使用指南

N32H7xx系列安全功能使用指南

简介

此文档的目的在于让使用者能够快速熟悉 N32H7xx 系列微控制器（MCU）的安全特性和使用方法，用于指导用户更容易的了解和使用本产品。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

目录

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

1. 概述

欢迎使用国民技术 N32H7xx 系列芯片，本文介绍了 N32H7xx 系列微控制器（MCU）的安全特性和使用方法，用于指导用户更容易的了解和使用本产品。

1.1. 安全介绍

安全保护主要包括如下几个方面：固件知识产权保护、设备私有数据保护以及代码可信检查等。

安全性主要是指保护内置的固件、数据以及系统功能的安全，在特殊应用场合，密钥和个人数据尤为重要。

安全保护通过一系列硬件和软件机制来实现，通过选项字节、APIs 以及安全模式来配置：

- 存储器保护：用于保护代码和数据免受攻击
- 软件隔离：用于避免内部进程免受攻击
- 接口保护：用于保护器件的入口点，比如串行或调试端口
- 系统监控：监测器件外部入侵或异常行为

1.2. 安全特性

本产品提供多种保护机制，用于保护不同的资产，主要特性有：

- 读出保护（RDP）：用于对所有的存储区提供读出保护，同时也对接口提供保护。
- 写保护（WRP）：用于对所有存储区提供擦除和写入保护。
- 专有代码仅执行（PFOER）：此保护提供了敏感代码仅执行功能，可防止其它任何访问。
- 安全模式和用户安全区域：提供一个高级别的安全运行环境，可以通过此功能对其它高价值资产进行授信，保证资产安全。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2. RDP

2.1. 介绍

主要为主存储区提供读出保护，可保护 Flash 用户区域，以防止不可信代码进行的读操作，

它包括 3 个保护级别：

- L0，无读保护
- L1，非启动用户，不能访问任何 Flash 资源，包括备份 SRAM 和备份寄存器
- L2，禁用调试接口，所有的选项字节不能被修改

还提供了一组机制用于对 ITCM/SRAM 提供进一步的保护，用户可以根据需要设置相应的 ITCM/SRAM 的受保护区域，除此之外的为非受保护区域。当加密保护功能开启时，系统自动将对应的 ITCM/SRAM 区域设置为受保护区域。

根据访问用户和被访问资源的不同提供相应的保护，以本产品为例：

访问用户有：BOOTROM、主存储区、保护 ITCM、非保护 ITCM、保护 SRAM、非保护 SRAM 以及调试接口。

被访问资源有：BOOTROM、OTP(系统信息、系统配置、用户区)、Flash（用户 APIs、选项字节、主存储区）、保护 ITCM、非保护 ITCM、保护 SRAM、非保护 SRAM、Backup SRAM 以及 Backup 寄存器。

BOOTROM：芯片内置的启动引导和自举程序

OTP（系统信息）：UCID、DBG_ID

OTP（系统配置）：JTAG 模式、JTAG KEY、BTM、BOR、NRST_IWDG、TCM_SZ

OTP（用户区）：1KB 空间，预留给用户使用

Flash（用户 API）：用于系统配置、选项字节修改、Flash 读写以及扩展功能

Flash（选项字节）：选项字节字段

Flash（主存储区）：用户存储区

调试接口：JTAG/SWD

备份 SRAM：4KB，RUN/SLEEP/STOP/STANDBY/Vbat 模式下可保持

备份寄存器：32 个 32 位备份寄存器，RUN/SLEEP/STOP/STANDBY/Vbat 模式下可保持

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2.2. 权限表

保护等级	访问用户 / 被访问区		BOOTROM	主存储区	ITCM/SRAM		调试接口
					受保护区	非保护区	
L0	BOOTROM		RO	NA	NA	NA	NA
	OTP	系统信息	RO	RO	RO	RO	RO
		系统配置	RW(1)	RW(1)	RW(1)	RW(1)	RW(1)
		用户区	RW	RW	RW	RW	RW
	Flash	用户 API	RO/J	J	J	J	J
		选项字节	RWE	RWE	RWE	RWE	RWE
		主存储区	RWE	RWE	RWE	RWE	RWE
	ITCM/SRAM	受保护区	RW	RW	RW	RW	RW
		非保护区	RW	RW	RW	RW	RW
	备份 SRAM		RW	RW	RW	RW	RW
	备份寄存器		RW	RW	RW	RW	RW
L1	BOOTROM		RO	NA	NA	NA	NA
	OTP	系统信息	RO	RO	RO	RO	RO
		系统配置	RW(1)	RW(1)	RW(1)	RW(1)	RW(1)
		用户区	RW	RW	RW	RO	RO
	Flash	用户 API	RO/J	J	J	J(2)	J(2)
		选项字节	RWE	RWE	RWE	RWE	RWE
		主存储区	RWE	RWE	RWE	NA	NA
	ITCM/SRAM	受保护区	RW	RW	RW	NA	NA
		非保护区	RW	RW	RW	RW	RW
	备份 SRAM		RW	RW	RW	NA	NA
	备份寄存器		RW	RW	RW	NA	NA
L2	BOOTROM		RO	NA	NA	NA	-
	OTP	系统信息	RO	RO	RO	RO	-
		系统配置	RO	RO	RO	RO	-
		用户区	RW	RW	RW	NA	-
	Flash	用户 API	RO/J(3)	J(3)	J(3)	J(2)(3)	-
		选项字节	RO	RO	RO	RO	-
		主存储区	RWE	RWE	RWE	NA	-
	ITCM/SRAM	受保护区	RW	RW	RW	NA	-
		非保护区	RW	RW	RW	RW	-
	备份 SRAM		RW	RW	RW	NA	-
	备份寄存器		RW	RW	RW	NA	-

RO： 只读
RW： 可读可写
RWE：可读可写可擦

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

J： 可跳转
NA： 禁止访问
-： 无

注：
1. *OTP 为单次可以编程存储器，内置了多个备份，支持最多修改 15 次*
2. *所有读写 Flash 的 API 不能使用*
3. *所有修改选项字节的 API 不能使用*

2.3. L0

无读保护

将 0xA5 写入读保护选项字节（RDP1）且将非 0xCC 的任意值写入选项字节（RDP2）时，读保护等级即设为 L0，此时，所有的访问用户都可以对主存储区、备份 SRAM 进行读取编程操作（如果未设置其它保护）。

注：对选项字节的编程，使用国民技术提供的 API 函数来实现，通过 GetRdpLvlApi()获取当前的 RDP 等级，通过 SetRdpLvlApi()设置想要的 RDP 等级。详情请见用户 API 章节。

2.4. L1

保护级别 1

将非 0xA5 的任意值写入选项字节（RDP1）且将非 0xCC 的任意值写入选项字节（RDP2）时，即激活读保护等级 1，此时：

如果调试器已连接或启动用户为非保护 ITCM/SRAM 区，则不允许访问（读、写、擦）主存储区和备份 SRAM。如果试图进行访问，则会将 MMU 状态寄存器的相应读/写错误标志置位。

如果从主存储区启动或者在受保护的 ITCM/SRAM 中执行代码的用户，则允许通过用户代码对 Flash 和备份 SRAM 进行读取、擦除和编程操作。

当读保护等级 1 激活时，如果通过修改选项字节将保护等级改为 L0（RDP 降级），则会对 Flash、受保护 ICTM/SRAM（如果有使用）以及备份 SRAM 执行批量擦除。当擦除完成后，读保护等级变为 L0。

如果降级时，存在安全区域和 PFOER 区域，且对应的 DMEP/DMES 位为 0，则批量擦除操作会保留安全区域和 PFOER 区域的内容。

如果降级时，存在安全区域和 PFOER 区域，且对应的 DMEP/DMES 位为 1，则批量擦除操作会将安全区域和 PFOER 区域的内容也一并擦除，但不影响已设置的安全区域和 PFOER 区域。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2.5. L2

保护级别 2，禁用调试接口

将 0xCC 写入选项字节（RDP2）时，可激活读保护级别 2。保护级别 2 是永久的，一旦设置为 L2，将再也无法降级回 L0 或 L1，也无法再通过调试接口进行异常分析。

保护等级 2 拥有保护等级 1 的所有保护，此外：

不再允许从非保护的 ICTM/SRAM 启动；

所有调试功能均禁止；

所有与 Flash、选项字节以及系统配置相关的 API 将不能使用；

从 Flash 启动时，允许通过用户代码对 Flash 和备份 SRAM 进行读取、擦除和编程操作。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

3. 版本历史

版本	日期	备注
V1.0.0	2024-12-12	创建文档
V1.0.1	2025-08-20	1，修改页眉的 logo

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

4. 声明

国民技术股份有限公司（下称“国民技术”）对此文档拥有专属产权。依据中华人民共和国的法律、条约以及世界其他法域相适用的管辖，此文档及其中描述的国民技术产品（下称“产品”）为公司所有。

国民技术在此并未授予专利权、著作权、商标权或其他任何知识产权许可。所提到或引用的第三方名称或品牌（如有）仅用作区别之目的。

国民技术保留随时变更、订正、增强、修改和改良此文档的权利，恕不另行通知。请使用人在下单购买前联系国民技术获取此文档的最新版本。

国民技术竭力提供准确可信的资讯，但即便如此，并不推定国民技术对此文档准确性和可靠性承担责任。

使用此文档信息以及生成产品时，使用者应当进行合理的设计、编程并测试其功能性和安全性，国民技术不对任何因使用此文档或本产品而产生的任何直接、间接、意外、特殊、惩罚性或衍生性损害结果承担责任。

国民技术对于产品在系统或设备中的应用效果没有任何故意或保证，如有任何应用在其发生操作不当或故障情况下，有可能致使人员伤亡、人身伤害或严重财产损失，则此类应用被视为“不安全使用”。

不安全使用包括但不限于：外科手术设备、原子能控制仪器、飞机或宇宙飞船仪器、所有类型的安全装置以及其他旨在支持或维持生命的应用。

所有不安全使用的风险应由使用人承担，同时使用人应使国民技术免于因为这类不安全使用而导致被诉、支付费用、发生损害或承担责任时的赔偿。

对于此文档和产品的任何明示、默示之保证，包括但不限于适销性、特定用途适用性和不侵权的保证责任，国民技术可在法律允许范围内进行免责。

未经明确许可，任何人不得以任何理由对此文档的全部或部分进行使用、复制、修改、抄录和传播。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057