N32H7xx Series Software Development User Guide

Introduction

The purpose of this document is to enable users to quickly get familiar with the software usage of the N32H7xx series microcontrollers (MCUs), to guide users to more easily understand and use this product.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

CONTENTS

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

1. Overview

Welcome to the NSING N32H7xx series chips. This article introduces the software usage of the N32H7xx series microcontrollers (MCUs) and how to use each module, to guide users to more easily understand and use this product.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

2. System Architecture

The N32H7xx series high-performance MCU adopts an ARM Cortex-M7 + Cortex-M4F dual-core architecture, with 2MB/4MB built-in sip flash and 1504KB built-in SRAM, of which 1024KB SRAM can be configured as TCM.

It supports mainstream development and debugging tools such as Keil, IAR, Eclipse, GCC, GDB, uLink, Jlink, and nsLink, and allows debugging via the JTAG/SWD interface. It supports simultaneous debugging on both cores (two IDEs need to be opened, and different AP nodes need to be selected for debugging: AP0 for CM7 and AP2 for CM4). See section 3.2 “Download and Debugging”,for details.

The Cortex-M7 and Cortex-M4 communicate via the AXI-AHB bridge, and both can access all Flash, SRAM, and peripheral resources (note: the M4 cannot access the TCM).

The SRAM5 on the AHB bus can be either a regular AHB SRAM or configured as a dedicated RAM for CAN. Care should be taken when using it.

To better leverage the performance of the N32H7xx series chips, it is recommended to execute user application code in the TCM. (For instructions on how to use TCM to accelerate, please refer to the document *CN_UG_N32H7xx_TCM_User_Guide.pdf*).

The N32H7xx series provides a set of boot API functions to implement functions including option byte configuration, flash erase/write, and memory protection.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3. Software Function Development

3.1. Boot Startup

The N32H7xx series products use a built-in system bootloader to perform permission protection management and user startup mode configuration during system startup.

The system always starts executing from the Boot program upon startup, then completes permission configuration based on OTP and Option bytes parameters, and finally completes user startup based on the boot0 pin level, Option bytes, and BTM field (see the OTPC section of the user manual for details)。

For information related to access control, please refer to
《*CN_UG_N32H7xx_Series_Security_Feature_User_Guide.pdf*》.

The N32H7xx is available in standard BOOT mode and serial download mode (Bootloader)：

Standard BOOT mode supports three boot methods: booting from Flash, booting from SRAM, and secure boot.

1. When the boot0 pin is low, the boot mode is standard BOOT mode. The address in the BOOT_ADDR field of the option byte determines whether to boot from Flash or SRAM. The value of the BOOT_ADDR field can be any address in the main memory area or the SRAM/ITCM region.
2. When the secure user mode in the option bytes is enabled and the secure user area is correctly configured, each boot from standard mode will force a boot from the secure user area. The secure user area must have the correct secure user code pre-downloaded; otherwise, the system will fail to boot. For details regarding the secure user area, please refer to the security features user guide.

Serial download mode, also known as system bootloader mode, is entered when the boot0 pin is high.

The N32H7xx also supports boot mode locking. When the BTM field is 0x5AA5, it forces booting from standard mode. When the BTM field is 0x4884, it forces booting from serial download mode. Except for the above cases, the boot mode follows the level of the boot0 pin.

Note: Please use this function with caution. Incorrect operation may cause the chip to lock up.

Startup mode selection：

BTM	boot0	Secure Mode	BOOT_ADDR	Startup location
x (unlocked)	0	0	0x15000000~ max user flash	Flash
			0x24000000~ max AXI SRAM shared (ITCM/DTCM)	AXI SRAM
			0x30000000~ max AHB SRAM	AHB SRAM
			0x00000000~ max ITCM	ITCM
		1	Secure User Area	Flash
	1	x	x	Serial download mode
0x5AA5	x	0	0x15000000~ max user flash	Flash
			0x24000000~ max AXI SRAM shared (ITCM/DTCM)	AXI SRAM

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

			0x30000000~ max AHB SRAM	AHB SRAM
			0x00000000~ max ITCM	ITCM
		1	Secure User Area	Flash
0x4884		x	x	Serial download mode

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.2. Download and Debugging

■ **Disable debug interface**

1. The JTAG/SWD debugging interface is enabled by default. Customers can choose whether to disable the debugging interface as needed. The debugging interface can be enabled again after being disabled. This configuration can only be modified 16 times.
2. This configuration is achieved by modifying the OTP field (SEC_JTAG_CFG_OTP). Modification requires BOOT0 to be pulled high to enter serial download mode. The modification can be performed using the Nations MCU Download Tool.

■ **Debugger connection precautions**

3. After the chip is powered on, it will run M7 by default, while M4 will be in STANDBY state.
4. Before connecting the debugger to M4, M7 needs to be enabled for M4 (RCC.M4RSTREL=1), otherwise the debugger will not be able to find the M4 device.
5. In any mode, the debugger interface is closed while the secure bootROM program is executing and is only restored when the secure bootROM program exits.

■ **Download and debugging precautions**

1. When downloading and debugging with M4, you need to select the kernel (VECEREST/CORE) reset method. If you select the SYSRESETREQ reset method, the entire system will be reset, and RCC.M4RSTREL will be reset, causing the debugger to be unable to connect.

2. When debugging with KEIL dual-core, M7 needs to be set to SYSRESETREQ. This reset will reset the entire system (including M7 and M4). After the reset, M7 will start M4. Only after M4 starts can normal debugging be performed.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.3. RCC Usage Instructions

Some peripherals have configurable clocks, allowing users to select and configure a specific clock as needed. However, before configuring a peripheral clock, ensure that the corresponding clock is correctly configured and running stably. The peripherals with configurable clocks are listed below; for details, please refer to the user manual.

1. The SDMMC1 kernel clock source can be selected from AXI divider clock, peri_clk, PLL2A, PLL3A, or PLL1B; the SDMMC2 kernel clock source can be selected from sys_bus_div_clk divider clock, peri_clk, PLL2A, PLL3A, or PLL1B.
2. The ADC pll_div_clk clock source can be selected from PLL2B, PLL1B, PLL3B, or PLL3C.
3. The Ethercat kernel clock source can be selected from sys_bus_div_clk divided clock, PLL2B, PLL3A, PLL3C, or PLL1B.
4. The GMII_TX_clk clock source for Ethernet1 can be selected from ETH1_125M_clk, PLL1C, PLL2B, or PLL3A; the ptp_clk clock source for Ethernet1 and Ethernet2 can be selected from sys_bus_div_clk divided clock, peri_clk, PLL3A, or PLL2C.
5. The I2S core clock source can be selected from the sys_bus_div_clk divided clock, PLL3B, HSI, or CK pin.
6. The kernel clock source for I2C can be selected from sys_bus_div_clk divided clock, PLL3C, HSI, or MSI.
7. The kernel clock source for FDCAN can be selected from sys_bus_div_clk divided clock, PLL1C, PLL2C, PLL3B, or peri_clk.
8. The clock source for DSMU core A can be selected from APB2 clock, PLL1B, PLL2B, PLL3A, i2s_ckin_clk, or peri_clk. i2s_ckin_clk can be further selected from pins of I2S1, I2S2, I2S3, or I2S4. The core clock source can be selected from a divided clock of sys_bus_div_clk or the APB2 clock.
9. The clock sources for M0 and M1 of FEMC can be selected from AXI divider clock, peri_clk, PLL2C, PLL3B, or PLL1B.
10. The LCD pixel_clk clock source can be selected from AXI divider clock, peri_clk, PLL2C, or PLL3B.
11. The XSPI ssi_clk clock source can be selected from AXI, PLL3C, PLL1B, PLL2A, or PLL2C.
12. The SDRAM mem_clk clock source can be selected from AXI divider clock, peri_clk, PLL2A, PLL3A, or PLL1.
13. The RTC clock source can be selected from LSE, LSI, or HSE frequency division clocks.
14. The DVP clock source can be selected from AXI divider clock, peri_clk, PLL2C or PLL3A.
15. The TRNG clock source can be either the sys_bus_div_clk divider clock or the HIS clock.
16. The LPTIM core clock source can be selected from APB5, LSI, LSE, HSE, HSI, MSI, comp1_out, comp2_out, comp3_out, or comp4_out. When comp_out is selected as the clock source, it is optional to add a filter.
17. The LPUART kernel clock source can be selected from sys_bus_div_clk divided clock, HSI, LSE, HSE, or MSI.
18. The COMP low-speed clock source can be either LSE or LSI.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.4. PWR (Power Management Module) Software Configuration

To correctly configure the power supply mode of the core voltage Vcap, PWR has four power supply modes:

- **Mode 0：** This is the transient power mode when Vcap is powered on, during which SMPS is enabled. After CM7 starts up, the power supply mode should be configured to one of the following valid power supply configurations (mode 1/2/3);
- **Mode 1：** SMPS power supply Vcap;
- **Mode 2：** External LDO power supply Vcap;
- **Mode 3：** Vcap is powered by an external power source, and SMPS is turned off.

Notice：

1. *Mode 0 is a transient power supply mode and cannot be selected as the chip's continuous power supply mode.*
2. *If the software attempts to write an invalid configuration other than modes 1, 2, or 3, the register bits for the mode configuration will remain locked in mode 0 until the system resets and clears the lock;*
3. *After the chip is powered on, the mode 1/2/3 configuration can only be operated once. Subsequent operations will keep it locked. The lock will only be cleared by system reset.*

Users must select the correct PWR mode in the firmware library *system_n32h7xx.c* to match the external circuitry.

For example, if the user's external circuitry is designed to power the chip using SMPS, in order to correctly configure PWR, the user needs to uncomment the code on line 85: "#define PWR_SUPPLY_SELECTION (PWR_DIRECT_SMPS_SUPPLY)". See the diagram below.

```
79  #define TCM_SIZE_VALUE (0x20)          /*TCM_SIZE=0x20:256K ITCM;256K DTCM;512K AXI_SRAM*/
80
81  /** Private_Functions */
82
83  /* defaule power supply is extern LDO. User can change the way of power supply*/
84  //#define PWR_SUPPLY_SELECTION       (PWR_LDO_SUPPLY)  /* External LDO Supply */
85  #define PWR_SUPPLY_SELECTION       (PWR_DIRECT_SMPS_SUPPLY)  /* DCDC Supply */
86  //#define PWR_SUPPLY_SELECTION       (PWR_EXTERNAL_SOURCE_SUPPLY)  /* VCAP Supply */
87
```

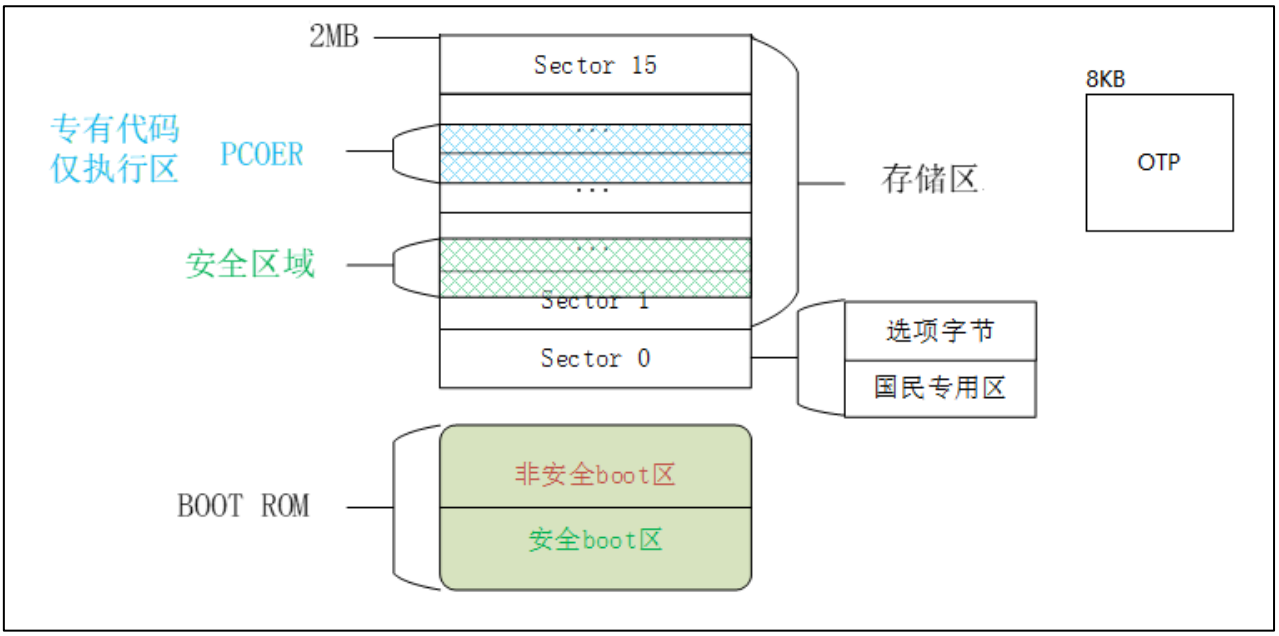
Similarly, if you choose to supply power to the chip via an external power source through Vcap, you need to comment line 85 and uncomment line 86 in the above diagram.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.5. SMU (System Management Unit)

SMU provides a set of API interfaces to implement a series of functions, including flash read/write, secure storage management, option bytes (RDP/WRP/secure mode, etc.), secure areas, execution-only regions, interface configuration, and so on.

The storage space diagram is shown below. The chip has a 32KB ROM area, divided into secure and non-secure parts. The secure boot area contains the official system boot firmware (bootloader) of NSING, while the non-secure boot area contains a series of user APIs. The chip integrates 2MB of QSPI Flash, with the first 128KB being a dedicated area of NSING, containing proprietary configuration and option bytes. The remaining space is the user main memory (main flash). In addition, there is an 8KB OTP area for system configuration, of which 1KB is the user area.



The user API provides interfaces for operating on all the above areas, and offers corresponding access control and security features to prevent unauthorized access and tampering, and to avoid the leakage of sensitive information. (For system security and access control policies, please refer to the relevant sections of the user manual)

There are two types of user APIs: one is the Get type (such as GetM4StoreAddrApi), used to retrieve the current configuration parameters, and the other is the Set type (such as SetM4StoreAddrApi), used to configure the parameters. When using them, you should first get the current status through the Get API, identify the current status, and confirm that modifications are needed before using the corresponding Set API for configuration.

Get type APIs will directly return the current configuration parameters when called. Set type APIs will write the configuration parameters to a temporary register and then generate a system reset to make the configuration effective. (Some APIs will not generate a reset but will take effect directly, depending on the specific API.) APIs that generate a reset will not return a value when called.

Users should consider the startup process when using the API to avoid repeated system resets. Generally, configurations that only need to be configured once and then reused should be written into option bytes or OTP to ensure they take effect by default on each power-on.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

The list of user APIs is as follows:

function	description
uint32_t GetCryptLvlApi(void)	Get the current encryption level
uint32_t SetCryptLvlApi(uint32_t crypt)	Set the current encryption level
uint32_t GetDcDcHvEnApi(void)	Get the DC-DC High Core voltage
uint32_t SetDcDcHvEnApi(uint32_t state)	Set the DC-DC High Core voltage
uint32_t GetJtagModeApi(void)	Get JTAG mode
uint32_t SetJtagModeApi(uint32_t jtag_state,uint32_t* check_key)	Set JTAG mode
uint32_t GetM4BootAddrApi(void)	Get M4 boot address
uint32_t SetM4BootAddrApi(uint32_t addr)	Set the M4 start address
uint32_t GetM7BootAddrApi(void)	Get M7 boot address
uint32_t SetM7BootAddrApi(uint32_t addr)	Set the M7 start address
uint32_t GetPfoerCfgApi(uint32_t idx)	Get PFOER region
uint32_t GetRdpLvlApi(void)	Get RDP level
uint32_t SetRdpLvlApi(uint32_t rdplvl)	Set RDP level
uint32_t GetSecCfgApi(uint32_t idx)	Get Secure Area
uint32_t GetSysCfgBorApi(void)	Get BORLS
uint32_t SetSysCfgBorApi(uint32_t borcfg)	Set BORLS
uint32_t GetSysCfgBtmApi(void)	Get BTM
uint32_t SetSysCfgBtmApi(uint32_t mode)	Set BTM
uint32_t GetSysCfgNrstIwdgApi(void)	Get IWDG
uint32_t SetSysCfgNrstIwdgApi(uint32_t nrst_iwdg_cfg)	Set IWDG
uint32_t GetTcmSzCfgApi(void)	Get TCM size
uint32_t SetTcmSzCfgApi(uint32_t tcm_sz_cfg)	Set TCM size
uint32_t GetWrpApi(void)	Get WRP
uint32_t SetWrpApi(uint32_t wrp_sector)	Set WRP

Note: For detailed explanations of the API functions, please refer to the relevant sections of the security user manual.

In addition, there is another type of root security service function. Root security services are code provided by NSING used to configure secure area functions. They are executed before any other software after a system reset. After execution and exit, they cannot be accessed again until the next reset.

To use the root security service, you need to enable secure mode first. Secure mode can be enabled by modifying option bytes using PC tools or by calling the corresponding API.

Users execute root security services by calling the RSS_xxx API, which may trigger multiple system resets during the execution process.

RSS_resetAndInitializeSecureAreas

prototype uint32_t RSS_resetAndInitializeSecureAreas(RSS_SecureArea_t area)

parameter The start and end addresses of the secure user area. Used to configure secure user area.

description This service sets the secure user area boundary according to the value stored in the option byte register:

- SEC_AREA_START1 and SEC_AREA_END1 in storage area 1

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

This service is only used when setting up the secure area for the first time. A system reset will be triggered after the service is completed.

RSS_SecureArea_t Structure：

```
typedef union
{
    struct
    {
        __IO uint16_t SEC_BEGIN : 13;
        uint16_t : 3;
        __IO uint16_t SEC_END : 13;
        uint16_t : 2;
        __IO uint16_t DMES : 1;
    }Bit;
    uint32_t Dword;
}RSS_SecureArea_t;
```

RSS_exitSecureArea

prototype void RSS_exitSecureArea(unsigned int vectors)

parameter Address of the application to jump after exiting the secure area

description This service is used to exit the secure user area and jump to the user's main application. This service will not trigger a system reset.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.6. Precautions for using power consumption modes

3.6.1. Standby mode

1. Before entering Standby mode, disable BOR as the system reset source (RCC_BDCTRL.BORRSTEN=0), and re-enable BOR as the reset source after exiting Standby mode; or clear PWR_SYSCTRL2[10] to 0 before entering Standby mode, otherwise the system will exit Standby mode immediately after entering Standby mode.

2. In dual-core products, before the M7 enters Standby mode, ensure that the M4 is also in Standby mode. Only after the M7 enters Standby mode will the system be in Standby mode (SSTBY_C1STBY_C2STBY). The M7 can only be woken up normally when a wake-up event occurs.

3.6.2. BKP SRAM retention in Standby mode

To disable the backup SRAM retention feature in Standby mode, regardless of whether it's a single-core or dual-core product, you need to set both PWR_M7CTRL2.BSRSTBRET=0 and PWR_M4CTRL2.BSRSTBRET=0. Otherwise, the backup SRAM retention feature in Standby mode will be enabled.

3.6.3. Notes on Code Execution in the ITCM in Sleep Mode

When the code executes in the ITCM, RCC_AXIEN3.M7TCMLPEN = 1 must be set before entering Sleep mode to ensure that the TCM clock is not turned off in low-power mode.。

3.7. Flash Access and Cache

Cache cannot be enabled when the program needs to access Flash or when the program is executed in Flash.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

3.8. 2.8. Configuration Considerations for Functional Peripherals

3.8.1. ADC

1. The maximum supported ADC_CLK is 20M. Exceeding 20M will affect the ADC sampling accuracy.

2. When it is necessary to acquire data from the ADC's internal channels (Temp Sensor / Vrefint / Vbat), the internal channel control bit register of ADC1 needs to be enabled, and ADC3 needs to be configured to complete the sampling and conversion of the internal channels. Refer to the VREFBUF example in the SDK for details.

3. When an ADC has multiple channels enabled and the data management method is set to DSMU mode, all data from all channels of this ADC is sent to the DSMU. However, the DSMU does not distinguish between ADC channels; all data from all ADC channels is processed by the DSMU.

3.8.2. OTP

1. During OTP programming, should not generate the NRST reset, otherwise OTP may write incorrect values.

3.8.3. ECCMON

1. When using any one or more ECCMONs, the clocks of all three ECCMONs need to be started. It is recommended to use the ECCMON_EnableClk(void) function to enable the ECCMON clocks.

2. If ECC of SRAM (AXI-SRAM or AHB-SRAM) is enabled, the corresponding SRAM region needs to be initialized, that is, a write 0 operation needs to be performed on the corresponding SRAM region.

3.8.4. WWDG1

1. If M7 enables WWDG1, you need to set RCC_CFG1.WWDG1RSTEN=1 to ensure that WWDG1's timeout reset will trigger a system reset.

3.8.5. LPTIM

1. In DBG_STOP0/DBG_STOP2 mode, RCC only turn off the LPTIM internal clock; LPTIM in external clock mode is unaffected.

3.8.6. XSPI

1. Configuration notes for XSPI when reading and writing memory:

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

- When the transfer mode is Rx-Only, the transfer start fifo of the Tx FIFO must be set to 1.
- When the transfer mode is Tx-Only, the transfer start fifo of the Tx FIFO must be set to 2.
- When the transfer mode is Tx and Rx, the transfer start FIFO of the Tx FIFO must be set to 2.

2. XSPI DMA Precautions

When configuring XSPI_TXFT.TXFTST and XSPI_DMATDL_CTRL.DMATDL, The following conditions must be met:：

- DMATDL >= TXFTST; otherwise, XSPI will fail to send and will not generate a DMA request.

3.8.7. SPI

1. When using SPI, both the internal pull-up/pull-down of the master CLK pin shall be configured according to the idle level of the master clock: set pull-up when CLKPOL is 1, and set pull-down when CLKPOL is 0.

3.8.8. FDCAN

1. It is recommended to configure the FDCAN kernel clock to 20M, 40M, or 80M. For details, please refer to the FDCAN_Classic demo in the SDK.

3.8.9. RCC

1. If you need to disable LSI (RCC_BDCTRL.LSIEN = 0), you also need to disable the LSI clock security detection function (i.e., set the RCC_BDCTRL.LSICSSEN bit to 0).

3.8.10. L1 Read Protection

1. When CM7 core is in L1 read protection mode, FLASH is protected against reading. Unprotected SRAM (or ITCM) cannot access the FLASH. The SMU_SetSRAMProtection (or SMU_SetITCMProtection) function must be called to configure the specified SRAM (or TCM) region as a protected area for normal access to be enabled.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

4. Version History

Version	Date	Remark
V1.2.0	2025-11-25	Create document

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg

5. Notice

This document is the exclusive property of NSING TECHNOLOGIES PTE. LTD. (Hereinafter referred to as NSING). This document, and the product of NSING described herein (Hereinafter referred to as the Product) are owned by NSING under the laws and treaties of Republic of Singapore and other applicable jurisdictions worldwide. The intellectual properties of the product belong to NSING Technologies Inc. and NSING Technologies Inc. does not grant any third party any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only. NSING reserves the right to make changes, corrections. enhancements, modifications, and improvements to this document at any time without notice. Please contact NSING and obtain the latest version of this document before placing orders. Although NSING has attempted to provide accurate and reliable information, NSING assumes no responsibility for the accuracy and reliability of this document. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. In no event shall NSING be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product. NSING Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, Insecure Usage'. Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to supporter sustain life. All Insecure Usage shall be made at user's risk. User shall indemnify NSING and hold NSING harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage Any express or implied warranty with regard to this document or the Product, including, but not limited to. The warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law. Unless otherwise explicitly permitted by NSING, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.

NSING Technologies Pte. Ltd.
Address: 20 Science Park, #03-15/16
Teleteck Park, East Wing, Singapore 117674
Email: sales@nsing.com.sg