TECHNICAL BULLETIN ***[1 / 17]***

[Issue No.] GOT-A-0077-E

[Title] Guidelines on Compliance with FDA 21 CFR Part 11 for the GOT2000 and GOT1000 Series

[Date of Issue] November 2014 (Ver. E: September 2019)

[Relevant Models] GOT2000 Series (GT27 Model, GT25 Model), GT SoftGOT2000,
GOT1000 Series (GT16 Model), MELIPC Series MI3000

Thank you for your continued support of Mitsubishi Electric Graphic Operation Terminal (GOT).
The GOT complies with FDA 21 CFR Part 11 by a method shown in this document. However, some restrictions exist.
To use the GOT in accordance with the FDA 21 CFR Part 11, the users are required to construct an appropriate system and operate it properly. This document is issued as the instruction for constructing a system containing the GOT compliant with the FDA 21 CFR Part 11.
In this document, "GOT" indicates the GOT2000 series (GT27 model, GT25 model), GT SoftGOT2000, and GOT1000 series (GT16 model).
The small differences in specifications are defined in the descriptions of the GOT2000 series, GT SoftGOT2000, and GOT1000 series.
GT SoftGOT2000 is pre-installed in the MELIPC series MI3000.
Therefore, for the compliance of MI3000 with the FDA 21 CFR Part 11, refer to GT SoftGOT2000.

Contents

1. OVERVIEW

The FDA 21 CFR Part 11 is a regulation issued by the Food and Drug Administration (FDA) in 1990s. This regulation defines how to configure a paperless record system that complies with the Current Good Manufacturing Practice (CGMP) regulations.
Electronic record is more easily falsified than records on paper. This regulation provides criteria to judge that electronic record and an electronic signature are equivalent to records on paper and hand-writing signature.
The users must construct a system based on the points in Chapter 2 and later for the compliance with the FDA 21 CFR Part 11.

The following describes whether the compliance with each article of the FDA 21 CFR Part 11 is available.

1.1 Compliance of GOTs with each article of the FDA 21 CFR Part 11

■§11.10 Controls for closed systems.
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
The users need to construct a system.
➟ 3. FDA 21 CFR Part 11 USING GOT

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
The compliance with this article is possible with GOT functions.
➟ 3.4 Security and Viewing of Data

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
The users need to construct a system.
➟ 3.3 Completeness of Data

(d) Limiting system access to authorized individuals.
The compliance with this article is possible with GOT functions.
➟ 3.1 Managing Users Who Access the GOT

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
The compliance with this article is possible with GOT functions.
➟ 3.5 Audit Trail

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
The compliance with this article is possible with GOT functions.
➟ 3.7 System Development, Operation, and Management

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
The compliance with this article is possible with GOT functions.
➟ 3.1 Managing Users Who Access the GOT

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
The compliance with this article is possible with GOT functions.
➟ 3.6 Validation of Data and Operations

(i) Determinations that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
The users need to take some measures.
➟ 3.7 System Development, Operation, and Management

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
The users need to construct a system and take some measures.
➟ 3.7 System Development, Operation, and Management

(k) Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
The users need to take some measures.
➟ 3.7 System Development, Operation, and Management

■§11.30 Controls for open systems.
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.
The users need to take some measures.
➟ 3.7 System Development, Operation, and Management

■§11.50 Signature manifestations.
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
The compliance with this article is possible with GOT functions.
➟ 3.5 Audit Trail

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).
The compliance with this article is possible with GOT functions.
➟ 3.5 Audit Trail

■§11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

The users need to take some measures.

➟ 3.7 System Development, Operation, and Management

■§11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

The compliance with this article is possible with GOT functions.

➟ 3.1 Managing Users Who Access the GOT

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

The compliance with this article is possible with GOT functions.

➟ 3.1 Managing Users Who Access the GOT

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

The users need to construct a system and take some measures.

➟ 3.7 System Development, Operation, and Management

■§11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

The compliance with this article is possible with GOT functions.

➟ 3.1 Managing Users Who Access the GOT

(2) Be used only by their genuine owners; and

The compliance with this article is possible with GOT functions.

➟ 3.1 Managing Users Who Access the GOT

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

The users need to take some measures.

➟ 3.7 System Development, Operation, and Management

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The compliance with this article is impossible with GOTs.

■§11.300 Controls for identification codes/passwords.
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
The compliance with this article is possible with GOT functions.
➟ 3.1 Managing Users Who Access the GOT

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
The compliance with this article is possible with GOT functions.
➟ 3.1 Managing Users Who Access the GOT

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
The compliance with this article is possible with GOT functions and some measures taken by users.
➟ 3.1 Managing Users Who Access the GOT
3.7 System Development, Operation, and Management

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
The compliance with this article is possible with GOT functions.
➟ 3.7 System Development, Operation, and Management

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
The users need to take some measures.
➟ 3.7 System Development, Operation, and Management

2. LIST OF GOT FUNCTIONS RELATED TO FDA 21 CFR Part 11

The following shows the GOT functions related to the FDA 21 CFR Part 11 and compliance of the GOT series. To have the system using the GOT comply with the FDA 21 CFR Part 11, the users must construct a proper system and operate it in addition to using the following functions.

Chapter describing details	Compliance with FDA 21 CFR Part 11 by using the GOT	GOT function name	Compliance			Remarks
			GOT 2000	SoftGOT 2000	GOT 1000	
3.1	Managing users who access the GOT	Operator authentication	◯	○	○	
		Security level	○	○	○	
3.2	Managing drawing data	User management	○	○	○	
		Access authority	○	○	○	
3.3	Completeness of data	Network drive	○	○ *1	×	
		FTP client	○	×	○	
		FTP server	○	×	○	
3.4	Security and viewing of data	Operation log	○	○	○	Obfuscated because it is binary data.
		Alarm	○	○	○ *2	
		Logging	○	○	○	
		Recipe	○	○	○ *3	
3.5	Audit Trail	Operation log	○	○	○	
3.6	Validation of data and operations	Verification *4	○	○	○	
3.7	System development, operation, and management	Security level	○	○	○	

*1 Use GT SoftGOT2000 by assigning the network drive to the virtual drive.
*2 Only the advanced alarm complies.
*3 Only the advanced recipe complies.
*4 The function of GT Designer3.

3. COMPLIANCE WITH FDA 21 CFR Part 11 BY USING THE GOT

The following shows the GOT functions related to the FDA 21 CFR Part 11 and setting methods.
To have the system using the GOT comply with the FDA 21 CFR Part 11, the users must construct a proper system and operate it in addition to using the following functions.

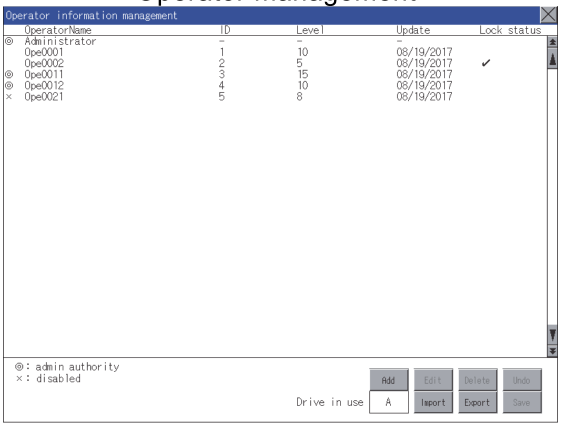
3.1 Managing Users Who Access the GOT

3.1.1 Operator authentication

Using the operator authentication function allows management on users who can log in to the GOT.
The users must have the uniqueness.
Before a user is registered, the individual must be identified.
At user registration, set the user name and password.
Set a complicated text as a password so that other users cannot guess easily, and use it properly. Allow only the passwords that follow the operation rules established by users to be set.
To prevent the default password distributed by the administer from being used as it is, the function can require the user to change the password at the first login.
Operators must use their own user accounts when logging in. Using the user account of other operators or sharing one user account among multiple operators is prohibited. The users must take some measures to observe the rules above.
To prevent impersonations, set the automatic logout time so that the operator is automatically logged out if no operation is performed for a certain period of time. Set the password expiration date for prompting the periodic update of the password. Do not divulge user account information (user name and password) to anyone other than the operator.
If a theft or loss of the password occurs, invalidate the account and reissue a password in accordance with the operation rules established by users.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10
§11.10 (d)
§11.100 (a)
§11.100 (b)
§11.200 (a)(1)
§11.200 (a)(2)
§11.300 (a)
§11.300 (b)
§11.300 (C)

Operator management



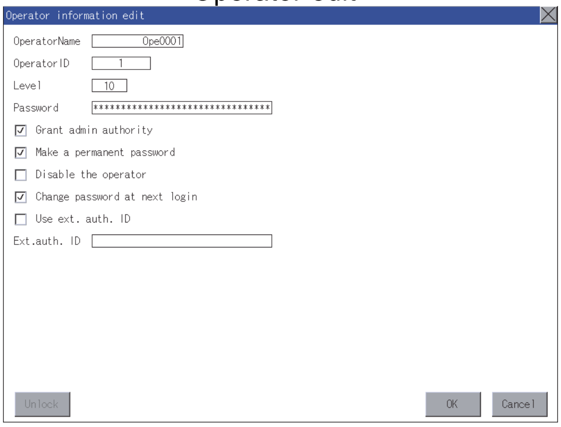
Operator information management

	OperatorName	ID	Level	Update	Lock status
◎	Administrator	–	–	–	
	Ope0001	1	10	08/19/2017	
	Ope0002	2	5	08/19/2017	✓
◎	Ope0011	3	15	08/19/2017	
◎	Ope0012	4	10	08/19/2017	
×	Ope0021	5	8	08/19/2017	

◎: admin authority
×: disabled

Drive in use: A

Operator edit



Operator information edit

OperatorName	Ope0001
OperatorID	1
Level	10
Password	********************************

☑ Grant admin authority
☑ Make a permanent password
☐ Disable the operator
☑ Change password at next login
☐ Use ext. auth. ID

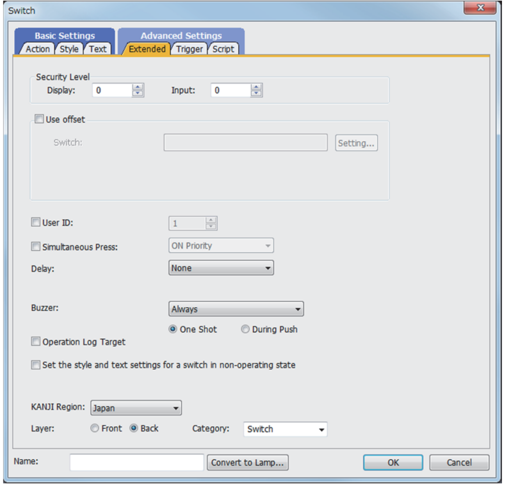
Ext.auth. ID

3.1.2 Security level

The security level can be set for each user.
The screens or objects displayed can be set according to the security level.
The security level can also be set for each object.
Doing so limits the range of operations that each user can perform according to their authorities.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10 (g)

Security level setting



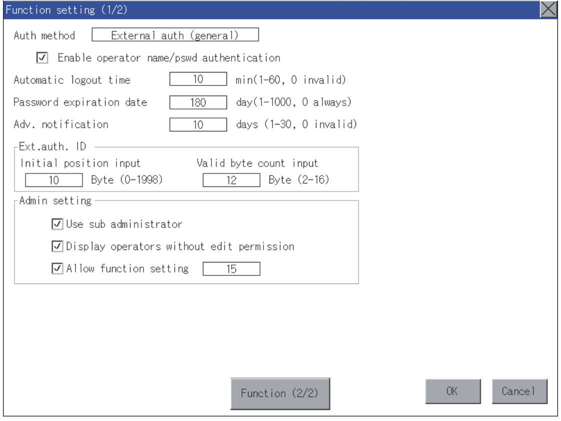
Security Level
Display: 0 Input: 0

□ Use offset
Switch:

□ User ID: 1
□ Simultaneous Press: ON Priority
Delay: None
Buzzer: Always
● One Shot ○ During Push
□ Operation Log Target
□ Set the style and text settings for a switch in non-operating state

KANJI Region: Japan
Layer: ○ Front ● Back Category: Switch
Name:

Function Setting (1/2)

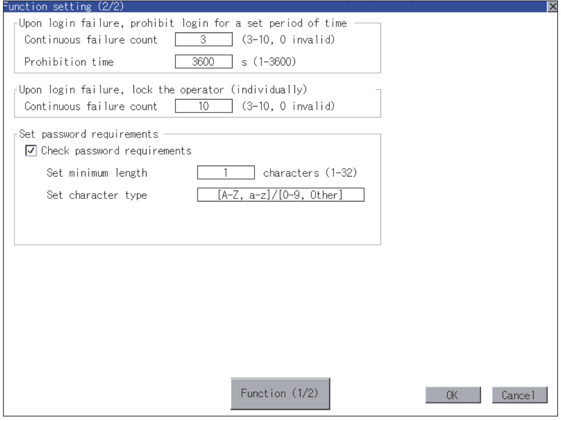


Auth method External auth (general)
☑ Enable operator name/pswd authentication
Automatic logout time 10 min(1-60, 0 invalid)
Password expiration date 180 day(1-1000, 0 always)
Adv. notification 10 days (1-30, 0 invalid)

Ext.auth. ID
Initial position input 10 Byte (0-1998)
Valid byte count input 12 Byte (2-16)

Admin setting
☑ Use sub administrator
☑ Display operators without edit permission
☑ Allow function setting 15

Function Setting (2/2)



Upon login failure, prohibit login for a set period of time
Continuous failure count 3 (3-10, 0 invalid)
Prohibition time 3600 s (1-3600)

Upon login failure, lock the operator (individually)
Continuous failure count 10 (3-10, 0 invalid)

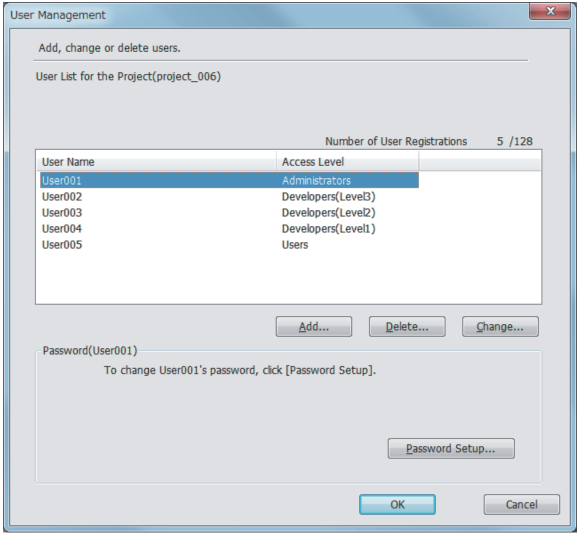
Set password requirements
☑ Check password requirements
Set minimum length 1 characters (1-32)
Set character type [A-Z, a-z]/[0-9, Other]

3.2 Managing Drawing Data

The users who are authorized to display and edit project data can be managed with this setting.
The authority of display and edit can be set for each user.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10

User management



User Management

Add, change or delete users.

User List for the Project(project_006)

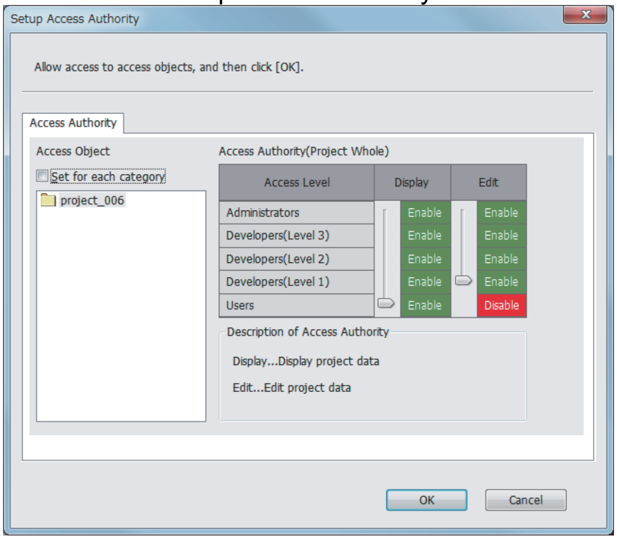
Number of User Registrations 5 /128

User Name	Access Level
User001	Administrators
User002	Developers(Level3)
User003	Developers(Level2)
User004	Developers(Level1)
User005	Users

Password(User001)

To change User001's password, click [Password Setup].

Setup access authority



Setup Access Authority

Allow access to access objects, and then click [OK].

Access Authority

Access Object

□ Set for each category

project_006

Access Authority(Project Whole)

Access Level	Display	Edit
Administrators	Enable	Enable
Developers(Level 3)	Enable	Enable
Developers(Level 2)	Enable	Enable
Developers(Level 1)	Enable	Enable
Users	Enable	Disable

Description of Access Authority

Display...Display project data

Edit...Edit project data

3.3 Completeness of Data

Some data collected by the GOT in the data storage is regularly overwritten and updated. Thus, users need to construct and operate a system to regularly back up and save data in a personal computer or a file server to prevent loss of data due to accidents or unauthorized access.
To save the data to a personal computer or file server periodically, the network drive function, FTP server function, and FTP client function of the GOT2000 series and GT SoftGOT2000 are provided.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10 (c)

3.4 Security and Viewing of Data

3.4.1 Data security

The binary data in the data storage is obfuscated. Thus, reading the data is not easy.
The record data that needs protection from falsification shall be saved in the binary format.
The extensions of the binary format for each GOT series are as follows.

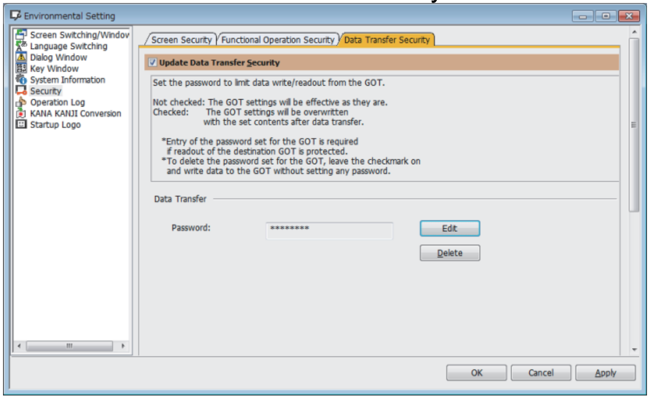
- For the GOT2000 series, GT SoftGOT2000: .G2□

- For the GOT1000 series: .G1□

Reading and writing data on the GOT can be managed with a password. This can prevent the settings in the GOT from falsification.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10

Data transfer security



☑ Update Data Transfer Security

Set the password to limit data write/readout from the GOT.

Not checked: The GOT settings will be effective as they are.
Checked: The GOT settings will be overwritten with the set contents after data transfer.

*Entry of the password set for the GOT is required if readout of the destination GOT is protected.
*To delete the password set for the GOT, leave the checkmark on and write data to the GOT without setting any password.

Data Transfer

Password: ********

3.4.2 Viewing the data

(1) How to view the binary data collected by the GOT on a personal computer

To view the data, convert a binary-format file read out to the personal computer into a CSV or Unicode text file by using GT Designer3 or Data Transfer Tool.
Furthermore, use CSV and Unicode text files only for checking the data to prevent falsification of data.
When saving the data, use a data format that makes falsification of data impossible, such as PDF with a security function.
"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10 (b)
§11.50

(2) How to check the binary-format data directly on the GOT or view it by printing

Create the data that can be viewed on the GOT2000 series using the report function.

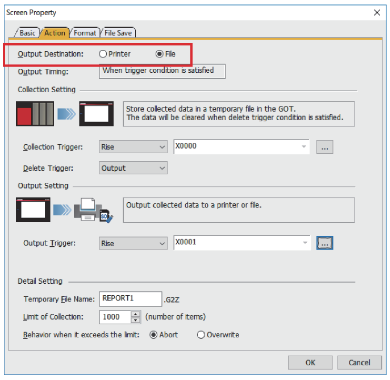
The data created for recording (binary format, extension: G2R) can be viewed on the GOT2000 series using the file print function. Also, to view the data on the paper, print it from the GOT2000 series using a printer.

∗ Use GT Simulator3 to view the data created on the GOT2000 series on a personal computer.

"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10 (b)
§11.50

Report function setting



Screen Property

Tabs: Basic / Action / Format / File Save

Output Destination: ○ Printer ● File

Output Timing: When trigger condition is satisfied

Collection Setting

Store collected data in a temporary file in the GOT.
The data will be cleared when delete trigger condition is satisfied.

Collection Trigger: Rise X0000

Delete Trigger: Output

Output Setting

Output collected data to a printer or file.

Output Trigger: Rise X0001

Detail Setting

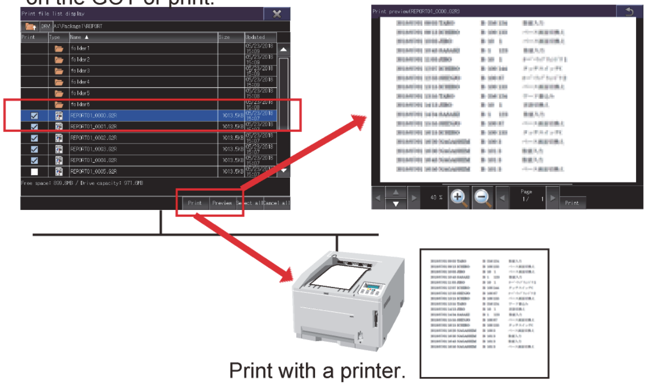
Temporary File Name: REPORT1 .G2Z

Limit of Collection: 1000 (number of items)

Behavior when it exceeds the limit: ● Abort ○ Overwrite

Select whether to view on the GOT or print.

View on the GOT.



Print with a printer.

3.5 Audit Trail

The audit trails (histories for the follow-up survey later) can be recorded by properly setting the operation logs.

The following information is required to be recorded.

- Time stamp
- User name of the logged-in operator
- Description and details of the operation performed by the operator (such as the results of data change)

The operation performed can be recorded with intended names by giving objects names.

The GOT2000 series and GT SoftGOT2000 can record up to 100 characters and the GOT1000 series can record up to 30 characters in the log.

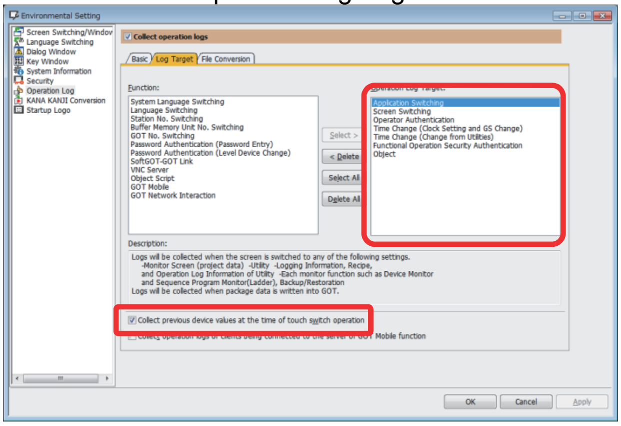
Revising of the operator management information can also be logged.

Set the log targets of the operation log as follows.

"Corresponding articles of the FDA 21 CFR Part 11"

➟ §11.10 (e)
§11.50

Operation log target



Environmental Setting

☑ Collect operation logs

Tabs: Basic / Log Target / File Conversion

Function:
System Language Switching
Language Switching
Station No. Switching
Buffer Memory Unit No. Switching
GOT No. Switching
Password Authentication (Password Entry)
Password Authentication (Level Device Change)
SoftGOT-GOT Link
VNC Server
Object Script
GOT Mobile
GOT Network Interaction

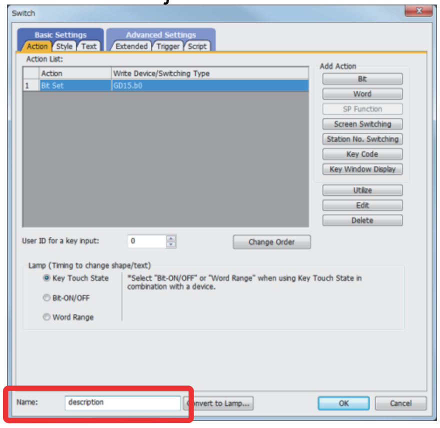
Operation Log Target:
Application Switching
Screen Switching
Operator Authentication
Time Change (Clock Setting and GS Change)
Time Change (Change from Utilities)
Functional Operation Security Authentication
Object

Description:
Logs will be collected when the screen is switched to any of the following settings.
-Monitor Screen (project data) -Utility -Logging Information, Recipe,
and Operation Log Information of Utility -Each monitor function such as Device Monitor
and Sequence Program Monitor(Ladder), Backup/Restoration
Logs will be collected when package data is written into GOT.

☑ Collect previous device values at the time of touch switch operation

□ Collect operation logs of clients being connected to the server of GOT Mobile function

Object name



Switch

Tabs: Basic Settings (Action / Style / Text) / Advanced Settings (Extended / Trigger / Script)

Action List:

	Action	Write Device/Switching Type
1	Bit Set	GD15.b0

User ID for a key input: 0

Lamp (Timing to change shape/text)
● Key Touch State
○ Bit-ON/OFF
○ Word Range

*Select "Bit-ON/OFF" or "Word Range" when using Key Touch State in combination with a device.

Name: description

3.6 Validation of Data and Operations

The users need to check if there are unauthorized falsifications in project data. The users can check changes by regularly backing up the project data and comparing the backup project data with the latest project data by using the verification function of GT Designer3.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.10 (h)

3.7 System Development, Operation, and Management

Design screens that do not accept unauthorized operations. For such screen design, set triggers or security level for every object and control screen transition and status transition properly when a switch is operated.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.10 (f)

It is important for proper system operation that developers who have appropriate skills construct a system and operators who use the system are properly trained. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.10 (i)

The GOT does not have a function for electronic signatures. To use electronic signatures, sign the signature with a personal computer when storing data files collected by the GOT to the personal computer.
Electronic signatures require the appropriate policy and observation on the policy. In addition, the users must prove to the FDA that the electronic signature has the legal binding force equivalent to hand-writing signatures. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.10 (j)
§11.100 (c)(1)
§11.100 (c)(2)

Electronic signatures must correspond to the electronic record and must be protected from being deleted, copied, or transferred. Creation of the false electronic records must also be prevented. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.70

The user's manual of the GOT can be downloaded from the MITSUBISHI ELECTRIC FA Global Website (www.MitsubishiElectric.com/fa/).
Distribution, access, and usage of the documents about the operation and maintenance of the user system must be properly managed. In addition, audit on the creation and revision of the documents must be tracked in chronological order. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.10 (k)

For the use as an open system, a system that provides safe application and data processing must be constructed. The GOT2000 series and GOT1000 series can be operated remotely with the VNC function. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.30

The GOT does not have a function of adding an electronic signature to each log data. The users need to construct a mechanism that converts the data format of log data to a format that makes falsification of data impossible, such as PDF with a security function, and add an electronic signature after log data is read out to the personal computer.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.200

For the electronic signature by proxy, establish operation rules so that two or more operators are required to perform the operation together.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.200 (a)(3)

If the user account lost the credibility due to loss, theft, or other reason, the account is required to be invalidated or locked out. In this case, flexible measures are required, such as preparing a substitute with appropriate control.
The operator authentication function can invalidate unnecessary users. Establish operation rules using this function and use them properly to manage the user account information properly. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.300 (c)

Log-in failures are recorded in the operation log. However, the recorded data does not include the information whether the name of the user was registered on the GOT before the login failure.
If an unauthorized login operation is performed, the Incorrect Login signal (GS242.b0) and Operator Locked signal (GS242.b1) notify the event. The users can use the signals as triggers to generate an alarm, or use the signals to construct a system to notify the event to external devices. Note that GS242 is available for the GOT2000 series and GT SoftGOT2000.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.300 (d)

Whether devices used operate normally and are not changed improperly must be checked before the use of the system and periodically. The users need to take some measures for the above.
"Corresponding articles of the FDA 21 CFR Part 11"
➟ §11.300 (e)

4. POINTS TO CONSIDER FOR REQUIREMENTS

4.1 System That Prevents Records from being Falsified

○: Available, △: Available with conditions, ×: Not available

Data	Availability	Support on the GOT	Points to consider
Operation log	○	1) Saving logging data in the binary format prevents the data from being easily falsified. *1 <Binary format file> G2O: GOT2000 series, GT SoftGOT2000 G1O: GOT1000 series 2) The MES interface function saves logging data in a database. *2	1) To keep log files in the binary format for the required period of time, construct a mechanism that regularly copies the files from the GOT into a personal computer and backs up them as needed. 2) To save log files in a database, construct a system that prevents the data from being falsified.
Alarm (GOT2000, GT SoftGOT2000), Advanced alarm (GOT1000)	○	1) Saving logging data in the binary format prevents the data from being easily falsified. <Binary format file> G2A: GOT2000 series, GT SoftGOT2000 G1A: GOT1000 series 2) The MES interface function saves logging data in a database. *2	
Logging	○	1) Saving logging data in the binary format prevents the data from being easily falsified. <Binary format file> G2L: GOT2000 series, GT SoftGOT2000 G1L: GOT1000 series 2) The MES interface function saves logging data in a database. *2	
Report (GOT2000, GT SoftGOT2000)	○	1) Saving logging data in the binary format prevents the data from being easily falsified. <Binary format file> G2R: GOT2000 series, GT SoftGOT2000 G1R: GOT1000 series 2) The data can be output to a printer using the file print function. *3	-
Recipe (GOT2000, GT SoftGOT2000), Advanced recipe (GOT1000)	△	Saving logging data in the binary format prevents the data from being easily falsified. <Binary format file> G2P: GOT2000 series, GT SoftGOT2000 G1P: GOT1000 series	Performing the read recipe operation updates the device values of the recipe file. Before performing this operation, construct a system that backs up the file into a personal computer.
Recipe (GOT1000)	×	The recipe data saved in the CSV format is inappropriate for use because the data may be easily falsified. Use the advanced recipe.	-

*1 Turning on the Prohibit Operation Log Information Operation signal (GS522.b3) restricts the operations on the Operation log information screen to only the [Latest] and [List] buttons.
This setting prevents operation log files from being copied or deleted unnecessarily.

*2 GT SoftGOT2000 does not support the MES I/F function.

*3 GT SoftGOT2000 does not support the file print function.
Open the created CSV file with a Windows application to print.

4.2 Records of Who Did the Operation

○: Available, △: Available with conditions, ×: Not available

Function	Availability	Support on the GOT	Points to consider
Operator authentication	○	Using the operator authentication function makes the currently logged-in operator name to be recorded in the operation log. By setting the automatic logout time, the operator is automatically logged out if no operation is performed for a certain period of time. This prevents impersonations of the operator. In addition, setting a password expiration date prompts the periodic update of a password. (It is also possible to prompt the change of the password before the expiration date.*1) To set a password correctly and use it, requirements (minimum text length and combination of character types) for a password can be specified. *1 When the default password distributed by the administer must be changed, this function can require the user to change the password at the first login. *1 To prevent improper use of the operator information that is no longer used, the target operator can be invalidated. *1	To identify the logged-in operator, do not share one account among multiple operators. Create different accounts for each operator. Establish operation rules for encouraging the periodic update of a password and requirements for a password. Establish operation rules for invalidating or deleting unnecessary operator account to manage the operator information properly.
		Unauthorized login attempts (repeated login failures) can be detected and notified with alarms, lamps, etc. *1	-

*1 Available to the GOT2000 series and GT SoftGOT2000.

4.3 Records of When the Operation was Performed

○: Available, △: Available with conditions, ×: Not available

Function	Availability	Support on the GOT	Points to consider
Operation log	○	When device values affecting control are changed by operating a touch switch, numerical input, text input, or others, information on the change (who, when, what, and how) can be logged. *1	-

*1 For the update of data, refer to the following.
➟ 2.4 Records of Updated Data

4.4 Records of Updated Data

○: Available, △: Available with conditions, ×: Not available

Data	Availability	Support on the GOT	Points to consider
Object name	○	When the object name is specified in the setting of the touch switch, numerical input, or text input (ASCII input), the object name can be recorded in the operation log.	-
Values before/after change	○	• Touch switch: To record the value before change, select [Collect previous device values at the time of touch switch operation] in the operation log setting. *1 • Numerical input, text input (ASCII input): Values both before and after change can be recorded.	-
Device	△	When a device value is changed by operating a touch switch, numerical input, or text input (ASCII input), the target device (device type and address) can be recorded. *2	-
		[Unsupported item] Changes in devices by the following functions cannot be recorded. When using the GOT2000 series: • Device monitor • Sequence program monitor When using the GOT1000 series: • System monitor • Ladder monitor	When constructing a system compliant with the FDA 21 CFR Part 11, do not use the functions shown on the left. If the functions are used, set security measures for starting the functions with touch switches and calling up the utility screen. Define clear operation rules so that specific operators can use the functions.
Screen number	○	The numbers of the screens on which operation was performed can be recorded.	-
Recipe (GOT2000, GT SoftGOT2000), Advanced recipe (GOT1000)	△	When the target recipe setting number and record number are set to be written to word devices by using touch switches, the numbers can be logged. *3	To record device values to be updated using the recipe function, take measures, such as constructing an external system to obtain and save the target recipe file at the recipe execution in a personal computer.
Script	×	Device operation events cannot be recorded by using scripts. *4	-
Alarm history (GOT2000, GT SoftGOT2000), Advanced alarm (GOT1000)	△	The alarm history and advanced alarm can record deletion operations. However, it is not possible to record which alarm was deleted.	To identify a deleted alarm, take measures, such as constructing a system to read alarm log files before and after the delete operation to a personal computer, and compare the contents of the files.
Data deletion	×	Deletion or copy of files cannot be recorded by using utility operations or by scripts. *5	-
Operator information	○	The operator authentication function records the operations performed on the operator information in the log. *1*6	-

*1 Available to the GOT2000 series and GT SoftGOT2000.

*2 For the GOT1000 series, the extended function OS (Device Name Conversion Library) is required to record the target devices correctly.

*3 Events of writing data to the controller by using the recipe or advanced recipe function cannot be recorded.

*4 Design screens so that device operations are not performed by using scripts.

*5 To prevent important files, such as log files, from being deleted unintentionally, the users need to take measures, such as setting a password for startup with a special function switch and startup of the utility, and setting a security level to the touch switch for performing file operations.

*6 The information about who changed the operator information can be recorded in the log by setting the sub manager.

5. WHEN USING GT SoftGOT2000

GT SoftGOT2000 is an application that operates on Windows.
Users can use the following functions that interact with Windows applications when constructing a system.

- Application start-up function
- Internal device interface function
- Edgecross interaction function

6. PRECAUTIONS

For the proper system operation, the users must define clear operation rules and ensure that operators strictly adhere to the rules. This document describes how to comply with the FDA 21 CFR Part 11 when using a GOT-contained system. Some requirements of the FDA 21 CFR Part 11 can be satisfied by using the GOT functions. To comply with the other requirements, a combined use of operation rules and external systems is required.

7. REFERENCE INFORMATION

■Website of the FDA organization

For the details of the FDA, refer to the following website.

➟ www.fda.gov

REVISIONS

Version	Print Date	Revision
-	November 2014	- First edition
A	May 2016	- The descriptions of whether the compliance with each article of the FDA 21 CFR Part 11 is available have been added to "1. OVERVIEW". - The descriptions of the GOT2000 new functions have been added to "2. POINTS TO CONSIDER FOR REQUIREMENTS". - The descriptions of "3. COMPLIANCE WITH FDA 21 CFR Part 11 BY USING THE GOT" have been modified.
B	August 2017	- The descriptions of the GOT2000 new functions have been added to "2. POINTS TO CONSIDER FOR REQUIREMENTS". - The descriptions of "3. COMPLIANCE WITH FDA 21 CFR Part 11 BY USING THE GOT" have been modified.
C	November 2017	- The descriptions of the GOT2000 new functions have been added to "2. POINTS TO CONSIDER FOR REQUIREMENTS". - The descriptions of the GOT2000 function extension have been added to "3. COMPLIANCE WITH FDA 21 CFR Part 11 BY USING THE GOT".
D	October 2018	- The descriptions of the GOT2000 new functions have been added to "2. POINTS TO CONSIDER FOR REQUIREMENTS". - The descriptions of the GOT2000 function extension have been added to "3. COMPLIANCE WITH FDA 21 CFR Part 11 BY USING THE GOT".
E	September 2019	- GT SoftGOT2000 and the MELIPC series MI3000 have been added to Relevant Models. - "2. LIST OF GOT FUNCTIONS RELATED TO FDA 21 CFR Part 11" has been added. - "5. WHEN USING GT SoftGOT2000" has been added. - "7. REFERENCE INFORMATION" has been added.