使用指南



SPC1169 Security 使用指南

版本 A/1-2023 年 9 月

概述

为了降低软件盗窃的风险,许多芯片都有芯片内部的程序保护。SPC1169的设计考虑到了程序保护的重要性,为用户提供了强大可靠的程序保护功能,其中包括调试锁定和随机数保护。



目录

1	锁定芯片调试接口7
2	随机数据保护13
3	安全功能的具体实现



图片列表

图 1-1:	擦除 main flash	8
图 1-2:	确保 Erase Sector 选中	8
图 1-3:	产生密码	9
图 1-4:	通过上位机下载密码到 main flash	9
图 1-5:	Get Config	
图 1-6:	取消 Debug Unlock,并输入解锁密码	10
图 1-7:	解锁	11
图 1-8:	下载代码	
图 2-1:	随机数在应用程序中的流程图	13
图 3-1:	实际生产过程中安全功能的具体实现流程图	14



表格列表

表 1-1: 配置字的描述	7	,
---------------	---	---



版本历史

版本	日期	作者	状态	变更
A/0	2023-4-11	CanChai	Outdated	首次发布。
A/1	2023-9-4	HangSu	Released	更新章节1



术语或缩写

术语或缩写	描述



1 锁定芯片调试接口

当调试或烧录程序时,芯片的调试接口经常被使用。这也意味着通过调试接口可以读取或 修改芯片内部存储器的内容。因此,必须在批量生产过程中禁用芯片的调试功能。否则,通过 调试接口可以获取芯片内部程序。

通过设置配置字的 CHIP_SECURITY 字段,可以锁定 SPC1169 的调试接口。配置字的描述如表 1-1 所示。一旦 SPC1169 的调试接口被锁定,无法通过调试接口访问内部存储器。此外,通过 ROM 中的引导加载程序读取、编程和扇区擦除内部存储器也被禁用; ROM 中的引导加载程序仅支持擦除 Flash 存储器。

通过以下方法可以解锁 SPC1169 的调试接口:

- 通过 ROM 中的引导加载程序对整个内部 Flash 存储器进行芯片擦除。
- 通过 ROM 中的引导加载程序输入正确的非安全密钥(等于配置字的 UNSECURITY_KEY 字 段)。此方法临时解锁调试接口。这意味着芯片重新启动时调试接口将保持锁定状态。如果 UNSECURITY_KEY 字段的值为 0x0000000_00000000,则表示无法通过输入非安全密钥解锁 调试接口。

地址	名字	描述
		解锁芯片的调试接口需要输入一个 8 字节的密钥
0,10015550		UNSECURITY_KEY,当调试接口被锁定时,只有正确的密钥
UX1001FFF0		才能使调试接口暂时解锁。如果 UNSECURITY_KEY 字段的值
		全部为 0x00,则不能通过输入密钥来解锁调试接口。
		Watchdog 使能字
0x1001FFF8	WDT_ENABLE	OxFFFFFFF: 在芯片启动时禁用看门狗
		其他: 在芯片启动时启用看门狗
		芯片调试接口锁定字
0x1001FFFC	CHIP_SECURITY	OxFFFFFFF: 芯片调试接口将不被锁定
		其他值:芯片调试接口将被锁定

表 1-1: 配置字的描述

下面结合 SPINTROL ISP Tool v2.5.6, 演示了 CHIP_SECURITY 功能。

 按下复位键,之后点击 SPINTROL ISP Tool 中的 main flash 擦除按键,对芯片 main flash 进行 擦除,确保 CHIP_SECURITY 为 0xFFFFFFF,使芯片接口处于不被锁定的状态,如图 1-1 所 示。



图 1-1: 擦腳	余 main flash
SPINTROL ISP Tool v2.5.6 Device SPC1169 • Port COM14 • 0 • • Program Chip Vart Communication EEPROM Burner Nemor Program File	- □ × → ☆ ☆ ☆ ↓ ◇ × ↓ ③ y Area Download Options
D:\1_SDE\SPC1169_Platform\trunk\Project_ v Auto-Reload Code Info Start: Dx1000000 Sire: 0x000011DC Start: Sire: Get Information GetID Get Config UnLook	Program to Flash Program to SRAM Auto-ISP LIN Jump & Run No Handshake Solutions Brase Options Erase Sectors WVR Operation Brase Erase BEFROM
Id Time Level Message 0 19:37:16 000 Info Tx: 7F 1 19:37:16 000 Info Fx: rep 2 19:37:16 008 Info Fx: rep 3 19:37:16 008 Info Tx: 44 Bes 4 19:37:16 024 Info Tx: FF FF 00 6 19:37:16 024 Info Fx: FF FF 00 6 19:37:16 071 Info Fx: 79 19:37:16 071 Success Frase chip Success	
COM14 = [38400,8,None,1] Complete!	100%

- 确保调试过程中一直选中 Erase sector,而不是 Erase chip,从而在接下来的调试过程中位于 main flash 中的 CHIP_SECURITY 不会被误擦除,如图 1-2 所示。

		ase sector terp	
l	SPINTROL ISP Tool v2.5.6	×	
1	Device SPC1169 • Port COM14 • 0	▶ 奈 🔒 ② ヱ ① • Area	
	Program File D:\1_SDK\SPC1169_Platform\trunk\Project_ \ \ Auto-Reload Code Info Start: Ox10000000 Start: Size: Get Information GetID Get Config UnLock	Download Options Program to Flash Program to SRAM Auto-ISP LIN Jump & Run No Handshake Reset(DTR = LDW), BOOT(RTS = HIGH) Erase Options Erase Options WR Operation Erase © EEFROM	
	Id Time Level Message 0 19:37:16 000 Info Tx: 7F 1 19:37:16 000 Info Rx: 79 2 19:37:16 000 Info Rrase ohip begins 3 19:37:16 004 Info Tx: 44 BB 4 19:37:16 024 Info Rx: 79 5 19:37:16 024 Info Rx: 79 6 19:37:16 024 Info Rx: 79 7 19:37:10 071 Success Erase ohip Success		
	COM14 = [38400,8,None,1] Complete!	100% .::	

图 1-2: 确保 Erase Sector 选中

- 使能 Debug Lock,并 Generate Key,如图 1-3 所示。



图	1-3:	产生密码
---	------	------

Program File Download Options Divisions Divisions Program to SLAM Auto-Ralead Auto-Ralead Security Settings Security Settings </th <th>SPINTROL ISP Tool v2.5.6 Device SPC1169 • Port COM14 • 0 Program Chip Vart Communication EEPROM Burner 1</th> <th>♣ ◆ ✿ 🔒 🧷 🛛 🛈 Memory Area 1</th> <th>- 🗆 X</th> <th></th>	SPINTROL ISP Tool v2.5.6 Device SPC1169 • Port COM14 • 0 Program Chip Vart Communication EEPROM Burner 1	♣ ◆ ✿ 🔒 🧷 🛛 🛈 Memory Area 1	- 🗆 X	
Auto-Ralaad Security Settings Start: Dr 99 93 BB 63 D6 A2 48 Get Information Get Information Get Information Get Information Id Time 0 19:37:16 008 2 19:37:16 008 3 19:37:16 008 4 19:37:16 008 4 19:37:16 008 4 19:37:16 008 4 19:37:16 004 5 19:37:16 004 6 19:37:16 004 5 19:37:16 004 5 19:37:16 004 5 19:37:16 004 5 19:37:16 004 5 19:37:16 004 5 19:37:16 004 6 19:37:16 004 10 10 11 11 12 13:37:16 004 14 19:37:16 004 11 11 11 11 12 13:37:16 004 14 14 15 16:01 17:02 18:02 19:37:16 024 10:02 10:02 10:02 10:02 10:02 10:02 10:02 10:02 10:02 10:02 10:02 10:0	Program File D:\1_SDK\SPC1169_Platform\trunk\Project_	Download Options Program to Flash Auto-ISP	○ Program to SRAM ☑ Jump & Run	
	✓ Auto-Relead	× 3 Generate Key 2: 4B 2: 4B	RTS = MICH) v S	

 按下复位键,随便下载一个代码,UNSECURITY_KEY,WDT_ENABLE,CHIP_SECURITY 会在下载 的最后写入到 0x1001FFF0 开始的位置,如图 1-4 所示。

	SPINTROL ISP Tool v2.5.6 Device SPC1169 V Port COM14 0	\$\$ - □ × • • ≙ ♂ ≍ 0	
ſ	Frogram Chip Uart Communication EEPROM Burner Memory	y Area	
	Program File 1.洗hex文件 D:\1_SDK\SPC1169_Platform\trunk\Project_ >	Download Options Program to Flash Program to SRAM Auto-ISP LIN Jump & Run	
	Ed Auster Reland	No Handshake	
	Muto-verosa	Provide The Provide Pr	
	Code Info	Reset(Sin - Dony, Boot(ins - Hony +	
	Start: 0x10000000 Size: 0x000011DC	Russ Chie Russ Sectors	
	Start: Size:	O mase chip @ mase Sectors	
		NVR Operation	
	Get Information GetID Get Config UnLook	Eraze • EFFKUM	
	Id Time Level Message	^	
	121 20:04:56 421 Success Download code to	Flash successfully!	
	122 20:04:56 421 Info Write Config Data 123 20:04:56 421 Info Tx: 31 CR	<u>k</u>	
	124 20:04:56 429 Info Rx: 79		
	125 20:04:56 429 Info Tx: F0 FF 01 10 F	11	
	126 20:04:56 446 Info Rx: 79		
	127 20:04:56 446 Into Ix: 0F 07 9F 93 B	88 63 D5 A2 48 FF FF FF FF 00 00 00 00 CF	
	129 20:04:56 462 Info Tx: 21 DE		
	130 20:04:56 477 Info Rx: 79	×	
	Write Config Data		
	HART COMPANY AND C.		
	COM14 = [38400,8,None,1] Complete!	100%	

图 1-4: 通过上位机下载密码到 main flash

图 1-4 中 0xD7 0x9F 0x93 0xBB 0x63 0xD5 0xA2 0x4B 为 key, 0xFF 0xFF 0xFF 0xFF 0xFF 为 WDT_ENABLE, 0x00 0x00 0x00 0x00 为 CHIP_SECURITY, 如表 1-1 所示, 芯片启动时的 WDT 被禁止, 芯片调试接口将被锁定。

- 按下复位键,尝试下载代码,会发现握手失败,表明芯片调试接口已经关闭了。
- 平常也可以在按下复位键后点击 Get Config 查看芯片有无加锁,如图 1-5 所示。





图 1-5: Get Config

SPINTROL ISP TOOL V2.3.4		
Device SPD1179 • Port COM14 • 🕕 🕂	• 🔶 🛱 💾 🖉 🔟 🔘	
Program Chip Uart Communication EEPROM Burner Mem	ory Area	
Program File	Download Options	
D:\1_SDK\SPC1169_Platform\trunk\Project_ ~	Program to Flash Program to SRAM	
	Auto-ISP LIN Jump & Run	
Auto-Reload	No Handshake	
	Reset(DTR = LOW), BOOT(RTS = HIGH) \checkmark 5	
Code Info	Erase Options	
Start: 0x10000000 Size: 0x00000050	O Erase Chip 💿 Erase Sectors	
Start: Size:	NVR Operation	
	Erase EEPROM	
Get Information		
GetID Get Config UnLock		
		_
Id Time Level Message	· · · · · · · · · · · · · · · · · · ·	
7 09:31:55 151 Info Rx: 79	· · · · · · · · · · · · · · · · · · ·	
8 U9:31:55 151 Info Kx: UB U4 UU UU 9 09:31:55 151 Success Get Configure S	5 00 03 00 00 00 FF 01 00 00 79 Suggess!	
10 09:31:55 151 Info Flash NVR not I	Lock!	
11 09:31:55 151 Info FLASHFIN not Lo	ock!	
13 09:31:55 151 Info BOUTCNT = 3	J	
14 09:31:55 151 Info RAMBIST OK!		
15 09:31:55 151 Info FLASH Init 0K!		
16 09:31:55 151 Info EEPROM Init OK!		
D-bus I -shi		
Depug Lock:		
COM14 - [38400 8 Nevo 1]	0%	

- 共有两种解锁方式,可以按下复位键,将控制字全部擦除,从而恢复 UNSECURITY_KEY, WDT_ENABLE, CHIP_SECURITY 到全 F 默认值,如图 1-1 所示。
- 也可以输入密码进行解锁,取消选中 Debug Lock,选中 Debug Unlock,并在 Debug Unlock 下输入之前生成的密码,如图 1-6 所示。

SPINTROL ISP Tool v2.5.4		- 🗆 X			
Device SPD1179 - Port COM14 - 🕕 +) 🌣 🔒 🖉 🗵 🚺				
Frogram Chip Vart Communication EEPROM Burner Memory	Program Chip Vart Communication EEPROM Burner Memory Area				
Program File	Download Options				
D:\1_SDK\SPC1169_Platform\trunk\Project_ ~	Irogram to Flash	O Program to SRAM			
· · · ·	🗹 Auto-ISP 🗌 LIN	🗹 Jump & Run			
Auto-Reload	- 🗆 ×	(BTS = HIGH) 5			
Code Info Security Settings					
Start: 0x10000000 Debug Lock	Generate Key	se Sectors			
Start:					
Get Information	ר	κ			
GetID Get D7 9F 93 BB 63 D5 A2 4B					
	-				
Id Time Others					
🗌 WDT Enable					
Curvel .	07				
Lancel	40				
COM14 = [38400,8,None,1]		0%			

图 1-6: 取消 Debug Unlock,并输入解锁密码

- 复位芯片,点击 Unlock 按钮,如图 1-7 所示,使用密码进行解锁为临时行为, Unlock 成功 后,复位芯片解锁失效。



图 1-7:解锁

			Download Options	
D-\1_SDK\SPC1	169 Platform)tr	unk\Project	Program to Flach Program to SRAW	
D. (I_SDR (SICI	105_FIALLOF (F	unk (rroject_ V	I Trogram to Trash O Trogram to Shan	
		×	🗹 Auto-ISP 🗌 LIN 🗹 Jump & Run	
🗸 Auto-Reloa	d		🗌 No Handshake	
			Reset(DTR = LOW), BOOT(RTS = HIGH) V 5	
Code Info			Rease Options	L
Start: 0x100	00000	Size: 0x00000050		
		c' .	J Chrase Unip Chrase Sectors	
Start:		D1ZE:	NVR Operation	
			Erase 🔘 EEPROM	
Get Informati	on			
GetID	Get Confi	ig UnLock		
T 1 T 1		3 		=
1d Time	Leve	et Message	17.11	
0 09:48	14 678 Warn	n Un-Security En-	abled! - D7 97 93 BB 63 DE 42 4B	
2 09:51	:31 381 Infr	on Security Key	. DI VI VO DD DO NZ HD	
3 09:51	:31 387 Infr	o Rx: 79		
4 09:51	:31 387 Info	o UnSecurity chip	begins	
5 09:51	:31 387 Info	o Tx: 92 6D		
6 09:51	:31 403 Info	• Rx: 79	100 PE 10 4P 00	
1 / 00·E1	:31 403 Info	o Tx: D7 9F 93 Bl	63 J5 A2 48 CU	
09:51	·21 410 T_£.	. P 70		

- 选中 No Handshake,随便下载一个代码,下载成功。

U SPINTROL ISP Tool v2.5.4 2.下载 □ > Device SPD1179 - Port COM14 - ① ↓ ◆ ☆ ☆ ☆ ☆ ③ ② 玉 ⑥ Program Chip Uart Communication EEPROM Burner Memory Area	<
Program File 1.32524 Program to Statt D:\1_SDE\SPC1169_Platform\trunk\Project_ \ Start: D:\1_SDE\SPC1169_Platform\trunk\Project_ \ Get Information Erase Get ID Get Conf	
Id Time Level Message 92 10:12:50 798 Info Tx: 4F E1 EE 10 0A 70 47 00 00 28 0C 00 10 00 E0 FF 1F 28 00 93 10:12:50 838 Success Download code to Flash successfully! 94 10:12:50 838 Info Tx: 21 DE 95 10:12:50 846 Info Tx: 00 00 00 10 EF 97 10:12:50 846 Info Tx: 00 00 00 10 EF 98 10:12:50 862 Info Kx: 79 99 10:12:50 862 Info Kx: 79 91 10:12:50 862 Info Kx: 79 92 10:12:50 982 Info Kx: 79 93 10:12:50 982 Info Kx: 79 94 10:12:50 982 Info Kx: 79 93 10:12:50 982 Info Just 100 10:12:50 990 Info Just 101 10:12:50 990 Info t a Sample 0	▲
COM14 = [38400,8,None,1] Complete!	.::

图 1-8: 下载代码

注意**:**

正常使用时,需要取消勾选 No Handshake,否则芯片复位后,上位机与芯片无法通信。



使用密码解锁只能在每次解锁成功后临时解锁下载接口,芯片复位后失效,要想永久解锁,可以将控制字全部擦除,从而恢复 UNSECURITY_KEY, WDT_ENABLE, CHIP_SECURITY 到全 F 默认值,如图 1-1 所示。



2 随机数据保护

有些芯片破解者可能有能力使用特定设备去除芯片封装,读取 Flash 内存中的数据,然后 将其写入未编程的芯片以复制用户的产品。SPC1169 也针对这种情况具有适当的保护机制。

SPC1169 出厂时被写入一个 8 字节的随机数,该随机数无法修改。客户的应用程序可以在运行时从芯片中读取并验证随机数。如果随机数与应用程序预设的值不匹配,则应用程序将终止。由于芯片的随机数彼此不同,即使芯片破解者从一颗芯片的 Flash 存储器中获取程序数据,然后将程序数据写入其他 SPC1169 芯片,程序也无法正常工作。通过这种方式,客户的产品无法大量复制。





在图 2-1 中,应用程序预设的随机数(RN)可以在产品生产过程中通过编程器工具实现。 编程器工具读取目标芯片的随机数,并将其写入目标芯片 Flash 存储器的特定地址。当应用程 序启动时,写一段程序从目标芯片 Flash 存储器的特定地址读取预设的随机数,并将其与目标 芯片的随机数进行比较。



3 安全功能的具体实现

对于在现场大规模生产中实现芯片安全性的步骤如图 3-1 所示。



图 3-1: 实际生产过程中安全功能的具体实现流程图