

GigaDevice Semiconductor Inc.

**Precautions for
GD32H77x_H78x_BootLoader Operations**

Application Note

AN298

Revision 1.1

(Oct. 2026)

Table of Contents

Table of Contents	2
List of Tables	3
1. Overview	4
2. Option byte operation	5
2.1. DCRP operation	5
2.2. SCR operation	6
2.3. SCR and DCRP concurrent operation	8
3. OTP operation	9
4. SDIO interface	10
5. USB interface	11
6. OSPI interface	12
7. Revision history	13

List of Tables

Table 7-1. Revision history.....	13
----------------------------------	----

1. Overview

The GD32H77x_H78x's BootLoader supports three types of communication interfaces, USART, USB and SDIO. Different interfaces require different hardware support, USART interfaces have 3 ports, USART0 (PA9, PA10), USART1 (PA2, PA3) and USART2 (PB10, PB11) can be used; USB interface has only 1 port, USBHS0 (USBHS0_DP, USBHS0_DM); There is only 1 SDIO interface, SDIO0 (PC12, PD2, PB13, PC9, PC10, PC11). The basic operation of these interfaces will not be detailed here, you can refer to the relevant user manual. This mainly describes the operation of some special option bytes or OTPs in GD32H77x_H78x to prevent customers from misoperation and causing chip locking.

Note: This application note is for reference only. In case of any conflict with the user manual or datasheet, the user manual or datasheet shall prevail.

2. Option byte operation

The GD32H77x_H78x option bytes are mainly implemented by modifying the relevant registers, each register is divided into 2 groups (EFT registers, MDF registers), users can only modify MDF registers, please refer to the [GD32H77x_H78x User Manual](#). The following describes the options to which need attention to paid when operating BootLoader.

2.1. DCRP operation

The DCRP region is set in NVMC_DCRPADDR_MDF, and its active region is distributed in 3 memory region segments, namely CNVM region, ECNVM BANK0 and BANK1 region. The effective DCRP region must ensure that the start address must be less than the end address, and this area can be expanded outward but not inward, please refer to the [GD32H77x_H78x User Manual](#) for details. Customers can clear the original region and reset the new region. DCRP localization and clearing are not very direct operations and require certain operation procedures to complete. The configuration and clear process is as follows:

DCRP area configuration process:

1. First, set the enabling bit xxx _DCRP_EN 1 of the DCRP region segment, which can be CNVM, ECNVM BANK0 or BANK1.
2. The start and end bits of the DCRP region are usually set to be less than the end bits, and if the two bits are equal, the entire area segment will be set as the DCRP protected area.

After the above two steps are completed, the DCRP area configuration is completed. The following points need to be noted:

1. User can configure multiple region segments at the same time, but each region segment uses the same start and end address.
2. After DCRP region protection, the data can be read, but the data is all 0, which is the same as the default value of CNVM.
3. After the DCRP region is protected, it cannot be written, and an error will be reported when writing data.
4. After enabling the data mirroring function between CNVM and ECNVM BANK0/1, the DCRP protection settings need to set two region at the same time, otherwise it will lead to the risk of data leakage.

DCRP Area Clearance Process:

1. First, set the EREN bit of DCRP to 1, and then set SPC to any value except 0xAA and 0xCC, that is, set the chip to read protection state.
2. After step 1 takes effect, remove the read protection.

After the above two steps are completed, the DCRP region is cleared. The following points

need to be noted:

1. The EREN bit and the SPC bit can be set at the same time, or the SPC bit can be set again when the EREN bit is valid.
2. While removing the read protection, not only the DCRP region but also the EREN bit of the DCRP is removed.
3. Each read protection removal clear all DCRP regions content, whether CNVM or ECNVM BANK0 and BANK1.

2.2. SCR operation

SCR is a security area operation, so caution must be exercised when configuring the security region. After entering the security area, both the JTAG and SWD interfaces will be unusable, and the BootLoader will not be able to execute. However, the code in the security area can be set arbitrarily, and the user can write a piece of code into the program running in the security area to exit and get out of the security mode.

The SCR zone can be set in the NVMC_SCRADDR_MDF, but the start address must be less than the end address for it to take effect. In safe mode, the area can be modified at will, enlarged, shrunk or deleted. In non-secure mode, if the user wants to modify the area, they must clear the security area before they can modify it.

The implementation of the SCR region requires the SCR global enable bit, and the SCR region enable bit and the SCR region start/end address setting bit can be completed together. SCR global enablement is mainly achieved by setting the SCR bit of the NVMC_OBSTAT0_MDF register. SCR area enable and address configuration are set in NVMC_SCRADDR_MDF registers. The two processes of SCR global enablement and SCR area enablement and setting can be carried out independently in any order. However, there may be limitations for GD32H77xxI series for NVMC. For GD32H77xxI series, the SCR region can only be configured when the SCR global bit is set. The following describes the configuration characteristics of global enable bit and address configuration:

The characteristics of the SCR global enable bit setting (SCR region is not configured) are as follows:

1. Once the SCR global enable bit is enabled, the MCU will boot from the Boot ROM and then jump to the address which is located in BTADDR register according to the pin state of Boot0.
2. After enabling SCR, but without setting a valid SCR region, the MCU can be connected through the JTAG or SWD interface, but the application cannot be debugged or downloaded in the IDE.
3. The removal of the SCR global enable bit can be directly removed by setting the option byte of the BootLoader, and if the BL cannot be connected, if it can be connected to the Jlink commander, it can be removed through the commander tool.

The SCR area enable and address configuration are shown as follows:

Precautions for GD32H77x_H78x_BootLoader Operations

1. Once the SCR region enables the enabled bit, the SCR start and end addresses cannot be modified.
2. Different region segments can only set the corresponding SCR region enable bit and the region start and end addresses.
3. If the SCR region enable bit is not set, the SCR disable bit and the SCR address can be modified at will.

The security area can currently be configured in any of the three region segments of CNVM, ECNVM BANK 0 and BANK1, of course, there are many combinations in it, no matter how they are combined, in the end only the code in the security zone of the 1 zone segment can be run. Here is 1 principle:

No matter how many SCR area are set, the startup code will look for the first valid SCR region from the startup address, and if it has not been found at the end of the ECNVM, it will go to the search from 0x8000000 until the startup address is found.

Note: The startup code will not check whether there is a valid code in the SCR area, and the presence of invalid code in the SCR region will cause a huge disaster, causing the chip to be bricked.

The following describes how to delete an SCR security zone:

Delete the SCR area in the non-secure area:

1. Firstly, set the EREN bit of SCR to 1, and then set SPC to any value other than AA and CC, that is, set the chip as read protection.
2. After step 1 takes effect, remove the read protection.

After the above two steps are completed, all SCR areas are cleared. During the operation, the following three points need to be noted:

1. The EREN bit and the SPC bit can be set at the same time, or the SPC bit can be set again when the EREN bit is valid.
2. When removing the read protection, the EREN bit of DCRP will be set, for removing the SCR region, the EREN bit of DCRP needs to be set.
3. After removing the SCR region, the EREN bits of SCR and DCRP will be set, and these two bits need to be cleared according to certain steps.

Of course, you can also delete its SCR security area in the security mode:

1. Directly set the start address of the secure area to be greater than the end address.
2. After disabling secure area, the SCR region enable and the SCR global enable bits are not removed, and the SCR region enabling bit needs to be removed by removing the SCR region in the non-safe area, and the SCR global enabling bit can be removed directly.

Note: the scope of the SCR region can be modified arbitrarily, but the scope modification may cause the application in the SCR region to fail to run.

The following describes an example of setting up an SCR region under NVMC CASE 1:

Precautions for GD32H77x_H78x_BootLoader Operations

1. Prepare bin files for 3 different region segments, download and run addresses of 0x8000000 (corresponding to CNVM), 0x8700000 (corresponding to ECNVM BANK0) and 0x8500000 (corresponding to ECNVM BANK1), The running programmer in the bin file will jump out of the SCR area at the end of the program and execute BootLoader again.
2. Adjust the MCU Boot pin to enter BootLoader mode and run the software All_In_One Programmer.
3. Download the corresponding bin file to the corresponding address, and do not check the "Jump to run the App program" option in the host computer.
4. Set the SCR global enable bit SCR _MDF of the NVMC_OBSTAT0_MDF register in the option byte, set it to 1, and set the BOOT_ADDR0 bit field of the NVMC_BTADDR_MDF register to 0x0800.
5. Set all SCR region enable and area clearing bits in the NVMC_SCRADDR_MDF register, and then set the start and end page addresses of the SCR region.
6. Once the SCR region is set, the MCU will enter the SCR region as it starts.
7. Since the SCR region is set to CNVM, ECNVM BANK0 and BANK1, the firmware will select the region segment closest to the startup address set in the NVMC_BTADDR register to boot, and since the address set in step 4 is the CNVM region segment, then the SCR program will be launched from CNVM.
8. If the value of the modified the startup address set in the NVMC_BTADDR register is 0x8700000 or 0x8500000, the MCU will start the SCR application from ECNVM BANK0 or BANK1 after booting.

2.3. SCR and DCRP concurrent operation

After both the DCRP region and the SCR bit are set, the SCR bit cannot be removed directly. At this time, the SCR bit and other bits in the register cannot be modified at the same time, and the modification will never take effect. The only way to clear the SCR bit is to set DCRP_EREN bit firstly.

3. **OTP operation**

OTPs can be operated by using the BootLoader, and each OTP bit corresponds to an OTP Lock bit. Normally, an OTP bit can be modified at will, but once the OTP lock bit is rewritten from 0 to 1, the corresponding bit cannot be restored to 0. In addition, once some OTP bits are set to 1, the corresponding lock bits will be automatically set to 1 by the hardware. Therefore, user are advised not to change the OTP at will, please read the user manual carefully before changing the OTP. The following mainly describes the SCR and DCRP region configurations in OTP.

There is a SCR_EFFCTL bit in the OTP about the SCR, which determines whether the SCR uses the configuration in the OTP or the configuration in the option byte, please refer to the user manual for details. It should be noted that the OTP bits related to SCR will be automatically locked by the hardware after setting, and can no longer be changed after the reset takes effect.

4. SDIO interface

The precautions for option bytes operations also apply to the SDIO interface BootLoader. Note that after an option byte is written, usually the BootLoader must perform a software reset for it to take effect. However, since SD card upgrade is an offline operation, you need to copy different upgrade files (the configuration information of option bytes is different) from the PC to the SD card multiple times before you can complete the operation when performing the option byte sequence operation.

5. USB interface

Since the PHY of the USB interface of the GD32H77x_H78x needs to be powered separately, the power supply method of the USB PHY needs to be paid special attention. If the USB PHY is powered incorrectly, the DFU will not be recognized. For the USB PHY power supply method, please refer to the [*"AN117 Precautions for the use of USBHS of GD32H7xx series"*](#). In addition, if the USB PHY is not powered, it will not affect other interfaces.

6. OSPI interface

The USART interface of the GD32H77x_H78x BootLoader supports writing data to OSPI flash. The OSPI interface includes two sets of sub-interfaces, OSPI0 and OSPI1, which can be selected as the default GPIO pin or specified by the host computer. Among them, the flash operation of the OSPI interface supports clock division, 1-wire and 8-wire modes, and other configurations. After setting the relevant configurations, the host computer can download a specified BIN file to OSPI flash, and the host computer also provides an upload function, which can upload the specified range of OSPI flash data to the specified file.

Note: After configuring the GPIO pins of OSPI with the host computer, the pins of USART, USB, and SDIO interfaces may be occupied, so you need to reset them before connecting to other interfaces.

7. Revision history

Table 7-1. Revision history

Revision No.	Description	Date
1.0	Initial Release	Oct.31, 2025
1.1	Revise proprietary terms	Oct.20, 2026

Important Notice

This document is the property of GigaDevice Semiconductor Inc. and its subsidiaries (the "Company"). This document, including any product of the Company described in this document (the "Product"), is owned by the Company according to the laws of the People's Republic of China and other applicable laws. The Company reserves all rights under such laws and no Intellectual Property Rights are transferred (either wholly or partially) or licensed by the Company (either expressly or impliedly) herein. The names and brands of third party referred thereto (if any) are the property of their respective owner and referred to for identification purposes only.

To the maximum extent permitted by applicable law, the Company makes no representations or warranties of any kind, express or implied, with regard to the merchantability and the fitness for a particular purpose of the Product, nor does the Company assume any liability arising out of the application or use of any Product. Any information provided in this document is provided only for reference purposes. It is the sole responsibility of the user of this document to determine whether the Product is suitable and fit for its applications and products planned, and properly design, program, and test the functionality and safety of its applications and products planned using the Product. The Product is designed, developed, and/or manufactured for ordinary business, industrial, personal, and/or household applications only, and the Product is not designed or intended for use in (i) safety critical applications such as weapons systems, nuclear facilities, atomic energy controller, combustion controller, aeronautic or aerospace applications, traffic signal instruments, pollution control or hazardous substance management; (ii) life-support systems, other medical equipment or systems (including life support equipment and surgical implants); (iii) automotive applications or environments, including but not limited to applications for active and passive safety of automobiles (regardless of front market or aftermarket), for example, EPS, braking, ADAS (camera/fusion), EMS, TCU, BMS, BSG, TPMS, Airbag, Suspension, DMS, ICMS, Domain, ESC, DCDC, e-clutch, advanced-lighting, etc.. Automobile herein means a vehicle propelled by a self-contained motor, engine or the like, such as, without limitation, cars, trucks, motorcycles, electric cars, and other transportation devices; and/or (iv) other uses where the failure of the device or the Product can reasonably be expected to result in personal injury, death, or severe property or environmental damage (collectively "Unintended Uses"). Customers shall take any and all actions to ensure the Product meets the applicable laws and regulations. The Company is not liable for, in whole or in part, and customers shall hereby release the Company as well as its suppliers and/or distributors from, any claim, damage, or other liability arising from or related to all Unintended Uses of the Product. Customers shall indemnify and hold the Company, and its officers, employees, subsidiaries, affiliates as well as its suppliers and/or distributors harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of the Product.

Information in this document is provided solely in connection with the Product. The Company reserves the right to make changes, corrections, modifications or improvements to this document and the Product described herein at any time without notice. The Company shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. Information in this document supersedes and replaces information previously supplied in any prior versions of this document.