N32H7xx Series Security Function User Guide

Introduction

The purpose of this document is to enable users to quickly familiarize themselves with the security features and usage methods of the N32H7xx series microcontrollers (MCUs), and to guide users to understand and use this product more easily.

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 security features and usage of the N32H7xx series microcontrollers (MCUs) to guide users in more easily understanding and using this product.

1.1. Security Introduction

Security protection mainly includes the following aspects: firmware intellectual property protection, device private data protection, and code trust checks, etc.

Security primarily refers to protecting the built-in firmware, data, and system functions. In special applications, keys and personal data are especially important.

Security protection is implemented through a series of hardware and software mechanisms, which can be configured via option bytes, APIs, and secure modes.

- Memory protection: Used to protect code and data from attacks.
- Software isolation: used to protect internal processes from attacks.
- Interface protection: Used to protect the entry points of devices, such as serial or debug ports.
- System monitoring: Monitors external intrusion or abnormal behavior of devices.

1.2. Security Features

This product offers multiple protection mechanisms to protect different assets, with key features including:

- Readout protection (RDP): Provides read protection for all storage areas, as well as for the interface.
- Write Protection (WRP): Used to provide erase and write protection for all storage areas.
- Program Firmware Only Execution Region(PFOER): This protection provides sensitive code execution only functionality, preventing any other access.
- Secure Mode and User Secure Area: Provides a high-level secure operating environment. This function can be used to grant credit to other high-value assets and ensure asset security.

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

2. RDP

2.1. Introduction

It primarily provides read protection for the main memory area, protecting user code from read operations performed by untrusted code.

It includes 3 levels of protection:

- L0, no read protection
- L1, the non-boot user, cannot access any Flash resources, including backup SRAM and backup registers.
- L2, disables the debuggers; all option bytes cannot be modified.

A set of mechanisms is also provided for further protection of the ITCM/SRAM. Users can set the secure areas of the ITCM/SRAM as needed, while the rest are non-secure areas. When encryption protection is enabled, the system automatically sets the corresponding ITCM/SRAM regions as the secure areas.

The product provides corresponding protection based on the access users and the accessed areas. Taking this product as an example:

Access is available to the following users: BOOTROM, Main Memory Area, Secure ITCM, Non-Secure ITCM, Secure SRAM, Non-secure SRAM, and Debuggers.

The accessed areas include: BOOTROM, OTP (System Information, System Configuration, User Area), Flash (User APIs, Option Bytes, Main Memory Area), Secure ITCM, Non-Secure ITCM, Secure SRAM, Non-Secure SRAM, Backup SRAM, and Backup Register.

BOOTROM: The chip's built-in bootloader and self-boot program.

OTP (System Information): UCID, DBG_ID

OTP (System Configuration): JTAG Mode, JTAG KEY, BTM, BOR, NRST_IWDG, TCM_SZ

OTP (User Area): 1KB space, reserved for user use.

Flash (User API): Used for system configuration, option byte modification, Flash read/write, and extended functions.

Flash (Options Bytes): Options Bytes Field

Flash (Main Storage): User Storage Area

Debuggers: JTAG/SWD

Backup SRAM: 4KB, can be maintained in RUN/SLEEP/STOP/STANDBY/Vbat modes

Backup registers: There are 32 32-bit backup registers, which can be maintained in RUN/SLEEP/STOP/STANDBY/Vbat modes.

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

2.2. Permissions table

Protection Level	Access User / Access Area		BOOTROM	Main Storage Area	ITCM/SRAM		Debuggers
					Secure Area	Non-Secure Area	
L0	BOOTROM		RO	NA	NA	NA	NA
	OTP	System Information	RO	RO	RO	RO	RO
		System Configuration	RW(1)	RW(1)	RW(1)	RW(1)	RW(1)
		User Area	RW	RW	RW	RW	RW
	Flash	User API	RO/J	J	J	J	J
		Option Byte	RWE	RWE	RWE	RWE	RWE
		Main Storage Area	RWE	RWE	RWE	RWE	RWE
	ITCM/ SRAM	Secure Area	RW	RW	RW	RW	RW
		Non-Secure Area	RW	RW	RW	RW	RW
	Backup SRAM		RW	RW	RW	RW	RW
	Backup Register		RW	RW	RW	RW	RW
L1	BOOTROM		RO	NA	NA	NA	NA
	OTP	System Information	RO	RO	RO	RO	RO
		System Configuration	RW(1)	RW(1)	RW(1)	RW(1)	RW(1)
		User Area	RW	RW	RW	RO	RO
	Flash	User API	RO/J	J	J	J(2)	J(2)
		Option Byte	RWE	RWE	RWE	RWE	RWE
		Main Storage Area	RWE	RWE	RWE	NA	NA
	ITCM/SR AM	Secure Area	RW	RW	RW	NA	NA
		Non-Secure Area	RW	RW	RW	RW	RW
	Backup SRAM		RW	RW	RW	NA	NA
	Backup Register		RW	RW	RW	NA	NA
L2	BOOTROM		RO	NA	NA	NA	-
	OTP	System Information	RO	RO	RO	RO	-
		System Configuration	RO	RO	RO	RO	-
		User Area	RW	RW	RW	NA	-

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

	Flash	User API	RO/J(3)	J(3)	J(3)	J(2)(3)	-
		Option Byte	RO	RO	RO	RO	-
		Main Storage Area	RWE	RWE	RWE	NA	-
	ITCM/SRAM	Secure Area	RW	RW	RW	NA	-
		Non-Secure Area	RW	RW	RW	RW	-
	Backup SRAM		RW	RW	RW	NA	-
	Backup Register		RW	RW	RW	NA	-

RO： Read-only
RW： Read-Write
RWE：Read-Write-Erase
J： Jump
NA： Access Denied
-： None

Note：

1. *OTP is One-Time Programmable memory with multiple built-in backups, supporting up to 15 modifications.*
2. *All APIs for reading and writing Flash memory are unavailable.*
3. *All APIs for modifying option bytes are unavailable.*

2.3. L0

No Read Protection

When 0xA5 is written to the read protection option byte (RDP1) and any value other than 0xCC is written to the option byte (RDP2), the read protection level is set to L0. At this time, all access users can perform read and program operations on the main memory area and backup SRAM (if no other protection is set).

Note: Programming of option bytes is implemented using API functions provided by NSING TECHNOLOGIES INC.. The current RDP level can be obtained via GetRdpLvlApi(), and the desired RDP level can be set via SetRdpLvlApi(). See the User API section for details.

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

2.4. L1

Protection Level 1

When any value other than 0xA5 is written to the option byte (RDP1) and any value other than 0xCC is written to the option byte (RDP2), read protection level 1 is activated. At this time:：

If the debugger is connected or the boot area is a non-secure ITCM/SRAM region, access (read, write, erase) to the main memory area and backup SRAM is not permitted. If an attempt is made to access them, the corresponding read/write error flag in the MMU status register will be set.

If the user boots from the main storage area or executes code in the secure ITCM/SRAM, then read, erase, and program operations on the Flash and backup SRAM are permitted via user code.

When read protection level 1 is activated, if the protection level is changed to L0 (RDP downgrade) by modifying the option byte, a mass erase will be performed on the Flash, secure ICTM/SRAM (if in use), and backup SRAM. After the erase is complete, the read protection level will revert to L0.

If a secure area and a PFOER region exist during downgrade, and the corresponding DMEP/DMES bits are 0, then the mass erase operation will retain the contents of the secure area and the PFOER region.

If a secure area and a PFOER region exist during downgrade, and the corresponding DMEP/DMES bits are 1, then the mass erase operation will also erase the contents of the secure area and the PFOER region, but will not affect the already set secure area and PFOER region.

Note: 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

2.5. L2

Protection Level 2, Disable Debuggers

Writing 0xCC to the option byte (RDP2) activates read protection level 2. Protection level 2 is permanent; once set to L2, it can never be downgraded back to L0 or L1, and anomaly analysis via the debuggers is no longer possible.

Protection level 2 has all the protection of protection level 1, in addition:

Booting from Non-Secure ICTM/SRAM is no longer allowed;

All debugging functions are disabled;

All APIs related to Flash, Option Bytes, and System Configuration will be unavailable;

When booting from Flash, user code is allowed to read, erase, and program Flash and backup SRAM.

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

3. Version History

Version	Date	Remark
V1.1.0	2025-12-15	Create document

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

4. 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