

How to Comply
with
FDA 21 CFR Part11

Sample Screen Manual

Mitsubishi Electric Corporation

Using the Samples

The sample screen data and files such as the instruction manual can be used upon agreement to the following matters.

- (1) This data is available for use by customers currently using or considering use of Mitsubishi products.
- (2) The intellectual property rights of the files provided by Mitsubishi (hereinafter referred to as the "Files") belong to Mitsubishi.
- (3) Alteration, reproduction, transfer, or sales of the Files is prohibited.
This does not apply when the content, in part or full, is used for Mitsubishi products incorporated in a device or system created by the customer. Furthermore, this does not apply to the transfer, reproduction, reference, or change of layout in the specifications, designs, or instruction manuals of built-in products prepared by the customer using Mitsubishi products.
- (4) Mitsubishi will not be held liable for any damages resulting from the use of the Files or the data extracted from the Files. The customer is responsible for all use.
- (5) If any usage conditions are appended to the Files, those conditions must be observed.
- (6) The Files may be deleted or the contents changed without prior notice.
- (7) When using the Files, please always read the corresponding manuals and related manuals indicated therein. Please pay special attention to safety, and correctly handle the product.

CONTENTS

REVISIONS	4
1. OUTLINE	5
2. SYSTEM CONFIGURATION	5
3. GOT	5
3.1 System Applications that are Automatically Selected	5
3.2 Controller Settings of Screen Design Software	6
3.3 Ethernet Settings of Screen Design Software	6
3.4 GOT Settings for Compliance with FDA 21 CFR Part11	6
4. SCREEN SPECIFICATIONS	7
4.1 Display Language	7
4.2 Screen List/Transition	7
4.3 Screen Specifications	8
4.3.1 Menu (B-30001)	8
4.3.2 Alarm (B-30002)	9
4.3.3 Parameter Setting (B-30003)	10
4.3.4 Utility Call (B-30004)	11
4.4 Device List	12
4.5 Comment List	12
4.6 Script List	13
5. GOT RELATED SETTINGS FOR USING OPERATOR AUTHENTICATION	14
5.1 Administrator Password Setting	14
5.2 Operator Registration	16
5.3 Function Setting for Operator Authentication	18
5.4 Precautions	21
6. OPERATION LOG SETTING	22
6.1 Basic Tab	22
6.2 Log Target Tab	23
6.3 File Conversion Tab	23
7. RESOURCE DATA (DATA GENERATED ON GOT)	24
7.1 Convert Binary File into Unicode Text/CSV File	24
7.2 Transfer to Database using MES Interface	24
8. PROJECT DATA PROTECTION	25
8.1 Data Transfer Security	25
8.2 Project Security	25
8.3 Project Verification	25

REVISIONS

Sample Screen Manual

Date	Control No.*	Description
2016/3	BCN-P5999-0665	First edition
2017/10	BCN-P5999-0665-2	Improved operation log function and operator authentication function

* The control No. is noted at the lower right of each page.

Project Data

Date	Project Data	GT Designer3*	Description
2016/3	FDA21CFR Part11_V_Ver1_E.GTX	1.152J	First edition
2017/10	FDA21CFR Part11_V_Ver2_E.GTX	1.185T	Renewed menu screen, improved operation log function

* The version number of screen design software used to create the project data is listed. Please use the screen design software with the listed version or later versions.

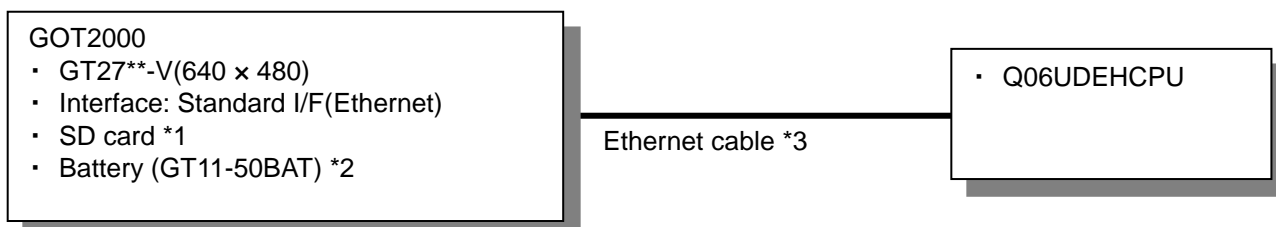
1. OUTLINE

This manual explains sample screens of GOT2000 that shows examples of settings which comply with FDA 21 CFR Part11. FDA 21 CFR Part11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES). Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper record. FDA 21 CFR Part11 is designed to ensure the traceability of the electronic data, to configure a structure in which the data is to be electronically saved, and to promote the application of the structure.

In the sample screens, the operator authentication function and operation log function are used in order to satisfy the requirements of FDA 21 CFR Part11. In addition, the alarm function is used as an example of recording the resource data (that is generated on the GOT). Note that the operator authentication cannot be used for the security for restricting the utility startup, and therefore, we set a security level to a screen for calling the utility function so that only authorized operators can access the screen.

*When creating a screen, change a sample setting appropriately in accordance with your system. The requirements of FDA 21 CFR Part11 are not entirely satisfied by the GOT. To ensure the full compliance with FDA 21 CFR Part11, please construct your own systems and operational rules. For the details on guidelines on compliance with FDA 21 CFR Part11 for GOT2000 Series and the scope of application on the GOT, please refer to "TECHNICAL BULLETIN (GOT-A-0077-B or later)".

2. SYSTEM CONFIGURATION



*1: SD card is used to save alarm log files or operation log files.

*2: Battery is used to backup the clock data and the user alarm data in the SRAM user area in case of power failures.

*3: For more details on the cable, please refer to "GOT2000 Series Connection Manual (Mitsubishi Products)".

3. GOT

3.1 System Applications that are Automatically Selected

Type	System application name	
Standard Function	Standard System Application	
	Standard Font	Japanese
Communication Driver	Ethernet Connection	Ethernet(MELSEC), Q17nNC, CRnD-700, Gateway
Extended Function	Standard Font	Chinese (Simplified)
	Outline Font	Alphanumeric/Kana
		Japanese (Kanji)
		Chinese (Simplified)
	Device monitor	
	Operation Log Screen Image *1	
	Operator Authentication *2	
	GOT Platform Library	

*1: The operation log screen image is a system application for use in displaying screen images of operation logs so that the logs can be viewed on the GOT.

*2: The operator authentication is a system application that is required to comply with FDA 21 CFR Part11.

3.2 Controller Settings of Screen Design Software

Detail Setting

Item	Set value	Remarks
GOT NET No.	1	
GOT Station	2	
GOT Standard Ethernet Setting	Refer to table below	
GOT Communication Port No.	5001	
Retry (Times)	3	
Startup Time (Sec)	3	
Timeout Time (Sec)	3	
Delay Time (ms)	0	
Servo Axis Switching GD Device First No.	10	

GOT Standard Ethernet Setting

Item	Set value	Remarks
Reflect the GOT standard Ethernet setting in the GOT	Checked	
GOT IP Address	192.168.3.18	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	
Peripheral S/W Communication Port No.	5015	
Transparent Port No.	5014	

3.3 Ethernet Settings of Screen Design Software

	Host	Net No.	Station	Unit Type	IP Address	Port No.	Communication
1	*	1	1	QnUD(P)V/QnUDEH	192.168.3.39	5006	UDP

3.4 GOT Settings for Compliance with FDA 21 CFR Part11

The following points shall be noted in creating screens.

3.4.1 Operator authentication

In order to allow only authorized operators to access the GOT and identify an individual operator, make sure to use the operator authentication function and set the followings.

- Screen setting for logout
- Authentication method: operator name + password
- Automatic logout time
- Password expiration date
- Password expiration prenotification

It is recommended to set the followings for higher security (FDA 21 CFR Part11 §11.300(d)).

- Prohibit a login for a set period of time upon a login failure
- Lock an operator upon a login failure
- Set an alarm to detect and notify an incorrect login attempt

To use the operator authentication, GOT related settings are needed. For the details on the GOT related settings, please refer to "5. GOT RELATED SETTINGS FOR USING OPERATOR AUTHENTICATION".

3.4.2 Operation log

Collect operation logs in order to record the operation information such as "when", "who", and "which operation was performed". For more details, please refer to "6. OPERATION LOG SETTING".

3.4.3 File format for saving resource data

Save the resource data (such as alarm log files or operation log files that are generated on the GOT) in the binary file in order to prevent the data from being easily falsified. To convert the binary file into a readable format, please refer to "7.1 Convert Binary File into Unicode Text/CSV File".

3.4.4 Power failure backup

Attach a battery in order to hold the clock data.

4. SCREEN SPECIFICATIONS

4.1 Display Language

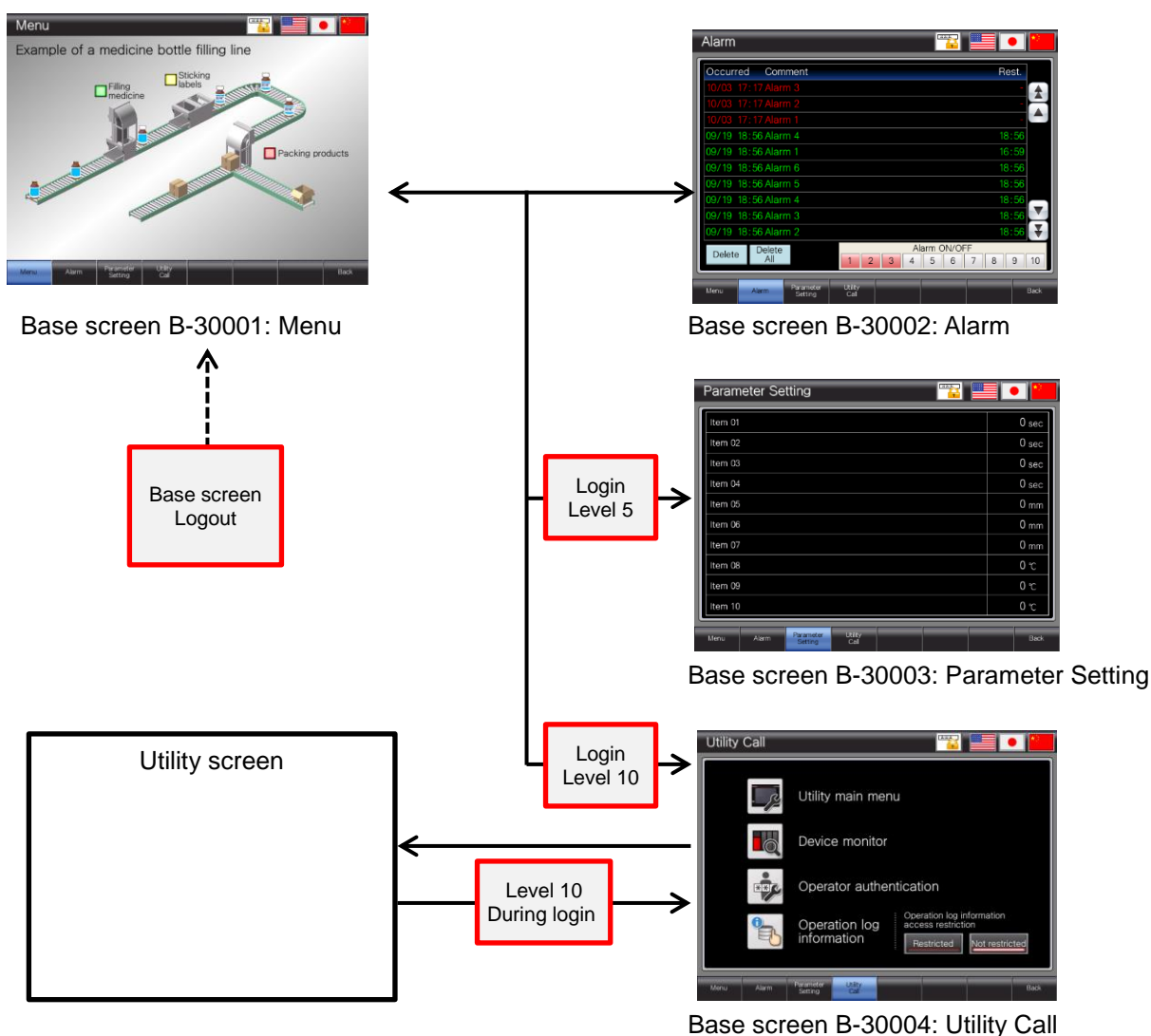
The language of the text displayed on the screen can be switched between English, Japanese, and Chinese (Simplified). The texts in three languages are registered in the columns No.1 to No.3 respectively in the comment group No.499 and No.500 as shown below. When the column No. is stored in the language switching device, the text in the language corresponding to the column No. will be displayed.

Column No.	Language
1	English
2	Japanese
3	Chinese (Simplified)

4.2 Screen List/Transition

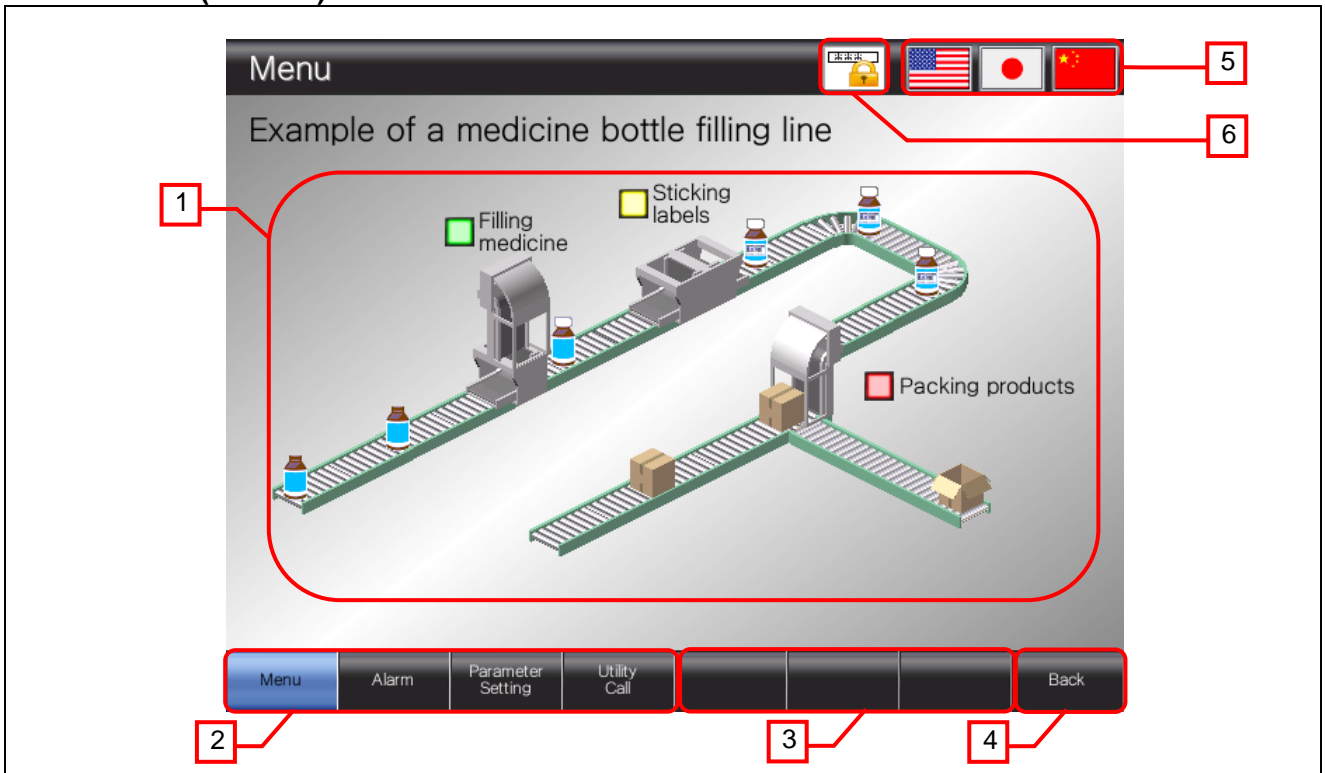
With the operator authentication, a security level (1 to 15) can be set on a screen. It restricts the access to the screen by an operator who does not have the specified security level.

The sample screen shows examples of setting the screen access authority and switch operation authority per operator. For example, the security level 5 is set for [Base screen B-30003: Parameter Setting] and the [Delete] / [Delete All] switches on [Base screen B-30002: Alarm], and the security level 10 is set for [Base screen B-30004: Utility Call]. After writing the project data into the GOT, register an operator before starting to operate a user screen. For the details on the settings required for the operator authentication such as operator registration, please refer to "5. GOT RELATED SETTINGS FOR USING OPERATOR AUTHENTICATION".



4.3 Screen Specifications

4.3.1 Menu (B-30001)



OUTLINE

This screen shows the menu. When an operator logged out, this screen is displayed.

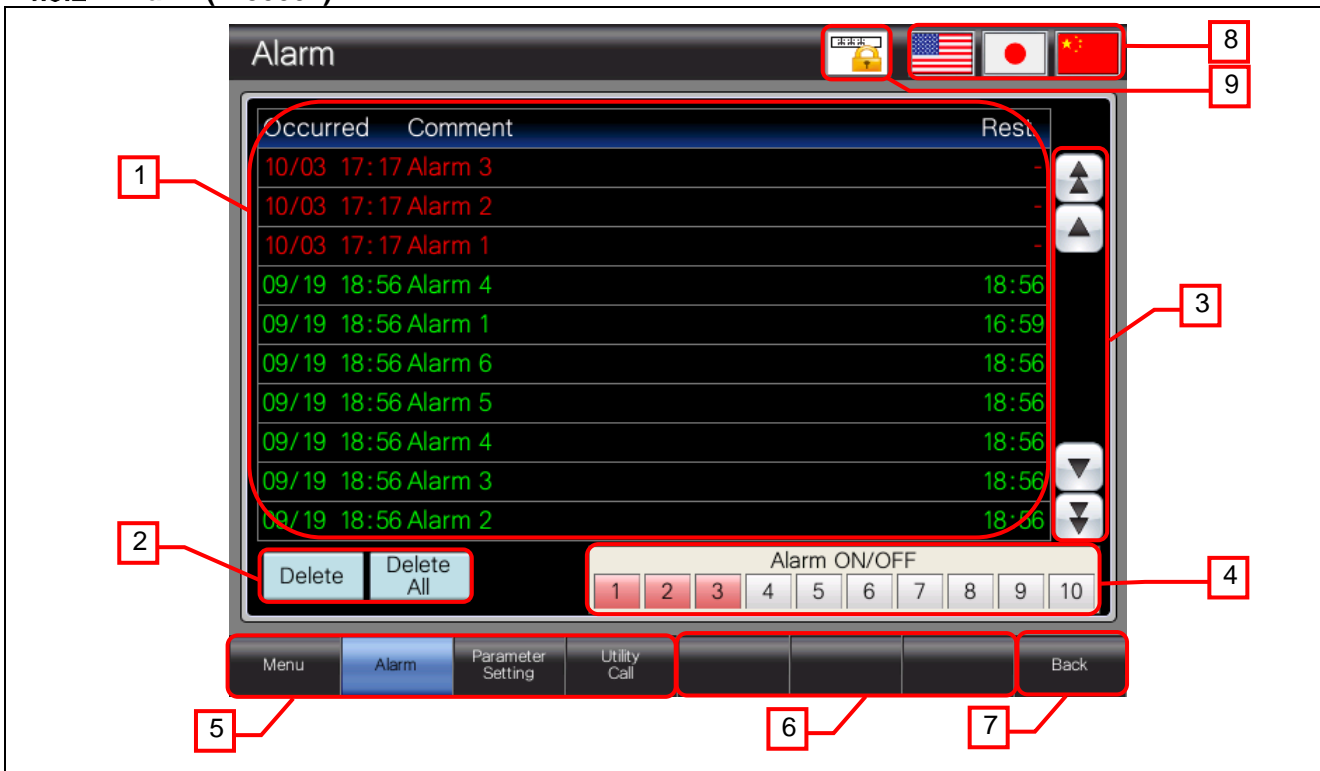
Description

1. Displays demo mode screen for a medicine bottle filling line as an example.
2. Switches between the screens. The blue switch that indicates the current screen does not switch the screen.
3. Indicates unused switches for base screen switching.
4. Switches to the previously opened screen.
5. Switches the display language between three languages.
6. During logout: Displays the login window.
During login: Displays the confirmation window to select logging out or operator switching.

Remarks

- A screen script is being set to control the demo operation of a medicine bottle filling line. For the details on the script, please refer to [4.6 Script List].
- [Base screen B-30004: Utility Call] is provided as the menu for selecting the utility function. For this utility function menu, we have applied the setting that identifies an operator who performs the utility function and records it in the operation log file.
- For the switches shown as [5], we have applied the setting that switches the system language in accordance with the display language.

4.3.2 Alarm (B-30002)



OUTLINE

This screen is designed to check equipment status and operation history (such as alarm log files and operation log files), which is required to comply with FDA 21 CFR Part11. The input security level is set for the [Delete] and the [Delete All] switches so that only an authorized operator can use them.

Description

1. Displays occurred alarms.
2. These switches are activated while an operator who has the security level 5 or higher is logging in. Having become grayed out, these switches cannot be used.
Delete: Deletes a selected restored alarm.
Delete All: Deletes all of the restored alarms.
3. : Scrolls a page up and down.
 : Scrolls row by row up and down.
4. Generates or restores an alarm alternately with a single touch. These switches are provided for operational validation.
5. Switches between the screens. The blue switch that indicates the currently displayed screen does not switch the screen.
6. Indicates unused switches for base screen switching.
7. Switches to the previously opened screen.
8. Switches the display language between three languages.
9. During logout: Displays the login window.
During login: Displays the confirmation window to select logging out or operator switching.

- For operational validation, generate or restore an alarm using the switches shown as [4], and then, delete the restored alarm using the switches shown as [2]. The alarm deletion is recorded in the operation log.
- We have applied the setting for collecting the alarm of the login prohibition and operator lock when the login prohibition and operator lock due to login failures are set for the GOT.
- When an operator logged out, [Base screen B-30001: Menu] is displayed.
- For the switches shown as [8], we have applied the setting that switches the system language in accordance with the display language.

4.3.3 Parameter Setting (B-30003)



OUTLINE

This screen is designed to show setting items. We have applied the setting that allows this screen to be opened only by an operator who has the security level 5 or higher.

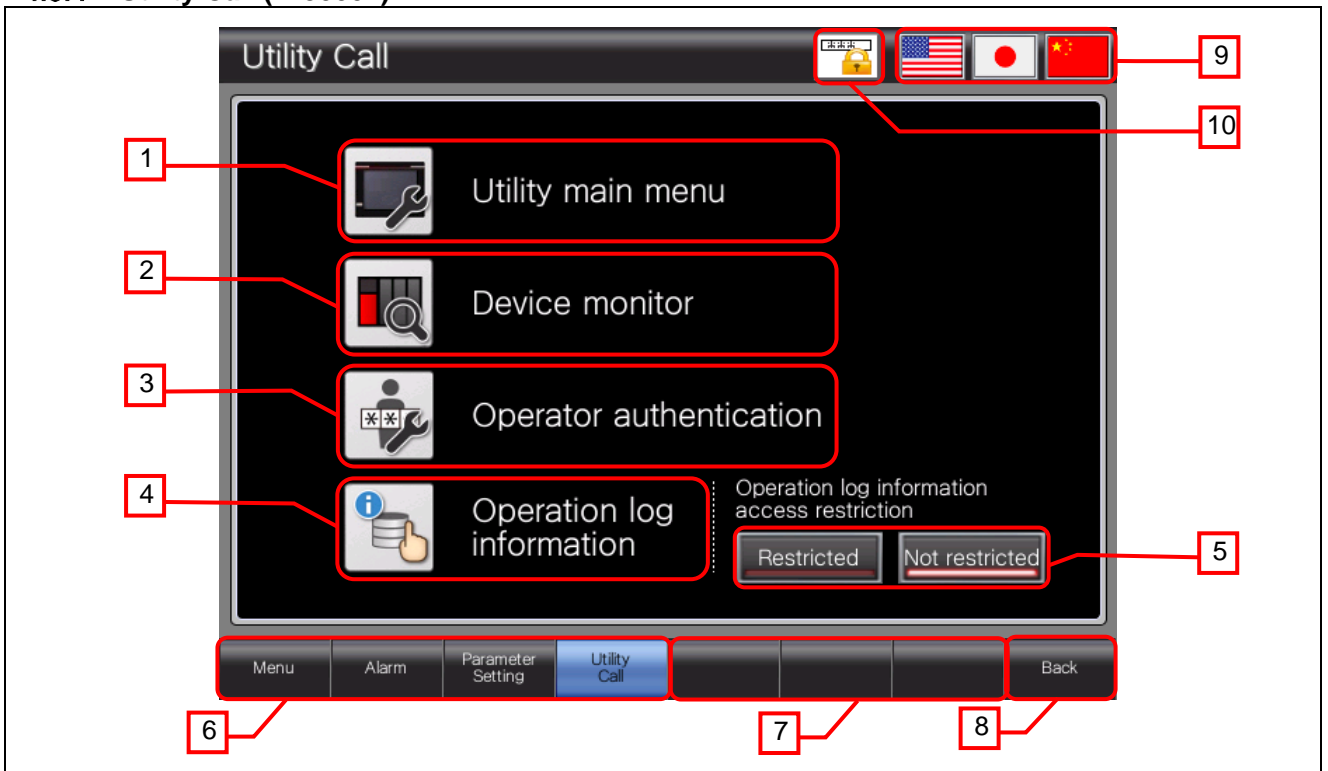
Description

1. Indicates the numerical input.
2. Switches between the screens. The blue switch that indicates the currently displayed screen does not switch the screen.
3. Indicates unused switches for base screen switching.
4. Switches to the previously opened screen.
5. Switches the display language between three languages.
6. During logout: Displays the login window.
During login: Displays the confirmation window to select logging out or operator switching.

Remarks

- An individual name is set for the numerical input shown as [1] in order to easily identify the numerical input that has been operated on the operation log.
- When an operator logged out, [Base screen B-30001: Menu] is displayed.
- For the switches shown as [5], we have applied the setting that switches the system language in accordance with the display language.

4.3.4 Utility Call (B-30004)



Outline

This screen is designed to select the utility function. We have applied the setting that allows this screen to be opened only by an operator who has the security level 10 or higher.

Description

1. Switches to the utility main menu.
2. Activates the device monitor.
3. Switches to the operator setting menu.
4. Switches to the operation log information screen.
5. Restricts the functions which can be used on the operation log information screen.
Restricted: Only functions of [Latest] and [List] can be used on the operation log information screen.
Not Restricted: All functions can be used on the operation log information screen.
6. Switches between the screens. The blue switch that indicates the currently displayed screen does not switch the screen.
7. Indicates unused switches for base screen switching.
8. Switches to the previously opened screen.
9. Switches the display language between three languages.
10. During logout: Displays the login window.
During login: Displays the confirmation window to select logging out or operator switching.

Remarks

- The operator authentication cannot be used for the security for restricting the utility startup. Therefore, this screen is provided in order to identify an operator who performs the utility function and to record it in the operation log file.
- When an operator logged out, [Base screen B-30001: Menu] is displayed. When an operator logged out while the utility function is used, the menu screen is displayed after the close of the utility screen.
- For the switches shown as [9], we have applied the setting that switches the system language in accordance with the display language.

4.4 Device List

Some of the devices specified to the on-screen switches and lamps, etc., are also used for common settings of functions such as scripts. Using [Batch Edit] is recommended to change these devices in a batch. For the details on [Batch Edit], please refer to "GT Designer3 (GOT2000) Screen Design Manual".

4.4.1 Controller devices

Type	Device No.	Application
Bit	None	
Word	None	

4.4.2 GOT internal devices

Type	Device No.	Application
Bit	GB61000 to GB61009	User alarm
	GB61101	Lamps for the medicine bottle filling line
	GS242.b0	Incorrect Login signal
	GS242.b1	Operator Locked signal
	GS522.b3	A control signal designated to restrict access to the operation log information
Word	GD60000	Base screen switching
	GD60021	Language switching
	GD60022	System language switching
	GD61000 to GD61009	Set value numerical input
	GD61100 to GD61101	Parts movement

4.5 Comment List

Comment Group No.	Comment No.	Base screen No.
499	No.1 to 12	B-30002 (User alarm observation ID 30001)
500	No.1 to 5	B-30001 to 30004
	No.6	B-30001 to 30004
	No.101 to 105	B-30001
	No.201 to 207	B-30002
	No.301 to 314	B-30003
	No.401 to 408	B-30004

4.6 Script List

Items	Settings
Project Script	No settings
Screen Script	B-30001
Object Script	No settings

4.6.1 Screen Script

Base screen 30001

Script No.	30000	Script Name	Script30000
Comment	Medicine filling line control		
Data type	Signed BIN16	Trigger Type	Sampling 1(second)
<pre>//This is a script for the menu screen which allows demo operation of a medicine bottle filling line. //GD61101: The parts position device on the bottle filling line //GB61101: The lamp display device on the bottle filling line if([w:GD61101] < 5){ [w:GD61101] = [w:GD61101] + 1; rst([b:GB61101]); }else{ [w:GD61101] = 1; set([b:GB61101]); }</pre>			

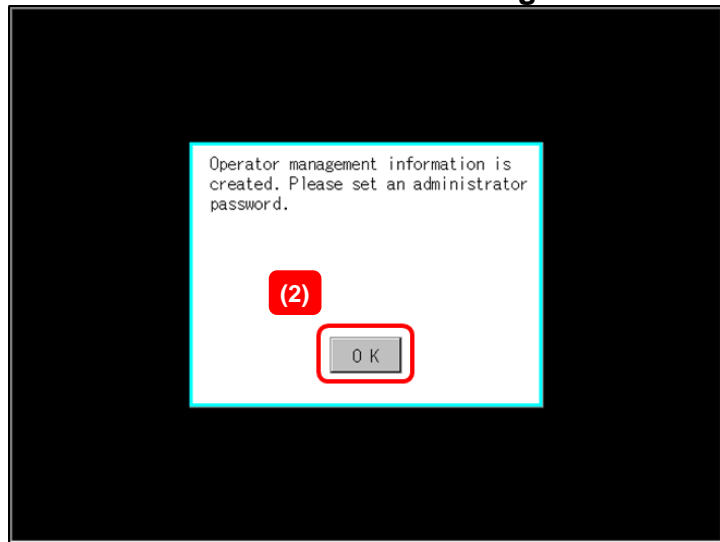
5. GOT RELATED SETTINGS FOR USING OPERATOR AUTHENTICATION

To use the operator authentication, some related settings on the GOT are needed, such as the administrator password setting, operator registration, and operator authentication function setting. After writing the project data into the GOT, make the settings with the steps shown below. You can skip the procedures for [5.2 Operator Registration] by saving the operator information file (AUTHINF.G2U *1) into the root directory of a SD memory card. For the details, please refer to [5.2 Operator Registration].

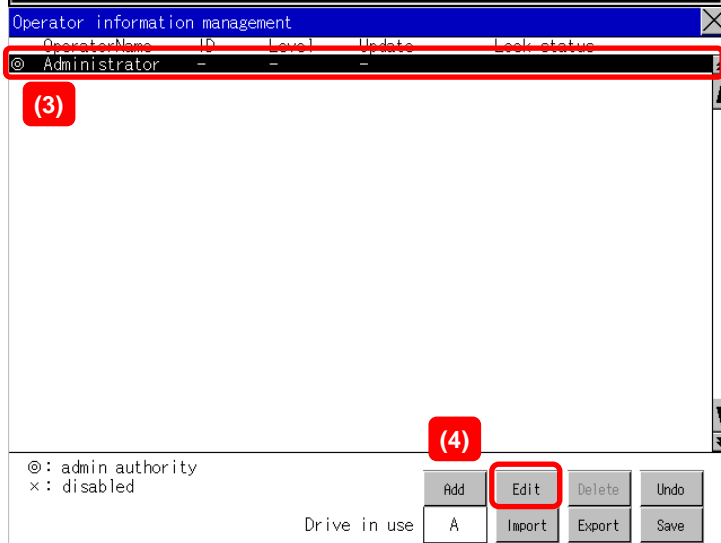
*1 : The operator information file is included in the below folder.

<The install path of the drawing software>\GTD3_2000\App\SampleProject\en-US\FDA21CFR Part11_V_Ver2

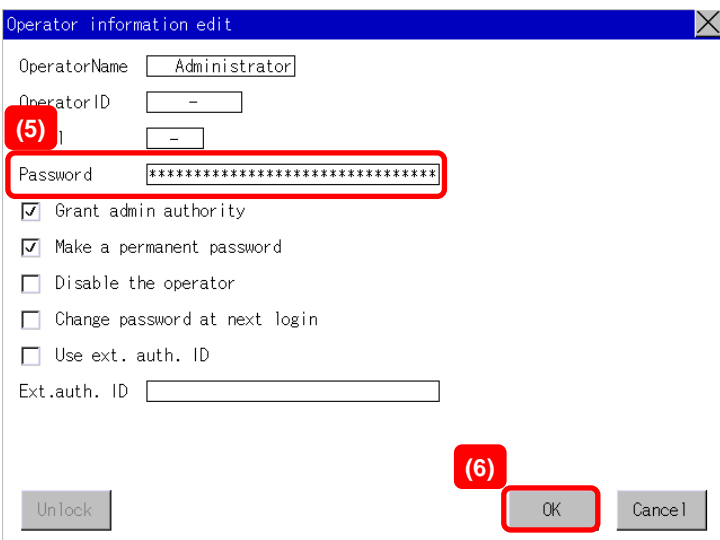
5.1 Administrator Password Setting



- (1) Write the project data into the GOT.
- (2) Touch [OK] in the message shown on the left.



- (3) Select [Administrator] in the [Operator information management] screen.
- (4) Touch [Edit].



- (5) Set a password in the [Operator information edit] screen.
Password: one-byte alphanumeric characters, space, or symbols (up to 32 characters)
- (6) Touch [OK].

Operator information edit

OperatorName Administrator

OperatorID -

Level -

Password ****

☒ Grant admin au

☒ Make a permane

☐ Disable the op

☐ Change passwor

☐ Use ext. auth.

Ext.auth. ID

The operator information editing process is completed.

OK

Unlock OK Cancel

(7) Touch [OK] in the message shown on the left.

Operator information management

OperatorName	ID	Level	Update	Lock status
Administrator	-	-	-	-

⊙: admin authority
×: disabled

Drive in use

Add Edit Undo

Import Export Save

(8)

(8) Touch [Save] in the [Operator information management] screen.

Operator information management

OperatorName	ID	Level	Update	Lock status
Administrator	-	-	-	-

⊙: admin authority
×: disabled

Drive in use

Add Edit Delete Undo

Import Export Save

The operator information saving process is completed.

OK

(9)

(9) Touch [OK] in the message shown on the left.

Caution: Do not touch [x] here.

The administrator password has been successfully set. Next, register an operator.

5.2 Operator Registration

After setting the administrator password, register an operator. In the sample screens, the switches for selecting the utility function are placed on the base screen with the security level 10. Therefore, make sure to set at least one operator who has the security level 10 or higher.

When you skip the procedures for [5.2 Operator Registration] by using operator information file (AUTHINF.G2U), please implement the procedure described below (*1). The operator information of level 10 and level 5, which are required for operation, are saved in the operation information file that is included in the folder.

(1) Touch [Add] in the [Operator information management] screen.

(*1) Touch [Import] in the [Operator information management] screen.

Below operators ID1 and ID2 will be registered upon import of the file.

ID1

Operator Name: Admin

Password : Admin

Level : 10

ID2

Operator Name: User

Password : User

Level : 5

(2) Set the followings in the [Operator information edit] screen.

Operator Name: one-byte alphanumeric characters, space, or symbols (up to 16 characters)

Level: 0 to 15

Password: one-byte alphanumeric characters, space, or symbols (up to 32 characters)

Grant admin authority: unchecked

Make a permanent password: unchecked

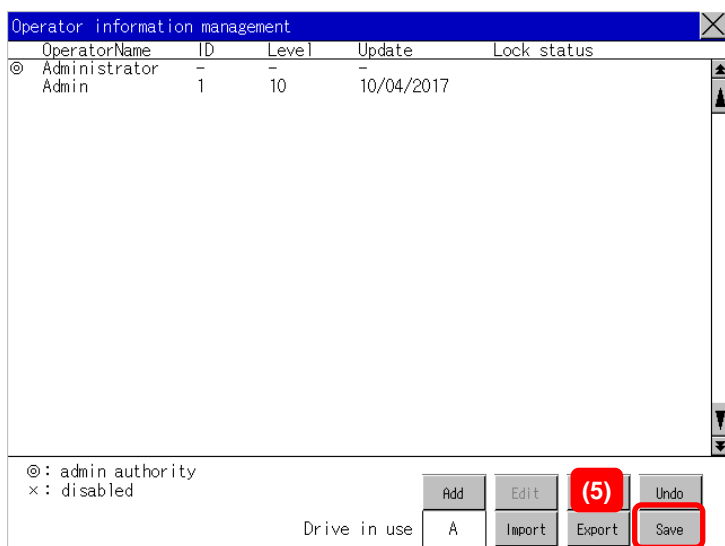
Disable the operator: unchecked

Change password at next login: unchecked

Use ext. auth. ID: unchecked

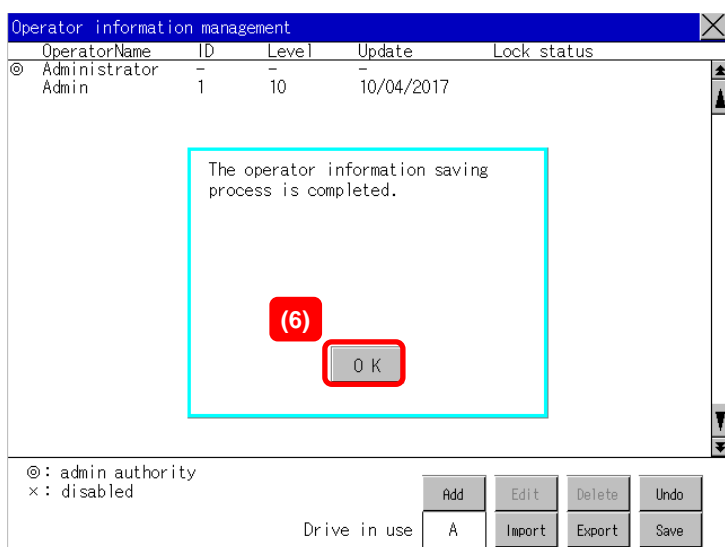
(3) Touch [OK].

(4) Touch [OK] in the message shown on the left.



(Repeat steps (1) to (4) to register two or more operators.)

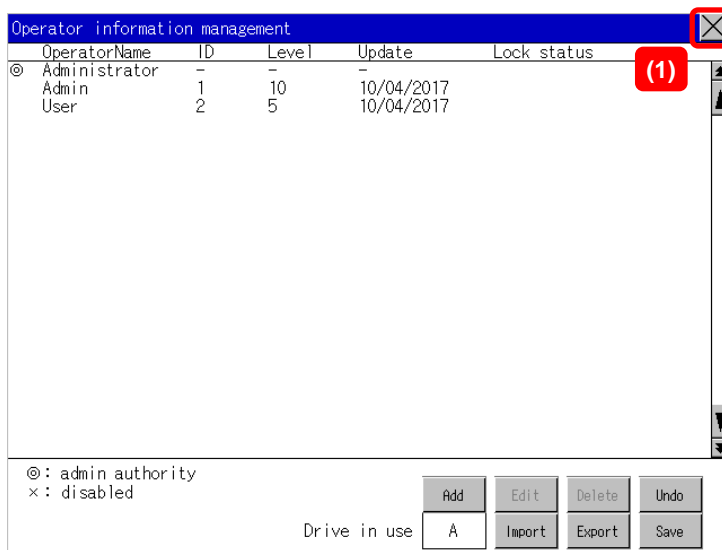
(5) Touch [Save] in the [Operator information management] screen.



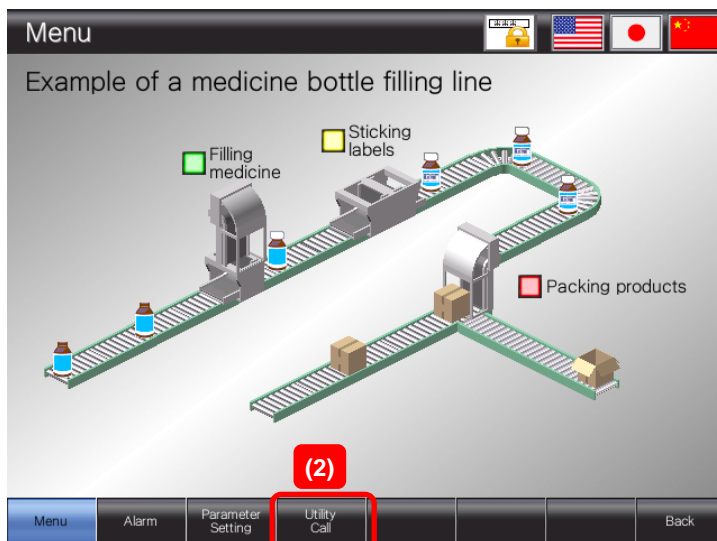
(6) Touch [OK] in the message shown on the left.

5.3 Function Setting for Operator Authentication

After registering an operator, make the function setting for operator authentication with the steps shown below.



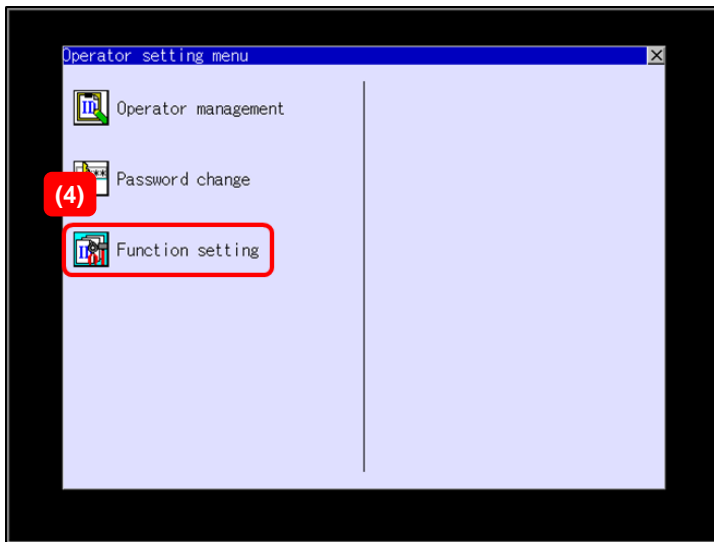
(1) Touch the close key [x] on the [Operator information management] screen.



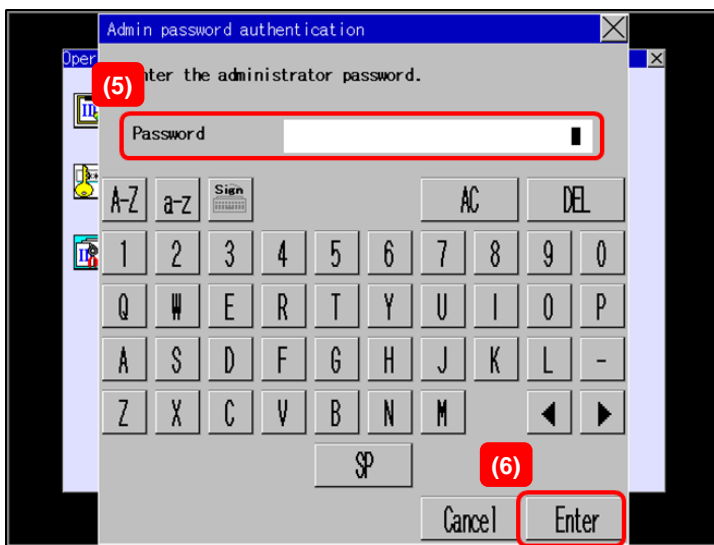
(2) Touch [Utility Call] on [Base screen B-30001: Menu].



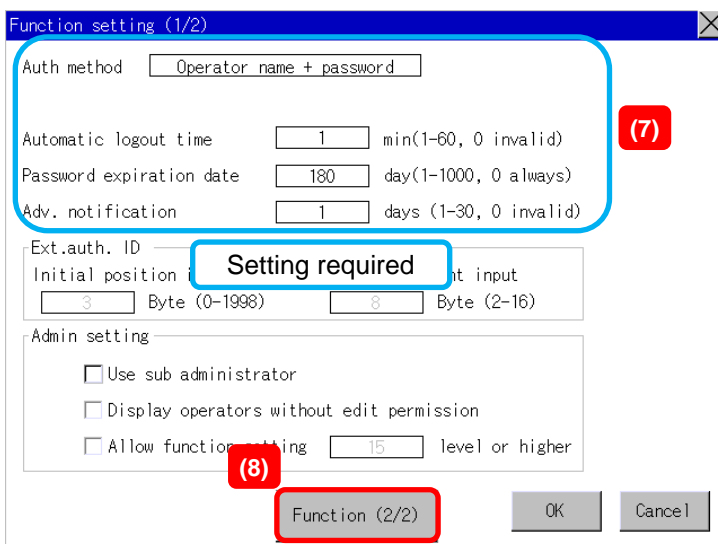
(3) Touch [Operator authentication] on [Base screen B-30004: Utility Call].



(4) Touch [Function setting] on [Operator setting menu].



(5) Input an administrator password.
(6) Touch [Enter].



(7) Set below in the [Function setting (1/2)] screen.

Authentication Method: Operator Name + Password

Auto Logout time : Other than 0

Password Expiration Date: Other than 0

Password Expiration Date: Other than 0

Password Expiration Prenotification : Other than 0

(8) Touch [Function Setting (2/2)].

Function setting (2/2) ✕

Upon login failure, prohibit login for a set period of time

Continuous failure count (3-10, 0 invalid)

Prohibition time s (1-3600)

Upon login failure, lock the operator (individually)

Continuous failure count (3-10, 0 invalid)

Set password requirement

☐ Check password

Set minimum length characters (1-32)

Set character type

(9)

(10)

Function (1/2)

(9) Set below in the [Function setting (2/2)] screen.

Login block (Recommended *1)

Operator lock (Recommended *1)

*1 Some settings are required to monitor the login block and operator lock by using the alarm function.

(10) Touch [OK] in the message shown on the left.

Function setting (2/2) ✕

Upon login failure, prohibit login for a set period of time

Continuous failure count (3-10, 0 invalid)

Prohibition time s (1-3600)

Upon login failure, lock the operator (individually)

Continuous failure count (3-10, 0 invalid)

Set password requirement

☐ Check password

Set minimum length characters (1-32)

Set character type

The function setting editing process is completed.

(11)

Function (1/2)

(11) Touch [OK] in the message shown on the left.

5.4 Precautions

In the sample data, we disabled the utility call key on the corner of the GOT screen. Instead of the utility call key, the switches for starting the utility are set on [Base screen B-30004: Utility Call] that has the security level 10. Therefore, make sure to register an operator who has the security level 10 or higher before closing the [Operator information management] screen that appears immediately after the project data is written into the GOT. If you close the [Operator information management] screen before registering an operator, you will be not able to switch to [Base screen B-30004: Utility Call], and accordingly, not to use the utility function. In addition, if you delete all the information of the operators who have the security level 10 or higher, and back to the user screen, you will be not able to switch to [Base screen B-30004: Utility Call], and accordingly, not to use the utility function.

If you back to the user screen without registering an operator who has the security level 10 or higher, press the [S.MODE] switch on the rear surface of the GOT while [Booting ...] is displayed on the upper left corner of the screen after the GOT power-on. Then, the utility main menu will be displayed. Select [GOT basic setting] - [Operator authentication] - [Operator management], and register an operator.

6. OPERATION LOG SETTING

Select [Common] - [GOT Environmental Setting] - [Operation Log], and make a check in the [Collect operation logs] box. Then, make a setting for operation log using the example shown below.

6.1 Basic Tab

The screenshot shows the 'Basic Tab' of the 'Operation Log Setting' window. The 'Basic' tab is selected, and the 'Log Target' and 'File Conversion' tabs are also visible. The 'Save to' dropdown is set to 'A:Standard SD Card'. The 'Folder Name' is 'Package1\OPELOG'. The 'File Name' is 'OPELOG' followed by a date-time suffix '_yyyymmdd_ssss.G2O'. The 'Status Notification' section has a checkbox for 'Notify the operation log status' which is unchecked. The 'Log File Switching Mode' section has 'Switching Mode' set to 'Daily' and 'Switching Time' set to '0 Hrs 0 Min'. The 'Log File Retention Period' is set to '7 Days'. The 'Log File Size' section has a checkbox for 'Specify the total log file size' which is unchecked, and the 'Behavior when memory card runs out of space' is set to 'Delete existing logs and continue to collect logs'. A red box highlights the 'Delete existing logs and continue to collect logs' dropdown. A 'Setting required' callout points to the 'Save to' dropdown.

Save to: A:Standard SD Card

Folder Name: Package1\OPELOG

File Name: OPELOG _yyyymmdd_ssss.G2O

Status Notification

☐ Notify the operation log status:

Log File Switching Mode

Switching Mode: ☒ Daily ☐ Weekly

Switching Time: 0 Hrs 0 Min

Log File Retention Period: 7 Days

Log File Size

☐ Specify the total log file size: 10 (MB)

Behavior when memory card runs out of space: Delete existing logs and continue to collect logs

☒ Display the screen image when using operation logs

Select [Delete existing logs and continue to collect logs] for [Behavior when memory card runs out of space]. The log file will be deleted when the days specified for [Log File Retention Period] have elapsed. Make sure to back up the log file before it is deleted.

6.2 Log Target Tab

Basic

Log Target

File Conversion

Setting required

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

Select >

< Delete

Select All

Delete All

Operation Log Target:

Application Switching

Screen Switching

Operator Authentication

Operator Management

Time Change (Clock Setting and GS Change)

Time Change (Change from Utilities)

Functional Operation Security Authentication

Object

Description:

Logs of switching time, function abbreviation, function type name, switched language, etc. will be collected after system language is switched.

☒ 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

As the log target, select [Application Switching], [Screen Switching], [Operator Authentication], [Operator Management], [Time Change (Clock Setting and GS Change)], [Time Change (Change from Utilities)], [Functional Operation Security Authentication], and [Object].

In order to record before-change values when you change the value using the touch switch, make a check the [Collect previous device values at the time of touch switch operation] box.

When you use the GOT Mobile function, make a check in the [Collect operation logs of clients being connected to the server of GOT Mobile function] box.

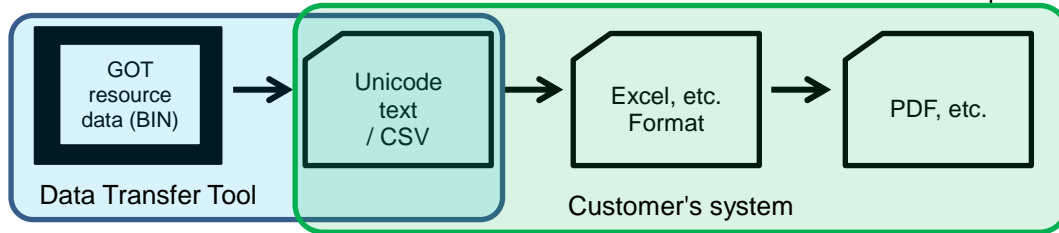
6.3 File Conversion Tab

Since the resource data should be saved in the binary file only, make sure not to change the setting for file conversion. To convert the binary file into the Unicode text or CSV file, please refer to "7.1 Convert Binary File into Unicode Text/CSV File".

7. RESOURCE DATA (DATA GENERATED ON GOT)

7.1 Convert Binary File into Unicode Text/CSV File

In the sample data, the resource data is saved in the binary format. To convert the data into Unicode text or CSV format, use the Data Transfer Tool. The Data Transfer Tool has a command for converting the resource data and a programming API. Please configure your systems or tools for converting the data into formats (PDF, etc.) that prevent the automatic falsification with no need for the Unicode text file or CSV file as an intermediate product.



Install the Data Transfer Tool using an installer in the [DataTransfer] folder which is stored below the [Disk4] folder in MELSOFT GT Works3 DVD-ROM or the [Disk5] folder in MELSOFT iQ Works DVD-ROM (Disc3).

For how to use the Data Transfer Tool, please refer to [Help For Data Transfer Tool] in the "got-data-trans-o-e.pdf" file in the installed folder "Program Files\MELSOFT\Datatransfer".

The following describes brief procedures for reading of resource data and file conversion with command lines.

(1) Setting of environment variables

In order to execute an operation by directly inputting a command name in a command prompt, select environment variables (PATH) for the folder of Data Transfer Tool.

- Select [Start] - [Control panel] - [System and Security] - [System] on the personal computer.
- Select [Advanced system settings], and click the [Environment Variables] button.
- Select [Path] in [System variables], and click the [Edit] button.
- Add a path to a variable value. There shall be an executable file in the path.

Example) C:\Program Files\MELSOFT\DataTransfer

(To set two or more paths, place ; (semi-colon) between paths.)

(2) Reading of resource data

Example) Read all of the resource data saved in drive A of the GOT, and save the data in the "C:\TEST" folder of the personal computer.

DtComm2000 /resourceup /Drv A /Dest C:\TEST all

Example) Read the resource data "OPELOG_20160121_0011.G2O" in "A:\Package1\OPELOG" of the GOT, and save the data in the "C:\TEST" folder on the personal computer.

DtComm2000 /resourceup /Drv A /Dest C:\TEST \Package1\OPELOG\OPELOG_20160121_0011.G2O

(3) Conversion of resource data

Example) Convert "C:\TEST\Package1\OPELOG\OPELOG_20160121_0011.G2O" of the personal computer into the CSV file.

rcconv2000 C:\TEST\Package1\OPELOG\OPELOG_20160121_0011.G2O CSV

Example) Convert "C:\TEST\Package1\OPELOG\OPELOG_20160121_0011.G2O" of the personal computer into the Unicode text file (English).

rcconv2000 C:\TEST\Package1\OPELOG\OPELOG_20160121_0011.G2O TXT ENG

7.2 Transfer to Database using MES Interface

The resource data can be saved in a database using a MES interface. For how to use the MES interface, please refer to "GOT2000 Series MES Interface Function Manual For GT Works3 Version1".

8. PROJECT DATA PROTECTION

8.1 Data Transfer Security

It is recommended to set the data transfer security to prevent the project data in the GOT from being falsified. Select [Common] - [GOT Environmental Setting] - [Security], make a check in the [Update Data Transfer Security] box in the [Data Transfer Security] tab. Then, set a password for data transfer. Make sure not to forget your password since the password cannot be confirmed.

8.2 Project Security

Registering a user for the project data allows only the registered user to open the project data. In addition, a user access level enables the restriction in displaying or editing the project data. It is recommended to strengthen the user management in order to prevent the falsification of project data.

8.3 Project Verification

The project verification provides the check of differences between the project data in the GOT and that in the personal computer. The falsification of data can be easily checked by verification.