

NXP AUTOMOTIVE

Technical Training and Cross Selling Camp

S32K1XX SECURITY AND FLASH PROTECTION

王云川

APPLICATION ENGINEER

DEC 2019



SECURE CONNECTIONS
FOR A SMARTER WORLD

INTERNAL/PROPRIETARY



提纲

- 芯片安全和Flash数据保护功能介绍
- 配置芯片安全功能
- 开启Flash数据保护

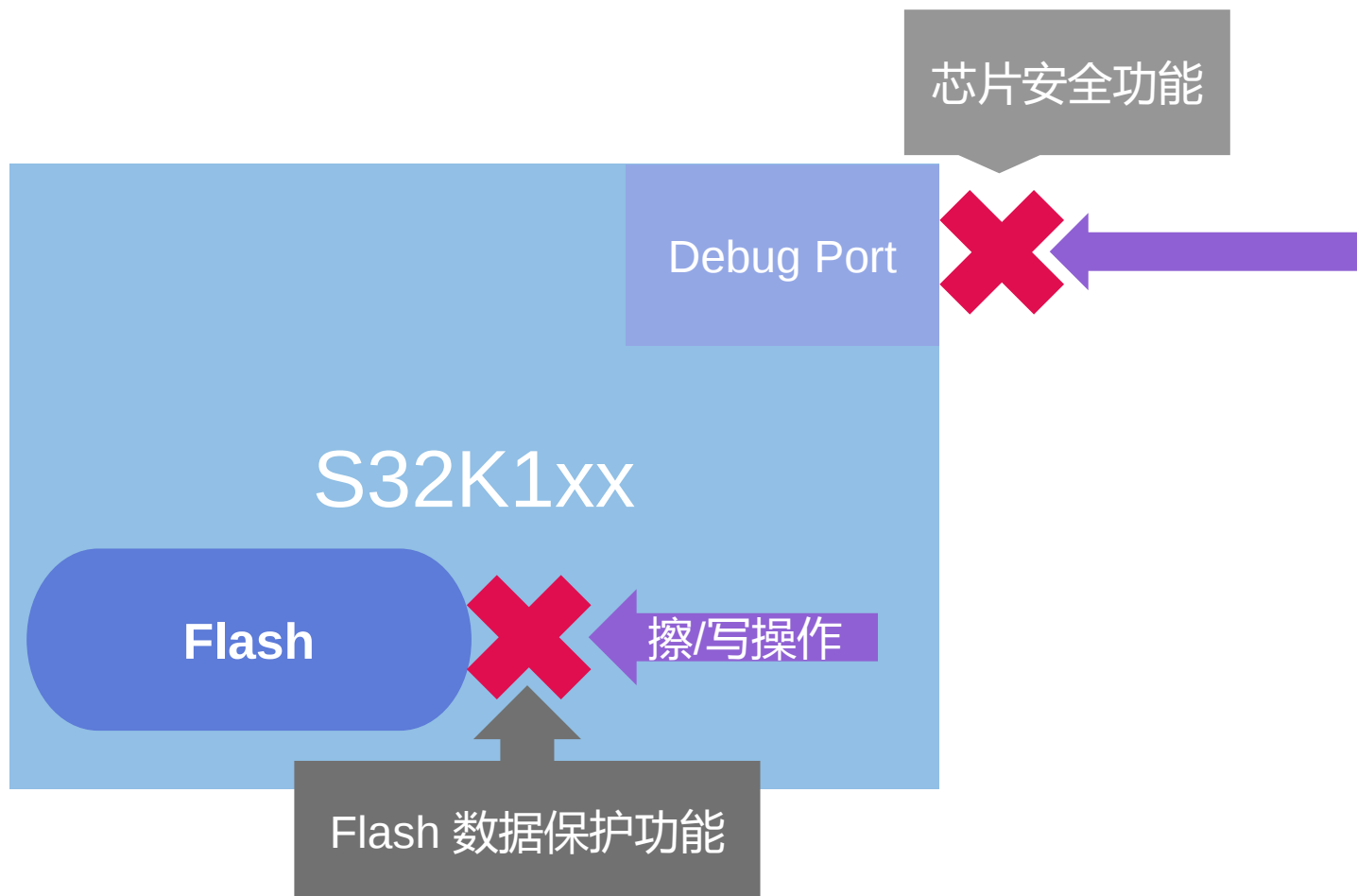


01.

芯片安全和Flash数据保护功能介绍

S321xx芯片安全和Flash数据保护功能

- 芯片安全功能：关闭调试口的功能，切断外部访问芯片的路径
- Flash数据保护功能：关闭设定Flash区域的擦写权限



配置段与相关寄存器

Flash 配置段



相关寄存器



Flash配置段地址	长度 (Bytes)	位域功能	初始化的寄存器
0x0_0400 - 0x0_0407	8	Backdoor key 配置段	——
0x0_0408 - 0x0_040B	4	P-Flash保护配置段	FPROT0-3
0x0_040F	1	D-Flash保护配置段	FDPROT
0x0_040E	1	E-Flash保护配置段	FEPROT
0x0_040D	1	Flash配置段 (详见芯片手册)	FOPT
0x0_040C	1	Flash安全功能配置	FSEC



02.

配置芯片安全功能

FSEC寄存器配置

Bit	7	6	5	4	3	2	1	0
	KEYEN		MEEN		FSLACC		SEC	

- KEYEN: backdoor 使能
- MEEN: mass erase使能
- FSLACC: 工厂失效分析访问码
- SEC: 芯片安全功能使能

芯片永久加锁

设置情况	可使用权限
芯片处于安全状态，Mass erase和工厂失效分析访问权限功能开启。	NXP 可以使用工厂失效分析码对芯片进行失效分析、关闭芯片的安全功能和访问Flash数据。
芯片处于安全状态，工厂失效分析访问权限功能关闭。	NXP 可以使用工厂失效分析码对芯片进行失效分析、关闭芯片的安全功能，但是无法访问Flash中的数据。只能通过工厂失效分析码擦除全部Flash





03.

开启Flash数据保护功能

Flash数据保护区域划分说明

- PFlash: 32的区域
- DFlash: 8个区域
- EFlash: 8个区域

Eg: 对于512k的Pflash, 每个区域为16KB

Region	Start Address	End Address
0	0x0000_0000	0x0000_3FFF
1	0x0000_4000	0x0000_7FFF
2	0x0000_8000	0x0000_BFFF
...	...	...
31	0x0007_C000	0x007_FFFF

开启Flash数据保护的方式

- 配置Flash配置段：
- 应用代码中直接配置寄存器：只能将未保护的区域设置为保护



SECURE CONNECTIONS
FOR A SMARTER WORLD