

MKXXxxx Internal Flash Memory Instructions Manual

DTS INSIGHT CORPORATION

- (1) No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the written permission of DTS INSIGHT CORPORATION.
- (2) The contents of this manual are subject to change without prior notice due to improvement of the functionality.
- (3) If any question about the contents of this manual arises, contact DTS INSIGHT CORPORATION.
- (4) DTS INSIGHT CORPORATION shall not be held responsible for direct or indirect adverse effects resulting from operation of this system irrespective of the above item (3).
- (5) Product and company names mentioned in this manual are the trademarks of their respective owners.

© 2013 DTS INSIGHT CORPORATION. All Rights Reserved.

Printed in Japan

Revision History

Edition	Date of issue	Description
1st Edition	January 31, 2013	<ul style="list-style-type: none">• Initial publication
2nd Edition	July 1, 2013	<ul style="list-style-type: none">• MK70FN1M0V is supported.• Supported version table is modified.
3rd Edition	August 23, 2013	<ul style="list-style-type: none">• FlexMemory is supported.• K60/K70 group is supported.
4th Edition	April 4, 2014	<ul style="list-style-type: none">• K10/K20/K30/K40/K50 group is supported.

Contents

1	Introduction	5
2	Supported Install Kit CDVersions.....	6
3	Advance Preparation	7
3.1	When Flash Security is valid.....	7
3.2	When Correct Address is not set in the Vector Table.....	7
3.3	Settings for when ETM is disabled	8
3.4	Allocation of DataFlash	9
4	Setting the Memory Mapping	10
4.1	Setting up Flash Memory Mapping.....	10
4.2	Setting up User RAM for ICE.....	12
5	Erase the Flash Memory.....	13
6	Download to Flash Memory	14
7	Software Break in Flash Memory.....	15
8	MPU-Specific Settings	16
8.1	RESET.....	16
8.2	Others.....	18
9	Notes & Points.....	19
9.1	Flowchart of Action on Error	19
9.1.1	Security Error	19
9.1.2	Setting Error of Flash Definition File (.frd).....	21
9.2	Watchdog Timer (WDT)	22
9.3	Flash Protection	22
9.4	Software Break in the Internal Flash Memory.....	22
9.5	Swap Function.....	22

1 Introduction

This is a brief manual for writing to on-chip flash memory.

For details of ICE operating instructions, see the microVIEW-PLUS User's Manual (Common Edition) and microVIEW-PLUS User's Manual (MPU-Specific Edition).

2 Supported Install Kit CDVersions

Device Model	Supported Versions	
	SLX600	ZX600
All Series	3.01	1.04

3 Advance Preparation

3.1 When Flash Security is valid

The ICE cannot be connected if flash security is valid. In case the following error occurred, see Section 9.1 “Flowchart of Action on Error”.

“ICE Error No.fe6: Flash Security is valid. The ICE cannot be connected.
In such cases, release the break setting, and then erase the symbol registration. After that turning on the Forced unsecured/unprotection on the MPU-specific setting [RESET] dialog box, and then reset the system.

* Please be aware that all data in the internal flash memory is cleared by forced-release.

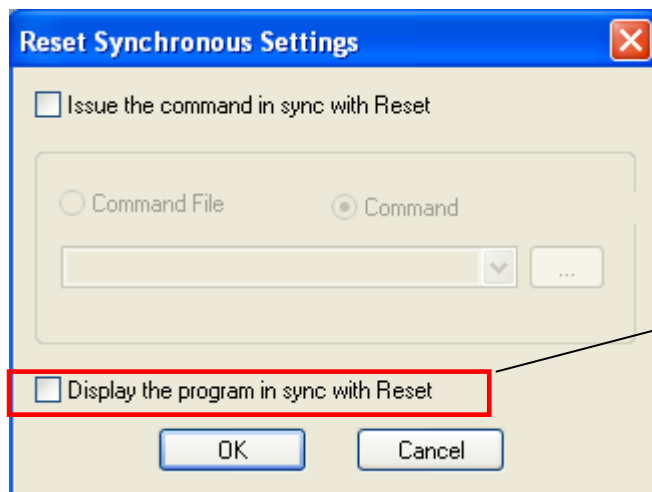
3.2 When Correct Address is not set in the Vector Table

microVIEW-PLUS dumps a reset vector area to display a program (disassemble display) after connecting by reset commands.

If the vector table is in erase (0xFFFFFFFF), 0xFFFFFFFFE will be dumped and “ICE Error No.f58: Sticky error” may occur.

[Provision]

Right-click the Reset button on the toolbar, and then open the Reset Synchronous Settings dialog box.



Clear the “Display the program in sync with Reset” check box.
(= does not dump by the reset command)

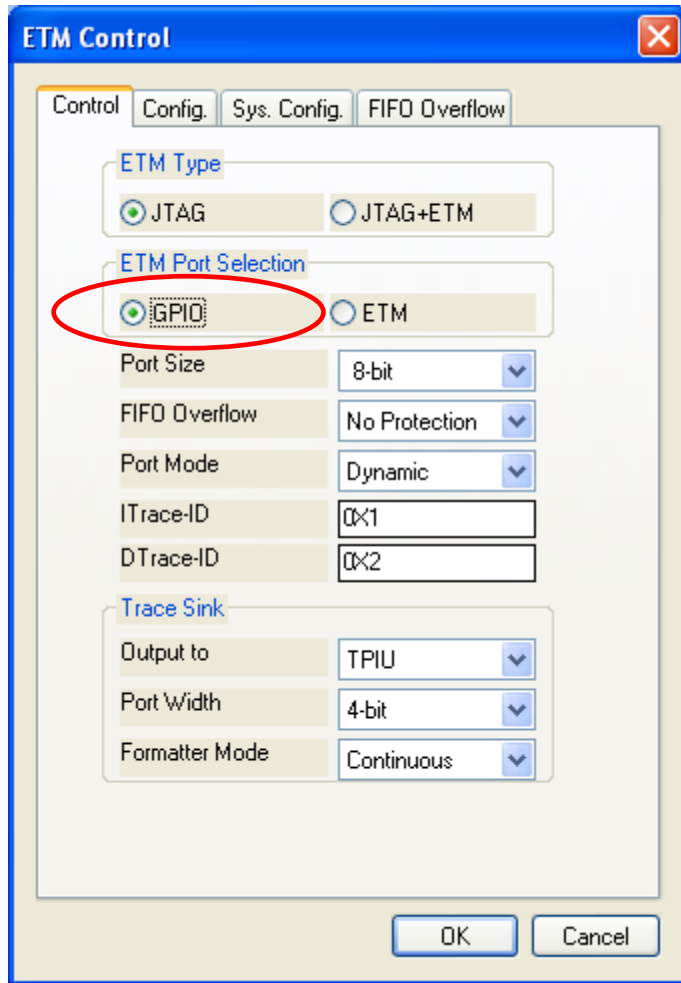
After downloading the program to the internal flash memory (correct vector table values are written), select this check box again.

3.3 Settings for when ETM is disabled

(When “ETM Type” setting is “JTAG”, this setting is unnecessary.)

When the ETM setting of the board is invalid, please set “GPIO” for “ETM Port Selection”.

MPU → ETM Control



3.4 Allocation of DataFlash

For devices with FlexMemory, if you want to download data into DataFlash, you need to set a size of DataFlash.

Set the size of DataFlash by using a program partition command. *1

Note:

Initialization of DataFlash size by block erase or mass erase is necessary to change the DataFlash size.

Please be noted that all memory area is erased by mass erase.

To do mass erase, select the security/protection forced-release on the MPU-specific setting dialog box.

For details, see Section 8.1 "RESET".

*1: Example: When FlexNVM size is 256 MB, and set 128KB for DataFlash

```

mem b 0x40020007 = 0x80;      # FCCOB0 register
mem b 0x40020006 = 0x00;      # FCCOB1 register
mem b 0x40020005 = 0x00;      # FCCOB2 register
mem b 0x40020004 = 0x00;      # FCCOB3 register
mem b 0x4002000b = 0x09;      # FCCOB4 register (EEPROM Data Size Code)
mem b 0x4002000a = 0x05;      # FCCOB5 register (FlexNVM Partition Code)
mem b 0x40020000 = 0x80 off;  # FSTATregister

# Check if the size setting of DatFlash is completed without error.
eval $a = 0x80 ;# Value of FTFE_FSTAT at when setting is completed successfully.
for($c=0;$c<100;$c++){
    eval $b = *(char *)0x40020000 ;      # FTFE_FSTAT register
    eval $b &= 0xF0
    if($a == $b){
        endloop
    }
}
if($a == $b){
    echo setting OK!;      # Setting is OK
}
else{
    echo setting error;    # Setting is NG. Check the setting value of each register of command.
}

```

Copy and paste the above texts and create a file with extension .mvw. You can use it as a script.

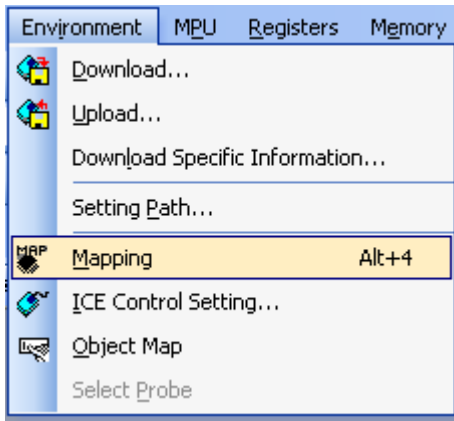
Change the register value of FCCOB4 and FCCOB5 according to the used EEPROM Data Size and FlexNVM Partition Code.

For details of each register value, see manuals of chip.

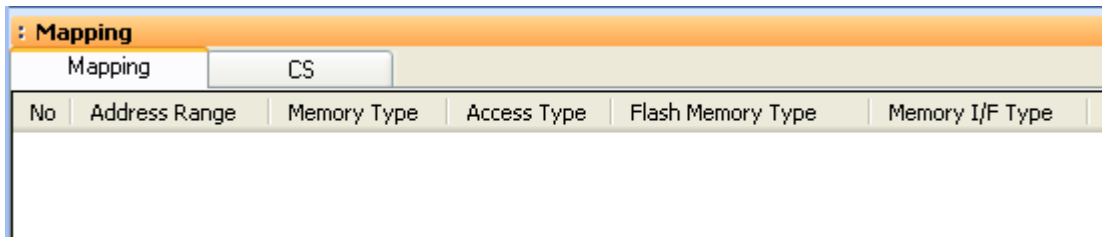
4 Setting the Memory Mapping

4.1 Setting up Flash Memory Mapping

Open the memory mapping window by clicking **Environments – Mapping**.

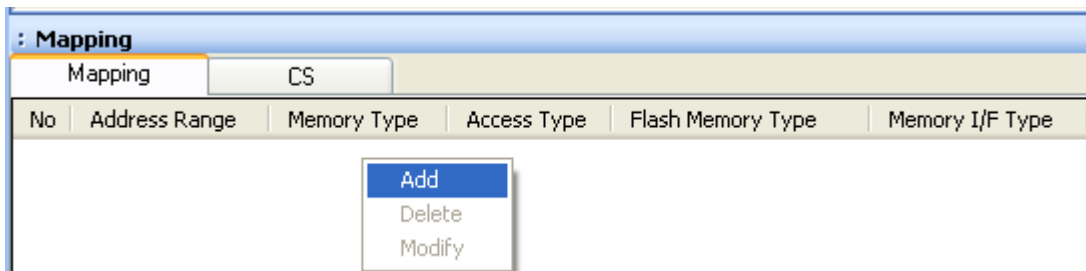


Memory map window as below is opened.

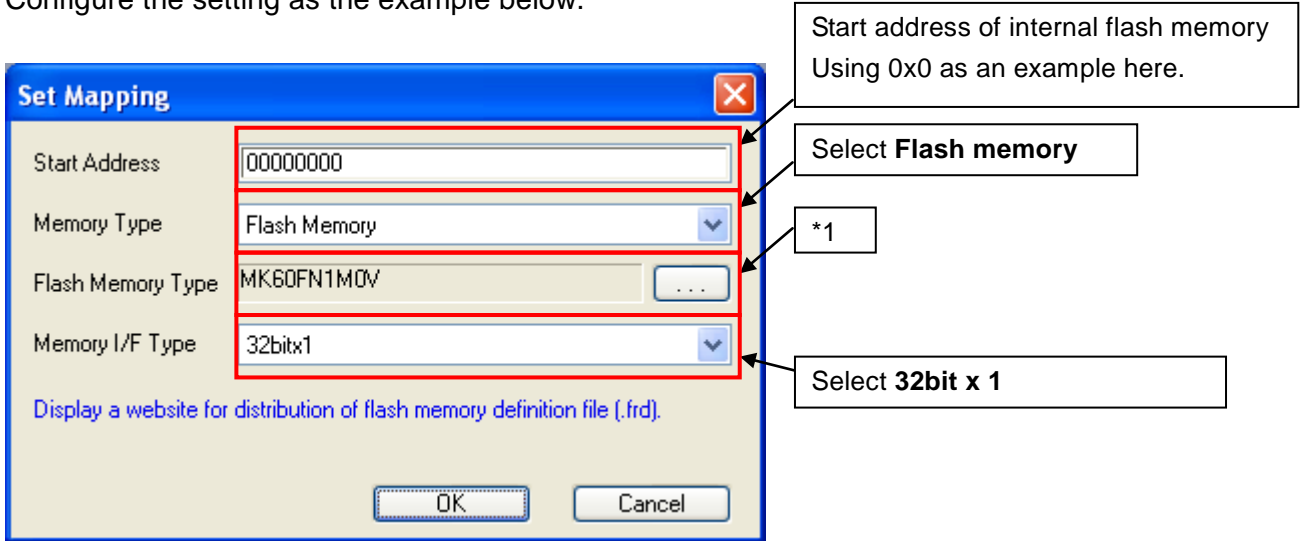


Set the mapping.

Right-click on the memory mapping window, and then select **Add**.



Configure the setting as the example below.



* Select the flash memory definition file (.frd) in accordance with your flash memory.

If you use FlexNVM as DataFlash, you need to set a mapping for DataFlash in addition to a mapping setting for ProgramFlash.

File name of [Flash memory programming definition file (frd)] for DataFlash is configured by the following rule. Please select the file suitable for your environment.

[FLEXNVM <whole size of FlexNVM>_DATA<Size, allocated for DataFlash>.frd]

Example for when the device is MK60DX256VMC10, and 128KB is set for DataFlash:

ProgramFlash

Start address: 0x00000000

Memory type: MK60DX256V.frd

Memory I/F type: 32bit x 1

DataFlash (FlexNVM)

Start address: 0x10000000

Memory type: FLEXNVM256KB_DATA128KB.frd

Memory I/F type: 32bit x 1

Specify the whole size of FlexNVM

Specify the DataFlash size you have set

Mapping						
Mapping		CS				
No	Address Range	Memory Type	Access Type	Flash Memory Type	Memory I/F Type	
0	00000000-0003FFFF	Flash Memory	---	MK60DX256V	32bitx1	
1	10000000-1001FFFF	Flash Memory	---	FLEXNVM256KB DATA128KB	32bitx1	
2	20000000-2000FFFF	User RAM for ICE	---	---	64KB	

4.2 Setting up User RAM for ICE

You can increase a download speed for flash memory by mapping a user RAM for ICE.

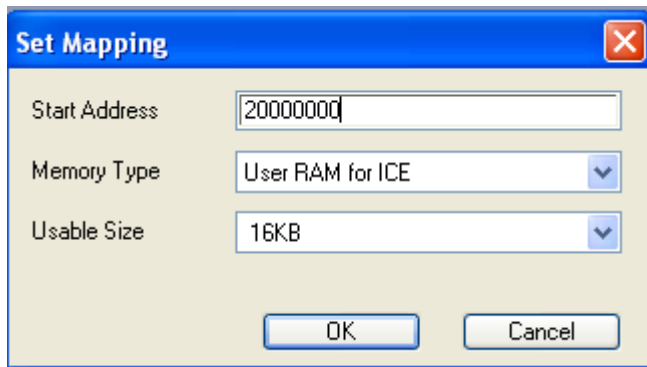
You can download the data to flash memory without the mapping setting though.

In such cases, make sure to execute the Reset command right before downloading.

For User RAM for ICE, specify an area where ICE can occupy.

The following example is for when setting 16KB from 0x20000000.

For the actual settings, refer to the Soc memory map of yours.



5 Erase the Flash Memory

For details, see the microVIEW-PLUS User's Manual (MPU-Specific Edition).

Details of memory mapping settings are described on this manual. Please refer to microVIEW-PLUS User's Manual (MPU-Specific Edition) for other contents.

Note:

If you erase the flash configuration field (0x400 to 0x40F) when "Invalid" is selected for [Force Setting at Downloading] on the MPU-specific setting [Others] dialog box, the flash security becomes secure. The connection with ICE is disabled if you reset the system with this condition.

If you cannot connect the ICE, see Section 9.1 "Flowchart of Action on Error".

6 Download to Flash Memory

For details, see the microVIEW-PLUS User's Manual (MPU-Specific Edition).

Details of memory mapping settings are described on this manual. Please refer to microVIEW-PLUS User's Manual (MPU-Specific Edition) for other contents.

Note:

- (1) Please be aware of the followings if you download data to the flash configuration field (0x400 to 0x40F).
 1. If you download data that secures the flash security when "Invalid" is selected for [Force Setting at Downloading] on the MPU-specific setting [Others] dialog box, the connection between ICE and user system becomes disconnected when you reset the system.
If you cannot connect the ICE, see Section 9.1 "Flowchart of Action on Error".
 2. If you download data protecting the flash protection when other than the "Forced unsecured/unprotection" is selected for [Force Setting at Downloading] on the MPU-specific setting [Others] dialog box, you cannot erase or download data to the target flash memory area. You can't do the software break on the target flash memory area also.
 3. Make sure to download MEEN bit (bit[5:4]) of flash security by switching it to b'11 (value which enables mass erase).
- (2) In case the "ICE Message No.1e41: Flash memory device protection error" occurred, see Section 9.3 "Flash Protection".
- (3) If the following abnormal end occurs, please download data without setting the user RAM for ICE or execute the reset command right before the download.
 - Detection of reset by the watchdog timer reset
 - Errors other than erase error or verify error
- (4) If you need to download data without setting the user RAM for ICE, execute the reset command right before the download.

7 Software Break in Flash Memory

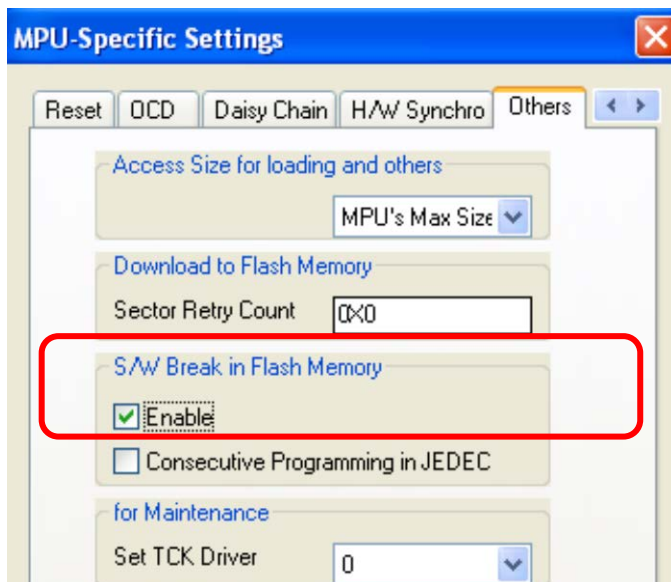
For details, see the microVIEW-PLUS User's Manual (MPU-Specific Edition).

Details of memory mapping settings are described on this manual. Please refer to microVIEW-PLUS User's Manual (MPU-Specific Edition) for other contents.

You are not allowed to set up software break in the flash memory in the initial state. In case you try to set up software break in the flash memory with the disabled status, it results in the following error.

"ICE Error No. 8c4: Set Software Break Verify Error".

To enable software break setting for flash memory, select the **Enable** check box of S/W Break in Flash Memory on the Others tab of the MPU-Specific Settings dialog box.



Note:

- (1) Software break to the flash configuration field (0x400 to 0x40F) is not allowed. If you set it, the following error occurs:

"ICE Error No.f2d2: Not the program area. Software break cannot be set."

- (2) If "ICE Message No.1e41: Flash memory device protection error" occurred, see Section 9.3 "Flash Protection".

8 MPU-Specific Settings

This chapter explains about MPU-specific settings for internal flash memory. For details on other MPU-specific settings, see the microVIEW-PLUS User's Manual (MPU-specific Edition).

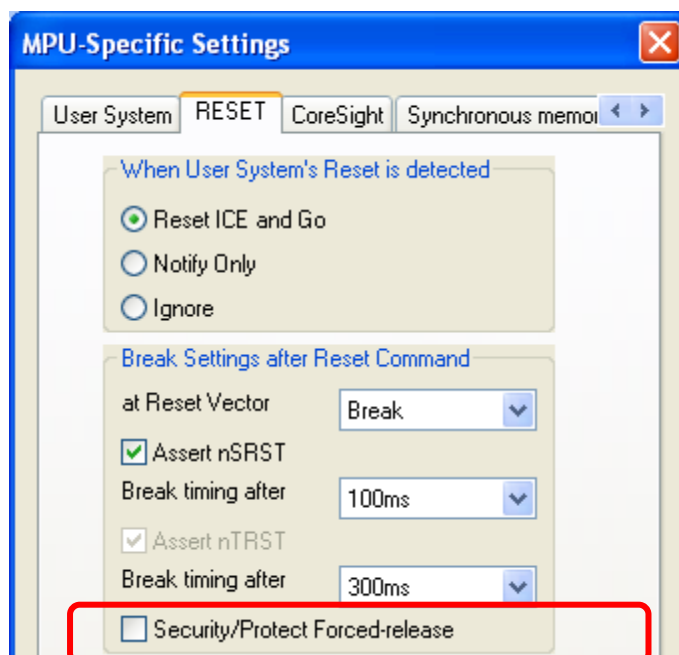
To set up MPU-specific settings, click on MPU menu, and then click the MPU-specific settings. Then, the MPU-specific settings window will be opened.

8.1 RESET

Security/Protect Forced-release

For Kinetis products family, you can disable the debug port or protect to not write or erase the memory by using the setting of flash security byte and flash protection byte within the internal flash memory.

By using this setting, you can control whether to forcibly release the security or protection by reset command. Make sure to execute the reset command after the setting.



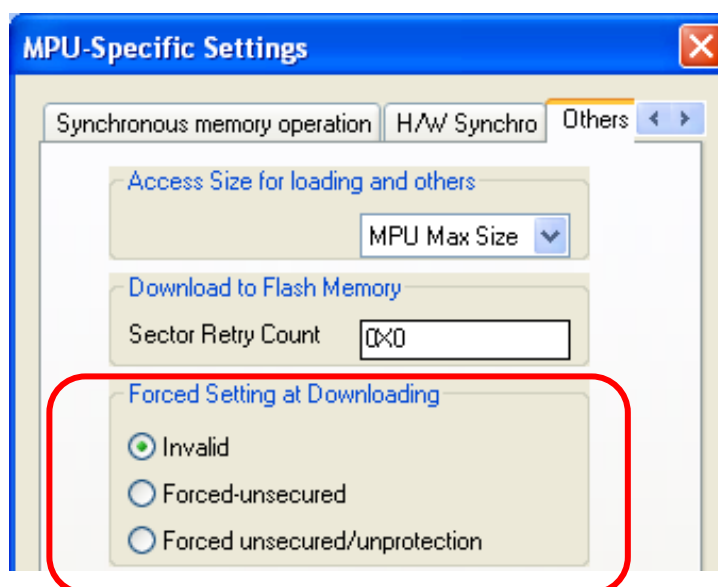
Uncheck the check box	ICE cannot be connected if a secured device is detected. (Default)
Select the check box (*1) (*2)	<p>Forcibly releases the security or protection when executing the reset command.</p> <p>The selection is automatically cleared after the completion of reset command.</p> <p>It does mass erase (erase all data within internal flash) when releasing. Therefore all data, including Swap, Data Flash/EEPROM area settings is erased.</p> <p>Delete the symbol registration by releasing all break settings before executing the reset command.</p>

- *1: Make sure to connect nSRST signal to ICE connection connector on the user system, because nSRST is involved with mass erase (deleting all data in the internal flash) which is operated when releasing the security. For details about connection, see the adviceLUNA User's Manual (MPU-Specific Edition). If you clear the nSRST assert checkbox, Flash Security may not be released.
- *2: For Kinetis K Series, there is a swap function which is able to switch the mapping of flash memory which is divided in two parts. If you do this operation while swap is valid, it is secured again after releasing the swap, so in such cases, select this check box and execute the reset command **twice in a row**.

8.2 Others

Forced Setting at Downloading

Controls whether to download data by switching it to data without the security or protection when downloading or erasing data in the sector/block containing the flash security byte or flash protection byte within the internal flash memory.



Invalid (*1)	If there are sectors or blocks containing the flash security byte (0x40C) in the download target area, switch MEEN bit (bit[5:4]) to b'11 (a value not disabling the mass erase). Other than that, data specified when downloading is written. (Default)
Forced-unsecured (*1)	If there are sectors or blocks containing the flash security byte (0x40C) in the download target area, switch data to values to not become secure state.
Forced unsecured/unprotection (*1)	If there are sectors or blocks containing the flash security byte (0x40C) in the download target area, switch data to values to not become secure state. If there are sectors or blocks containing the followings in the download target area, switch the data to values to not become protection state. <ul style="list-style-type: none"> • Program Flash Protection Byte (0x408 to 0x40B) • Data Flash Protection Byte (0x40F) • EEPROM Protection Byte (0x40E)

*1 adviceLUNA downloads switched values, not the original data. Please be aware this point when debugging the program of ROM sum check.

9 Notes & Points

9.1 Flowchart of Action on Error

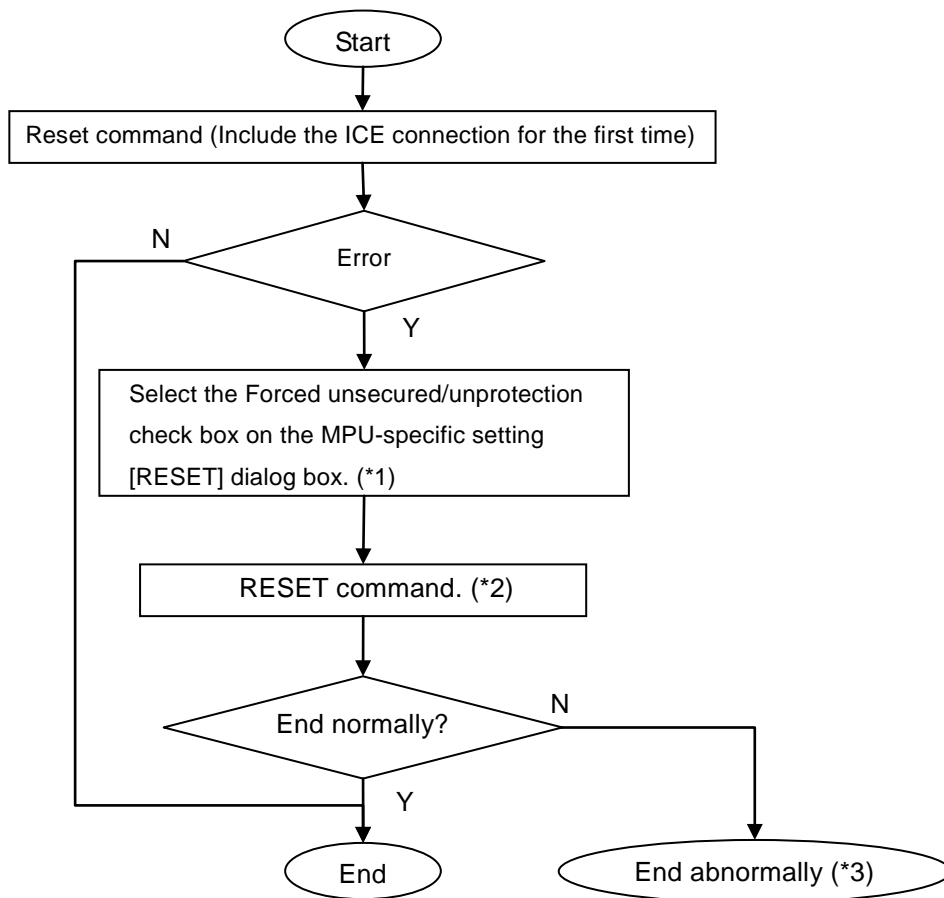
9.1.1 Security Error

The ICE cannot be connected if flash security is secured. In case the following error occurred, the flash security may be secured. See the flowchart below and take an action for error.

“ICE Error No.fe6: Flash Security is valid. The ICE cannot be connected.
In such cases, release the break setting, and then erase the symbol registration. After that turning on the Forced unsecured/unprotection on the MPU-specific setting [RESET] dialog box, and then reset the system.

* Please be aware that all data in the internal flash memory is cleared by forced-release.

Make sure to connect nSRST signal to ICE connection connector on the user system, because nSRST is involved with mass erase (deleting all data in the internal flash) which is operated when releasing the security. For details about connection, see the adviceLUNA User's Manual (MPU-Specific Edition).



Flowchart of Action on Error

*1 If you select this check box and execute the reset command, regardless of the security/protection state at that time, ICE does mass-erase (deleting all data in the internal flash) of internal flash memory.

*2 It does mass erase (deleting all data in the internal flash) when releasing. Therefore all data, (including Swap, Data Flash/EEPROM area settings) is deleted. Delete the symbol registration by releasing all break settings before executing the reset command.

*3 The following error occurs:

“ICE Error No.fe7: Mass erase is disabled, and flash security is secured.
The device with this state cannot be connected because the security cannot be released by ICE. Please contact a dealer of the device or board.

9.1.2 Setting Error of Flash Definition File (.frd)

Setting of the flash definition file (.frd) may be wrong if the following error occurred.

*ICE Error No.ffc: Specification of flash memory type is not correct.
Select the correct flash memory type by using the mapping setting.

Check the followings:

- When an error occurred when downloading to ProgramFlash:
Flash definition file suitable for the device is not set.
Set a flash definition file based on the device name.

- When an error occurred when downloading to DataFlash
Check the value of DEPART of Flash Configuration Register 1.
 - If the value of DEPART is "0xF"
DataFlash size may not have been set.
Set it by Program Partition command.
* The setting example is described on Section 3.4 "Allocation of DataFlash".

 - If the value of DEPART is other than "0xF"
DataFlash size that is set by program partition command and DataFlash size that is specified by the flash definition file are not conformed.
Set the flash definition file in accordance with the DataFlash size set by DEPART.
* For details on how to set the flash definition file, see Section 4.1 "Setting up Flash Memory Mapping".

9.2 Watchdog Timer (WDT)

You can write in the flash memory even if WDT (Watchdog Timer) is enabled.

WDT is temporarily disabled by an internal process of ICE while the flash memory is written. (After the writing, it is automatically restored.) Do not enable the WDT on the debug mode.

9.3 Flash Protection

You cannot set the erase, download or software-break in the flash area protected by flash protection.

*ICE Error No.1e41: Flash memory device protection error occurs.

If the flash configuration field (0x400 to 0x40F) is protected, turn on the Forced unsecured/unprotection on the MPU-specific setting [RESET] dialog box to release the protection. After that, reset the system.

9.4 Software Break in the Internal Flash Memory

Software break to the flash configuration field (0x400 to 0x40F) is not allowed. If you set it, the following error occurs:

“ICE Error No. fd2: Not the program area. Software break cannot be set.”

9.5 Swap Function

ICE does not follow up the setting of Swap of Kinetis. If you need to use Swap function, disable all features which require address information (such as event, break, and symbol information set in the swap area). After that, do the swapping. The debug operation after the swapping may become abnormal if you skip this setting.

If you need to do the swapping, download the data which does not secure a flash security byte (offset +0x40c) of the inactive block in advance.

If you do Forced unsecured/unprotection while swap is valid, it is secured again after releasing the swap, so in such cases, select the Forced unsecured/unprotection check box and execute the reset command **twice in a row**.