series				M8 Series					
	800VW	800VS	M80V	M80VW	800W	800S	M80	M80W	E80	C80
Email notification to operator	△	△	○	○	△	△	○	○	○	-
VNC server	-	△	○	-	-	-	-	-	-	-
Web Access	-	○*1	○*1	-	-	-	-	-	-	-
NC Monitor2	○	○	○	○	○	○	○	○	○	○
NC Explorer	○	○	○	○	○	○	○	○	○	○
Custom API library	○	○	○	○	○	○	○	○	○	-
EZSocket	○	○	○	○	○	○	○	○	○	-
Numerical Control (CNC) Communication Software FCSB1224W000	○	○	○	○	○	○	○	○	○	-
GX Works2	○	○	○	○	○	○	○	○	○	-
Ethernet input/output	○	○	○	○	○	○	○	○	○	○
MES interface library function	△	△	○	○	△	△	○	○	○	-
Remote service function (Connection with no RGU)	△	△	○	○	-	-	-	-	-	-

○: Standard function, △: Optional function, -: No function

*1 Available from the B2 version.

2.5.1 Email notification to operator

The Email notification to operator function can send emails from the NC.

Emails sent from the NC can be received by an external terminal via the email server (SMTP server). With this function, the NC can send emails to PCs and mobile terminals away from machines. You will be able to know machining conditions (such as machining completion, stop and failure) even if you are in remote places.

If this function is enabled, NC information is sent externally. Also, you need to register the sender and recipient email addresses to use this function.

For details of this function, refer to the "Email Notification Function to Operator" section in the "Instruction Manual".

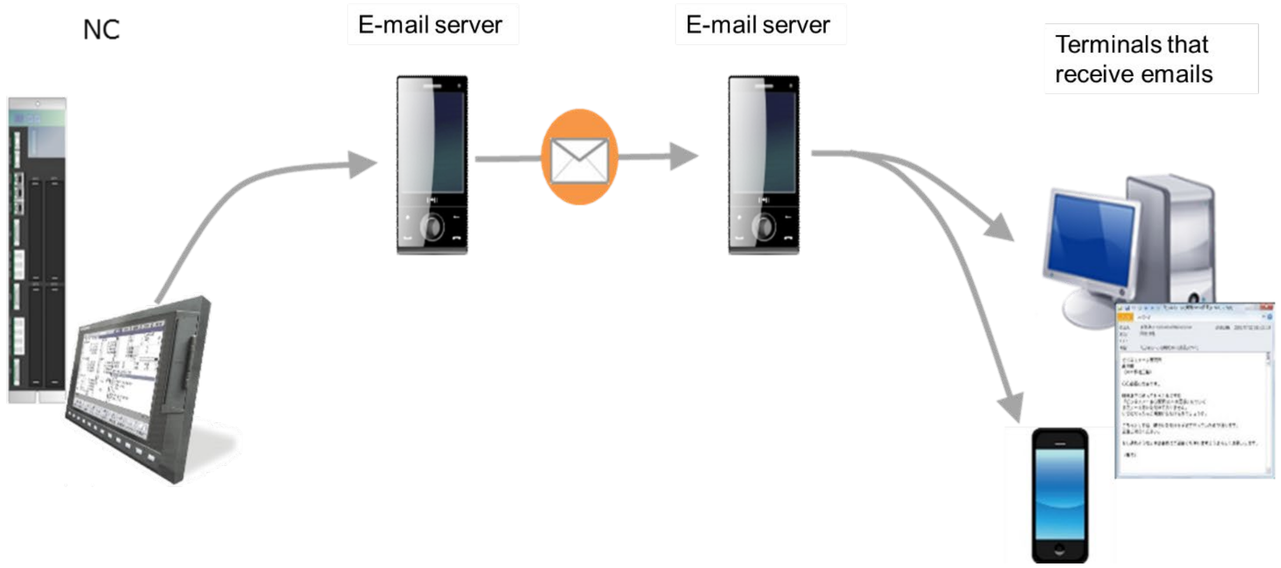


Figure 16 Email notification to operator

2.5.1.1 Disabling conditions

If the Email notification to operator function is specified, it is disabled under the conditions shown in Table 27 below.

Table 27 Conditions for disabling "Email notification to operator"

Item	Setting	Description
[Control parameter 1] #8134 (Email send disable)	1: Disable	Email sending by the email notification to operator can be disabled. 0: Enable 1: Disable
[Setup screen] Email notification to operator setting	If any of the items are not set, email sending is disabled.	If any of the items are not set on the Email notification to operator setting screen, email sending is disabled. ● Email transmission environment setting ● Email address setting for transmission ● Email transmission condition setting

2.5.1.2 Email address deletion

To delete the email address and its user ID and password registered to the NC unit, you need to enter "0" in each field on the Email notification to operator settings screen.

Table 28 Email address deletion method

Item	Setting	Description
[Setup screen] Email notification to operator setting	Enter "0" in each item to clear data.	Enter "0" in each field on the Email notification to operator settings screen; the data for that field is deleted. To delete user data, enter "0" in any of the fields below that have already been set. [Email address setting for transmission] ● From ● To ● CC [Email transmission environment setting] ● User ID ● Password

2.5.1.3 Precautions

The below describes precautions regarding using the Email notification to operator function.

- The communication data for this function is not encrypted. Install the email server that communicates with the NC on the factory network, and take measures to prevent eavesdropping and manipulation of communications.

2.5.2 Remote connection function

The remote connection function allows you to operate the NC from an external terminal by connecting to it.

Table 29 shows the functions that allow a remote connection.

To use these remote connection functions, disable the functions that you do not plan to use.

For details of each function, refer to the "Specifications Manual (Function)", or each Specifications Manual.

Table 29 Remote connection function

Function name	Description
VNC server	You can operate the NC from an external terminal by starting the VNC client on the external terminal and entering the specified-NC's IP address and the VNC password. Also, you can operate an external terminal that supports the VNC server from the NC screen by enabling the remote desktop connection function.
Web Access	This function displays the screen of the NC connected to the factory LAN in a web browser. When user authentication is performed on the web browser, the NC screen is displayed and the NC can be operated from the web browser. If this setting is made in the NC side, you can enable input restrictions on the [INPUT] key and operation restrictions other than the screen display function.
NC Monitor2	This function monitors the NC connected to the factory LAN. You can operate the NC by selecting the NC to be monitored from an external terminal on which the tool is installed. If this setting is made in the NC side, you can enable input restrictions on the [INPUT] key and operation restrictions other than the screen display function.
NC Explorer	This is a tool that allows you to operate the NC machining data file from the Explorer on the host PC for each NC connected to the host PC via Ethernet. If this setting is made in the NC side, you can restrict operations other than the screen display function or reject a connection from a tool.
Custom API library	This is an interface library between the NC and applications developed by the user. It allows you to perform operations such as setting and referencing data for the NC.
EZSocket I/F	This is a middleware product that makes it easy to develop applications that have a Windows interface. Various NC functions can be used from a Windows application using VC++ language, VB language, and VBA macro language.
Numerical Control (CNC) Communication Software FCSB1224W000	This is a software product that makes it easy to develop applications that have a Windows interface. To develop applications using this product, you can improve the development efficiency by using the same OLE interface without knowing the internal processing of the NC.
GX Works2	This is a PLC development tool for the Mitsubishi Electric PLC MELSEC Series. This tool can be used to develop ladders for the NC controller and also to write/read parameters and PLC programs from an external terminal, stop/run the PLC, and monitor a PLC program.

2.5.2.1 Disabling conditions

Table 30 shows the conditions to disable the wireless LAN function.

To enable this function, you may need to install and configure a client on the external device in addition to the settings below. For details, refer to the instruction manual for each function.

Table 30 Conditions for disabling the remote connection function

Function	Item	Setting	Description
VNC server	[Operation Parameters] #19701 Restrain VNCserver	0	Select whether to restrain the VNC client from connecting to the NC, displaying the NC screen or performing setting to the NC. Menu selection may be disabled depending on the set value. 0: Disables the VNC server function. 1: Enables the VNC server function, which allows the VNC client to display the NC screen and to perform the setting operation. 2: Enables the VNC server function, which allows the VNC client to display the NC screen, but restricts the setting operations for the INPUT key only.
Web Access	[Base Common Parameters] #1766 (cfgPR16/bit7)	0	Select whether to enable or disable the Web access (NC screen remote browsing) function. 0: Disable (default) 1: Enable
	[Operation Parameters] #19730 (WebAccess)	0	Specify whether to enable or disable Web access (NC screen remote browsing) function. Also set restrictions on screen operations when the function is enabled. 0: Disables the function. 1: Enables the function. Touch, click and key input are possible. 2: Enables the function. Touch, click and key input are possible. Input via [INPUT] key is not possible. 3: Enables the function. Touch, click and key input are not possible. Only the NC screen can be displayed.
NC Monitor2 NC Explorer	[Operation Parameters] #8931 (Display/Set limit)	2	Select the restriction of the connected NC's screen display/settings on/from the remote control tool (NC Monitor2, NC Explorer). 0: Permit the screen display/settings. 1: Permit the screen display only. 2: Restrict the connection.
GX Works2	[Base Common Parameters] #11094 (GX Restriction)	1	Blocks the connection from GX Developer or GX Works2. 0: Allow the connection 1: Block the connection

2.5.2.2 Precautions

The below describes precautions regarding using the remote connection function.

- You cannot disable the custom API library, EZSocket I/F, and numerical control (CNC) communication software FCSB1224W000. Enable the security function such as the IP filter setting (2.4.4) to deny accesses from unauthorized devices.

2.5.3 Server connection function

The server connection function allows you to send and receive data by connecting the NC to the server.

Table 31 shows the functions that allow a server connection.

To use these server connection functions, disable the functions that you do not plan to use.

Table 31 Server connection functions

Function name	Description
Ethernet input/output	NC data can be input and output between the NC and the host computer connected via Ethernet.
MES interface library function	This function enables to link the NC internal data and the database of information system (manufacturing execution system). Production control and traceability can be ensured with the registered information by registering at machining completion, alarm occurrence, or the user's arbitrary timing as needed. The data registered in the database can also be operated with CNC.
Remote service function	This function is a remote service to support remote maintenance of machine tools. Operation monitoring of machine tools and remote diagnostics of CNC are available.

2.5.3.1 Disabling conditions

Table 32 shows the conditions to disable the server connection function.

For details, refer to the Specifications Manual for each function.

Table 32 Conditions for disabling the server connection function

Function	Item	Setting	Description
Ethernet input/output	[Ethernet Parameters] #9711 Host1 host name #9731 Host2 host name #9751 Host3 host name #9771 Host4 host name	0	Set the host computer name. 0: Disables the Ethernet input/output function. Up to 15 alphanumeric characters: Connects to the specified host computer.
MES interface library function	[Base Common Parameters] #1475 (MES-IF_on)	0	Set whether to enable the MES interface function. 0: Disable (default) 1: Enable
Remote service function (Connection with no RGU)	[Control Parameters] #8170 (Remote Service)	0	Select whether to enable the Remote service function. 0: Disable (default) 1: Enable

2.6 Operation and maintenance of the NC unit

2.6.1 NC unit operation example

As physical security measures on the NC unit, restrict access to certain areas in the factory and install the NC unit in a secure location where it can be monitored (e.g., inside equipment or locked cabinet) to protect it from access by an unauthorized individual and physical destruction. In particular, separate rooms that house equipment that manages the network or equipment that is important for the continuous operation of the control system from other areas, and implement entry and exit management so that only authorized personnel can enter and exit these rooms.

The NC unit communicates with a personal computer (maintenance personal computer or production management personal computer) via a network. The files stored in the NC unit can be operated by installing the engineering software on a personal computer. To prevent these personal computers from being compromised, which causes files stored in the NC unit to be leaked, or files causing unintended behavior to be written to the product, take the following security measures on personal computers that are connected to the NC unit.

- Personal computer theft prevention measures using wire locks and others
- Access control for personal computer users
  - Allowing only authorized individuals to log in to the personal computer
  - Strict management of login information
  - Introduction of fingerprint authentication
- Introduction of anti-virus software

The files (customer's resources) stored in the SD memory card or USB flash drive may be leaked if it is stolen. In addition, a malicious third party may insert a storage medium containing unauthorized files, which may affect the control of the customer's equipment. Therefore, implement the following security measures for storage media managed within the factory.

- Anti-theft measures such as placing storage media in locked shelves
- Restrictions on storage media users
  - Formulation of rules for taking storage media out
  - Restrictions on personal computers that can write to storage media
- Restrictions on physical access to the LAN, SD card I/F, and USB flash drive I/F by keys and access control

To protect the factory where the NC unit is installed and the network where a personal computer is installed from unnecessary accesses from outside, install network devices such as firewalls and routers at the boundary between the Internet and the factory network and in the server room.

As a part of the continuous security operation in the factory where the NC unit is installed, plan to carry out the check items for each element shown in Table 33.

Table 33 Check items for performing continuous security operations

No.	Element	Check item
1	Backup	Periodically back up the user programs, parameters, or device values in preparation for a product failure.
2	Operation history check	To detect suspicious behavior, an effective method is to check the logs obtained by the operation history function. For example, you can check for possible unauthorized access by checking parameter changes and AC input power history. Also, to record the correct date and time, periodically check that the date and time on the NC unit are correct. Refer to the section "Cumulative Time" in the "Instruction Manual" to confirm and set the date and time.
3	Password	Periodically change the password you set. Unauthorized access can be prevented by updating the password periodically and using a character string that is difficult to guess.

When using the NC unit, select an appropriate person as the administrator. Also, provide sufficient education and training to the NC unit users on how to properly set up, manage, and operate the product. Use the NC unit appropriately in accordance with the operation manual and this guideline.

2.6.2 Periodic maintenance

To keep the system secure, perform regular security maintenance (at least once a year is recommended, and for the history function, once a month is recommended). Specifically, check that the functions shown in Table 34 are working properly. Also, Table 35 shows functions of which settings may affect security. Periodically check the settings as well.

Table 34 Operation verification items for the security function

No.	Function name	Check item
1	Protection settings screen	A password shall be required to enter the data to be protected (e.g. machine parameter data).
2	IP filter setting	When "Block" is selected in the IP filter setting, communications from the set IP address shall be blocked, but communications from other IP addresses shall not be blocked.
		When "Allow" is selected in the IP filter setting, communications from the set IP address shall not be blocked, but communications from other IP addresses shall be blocked.
3	Operation history	The enabled operation history items shall be saved.
		The date and time of the saved operation history shall be correct.
4	Data backup/restoration	When a backup is executed, the backup process shall be successful and a backup file shall be generated in the destination folder.
		When you select the backup file and perform restoration, the system shall return to the state it was in at the time it was backed up.

Table 35 Setting check item for the security function

No.	Function name	Check item
1	Protection settings screen	Check that the configured protection level settings remain unchanged.
2	IP filter setting	Check the IP addresses that are allowed to communicate with the product. If access from an unintended IP address is allowed, make sure that access from the target IP address is blocked.
3	"Functions that affect security risks" in general	Check that no unintended "functions that affect security risks" are enabled.
4	Wireless LAN	Check that the settings displayed on the Wireless LAN diagnosis screen are as intended. When the AP mode is used, check the number of connected devices displayed on the wireless LAN diagnosis screen. If extra devices are connected, set the encryption key again.
5	Operation history	Also, periodically check that the date and time on the NC unit are correct. Refer to the section "Integrated Time" in the "Instruction Manual" to confirm and set the date and time.

2.7 Removal and disposal of the NC unit

Incorrect disposal or transfer may result in leakage of data remaining in the product. To prevent data leaks, be sure to note the following points to remove and dispose of the product when ending use of the product.

- Use the user data deletion function to delete the asset data (machining programs, etc.) in the NC unit to be discarded. For details about the user data deletion function, refer to Section 2.4.9.
- Contact the machine tool builder, etc., and discard the machine tool.

If the data needs to be backed up before it is erased, use the backup function to make a backup.

Please note that backup data output from this product to an SD memory card or computer is not erased. When disposing of or transferring the product, be sure to remove the installed SD memory card or USB flash drive, and perform the appropriate management. For general precautions for disposal, refer to the section "Precautions for Safety" of the "Maintenance Manual".

When removing a device connected to an NC unit in the system, the device may still contain data that should be protected. Please remove it after taking measures such as deleting the data so that the information cannot be retrieved.

3 Contact information for security issues

Mitsubishi Electric collects information on product vulnerabilities from external security researchers and coordinating bodies (such as domestic and foreign CERT) to improve the information security of our products. For information regarding product vulnerabilities, please contact such coordinating bodies or contact Mitsubishi Electric through the contact form on the following website.

➢ Mitsubishi Electric PSIRT
https://www.mitsubishielectric.com/psirt/contact/

3.1 Disclosure of vulnerability information

We will notify you of any newly discovered vulnerabilities and the necessary measures for our products on the following website.
Please check the contents regularly and take appropriate measures for the relevant products.

➢ Vulnerability information
https://www.mitsubishielectric.com/psirt/vulnerability/index.html

➢ FA product vulnerability support status
https://www.mitsubishielectric.com/fa/about-us/security/vulnerability/

If it is necessary to update the NC firmware, please contact the machine tool builder or distributor from whom you purchased the product.
If the product manufacturer is not known, please contact a Mitsubishi Electric branch or distributor.
To contact the service center, refer to the end of the "Maintenance Manual".