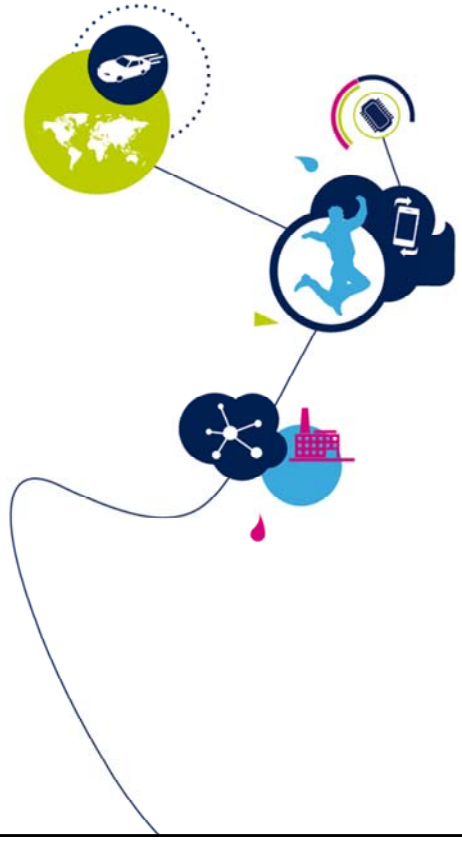
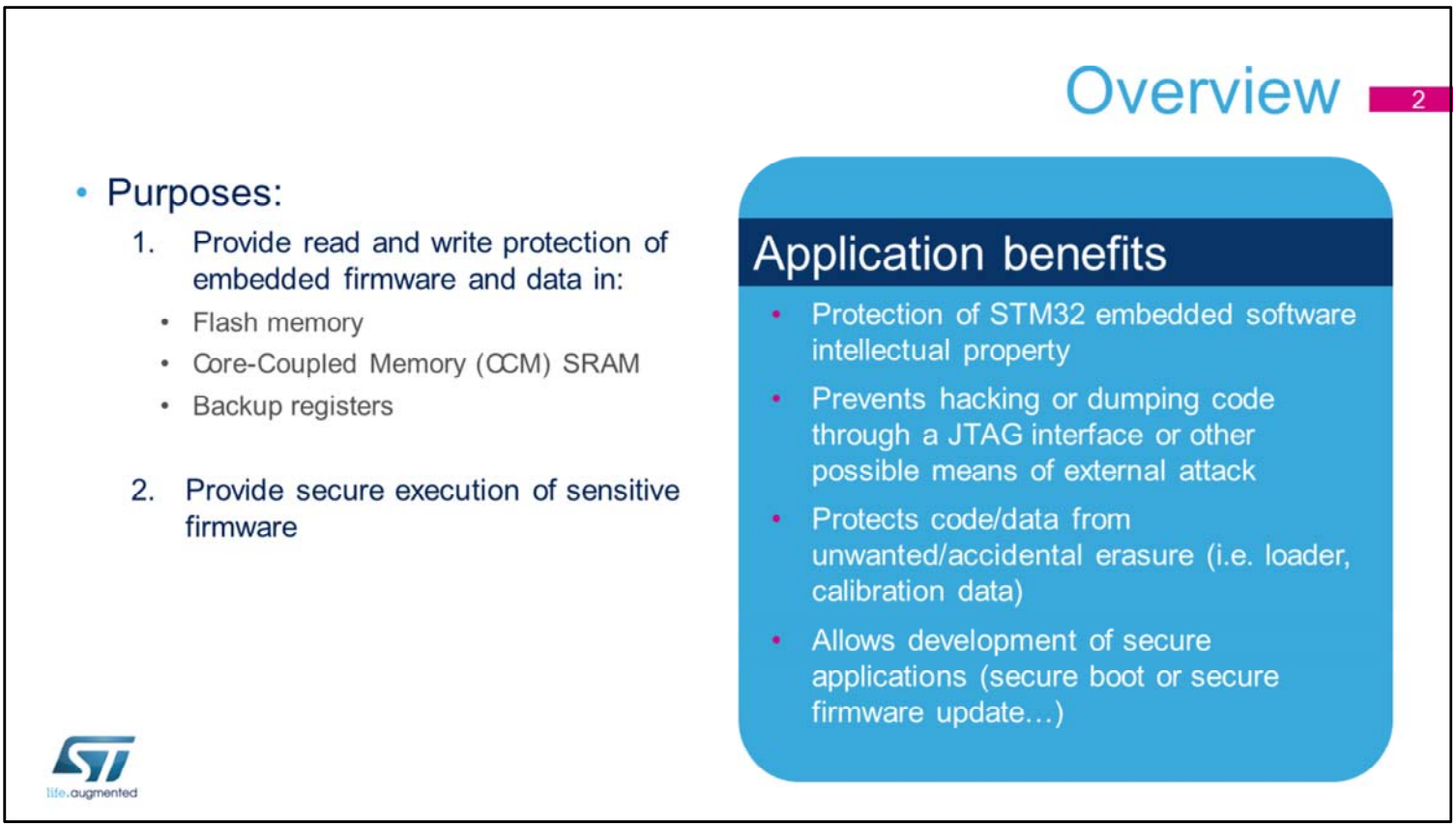
STM32G4 - MEMPROTECT

System Memory Protections
Revision 1.0



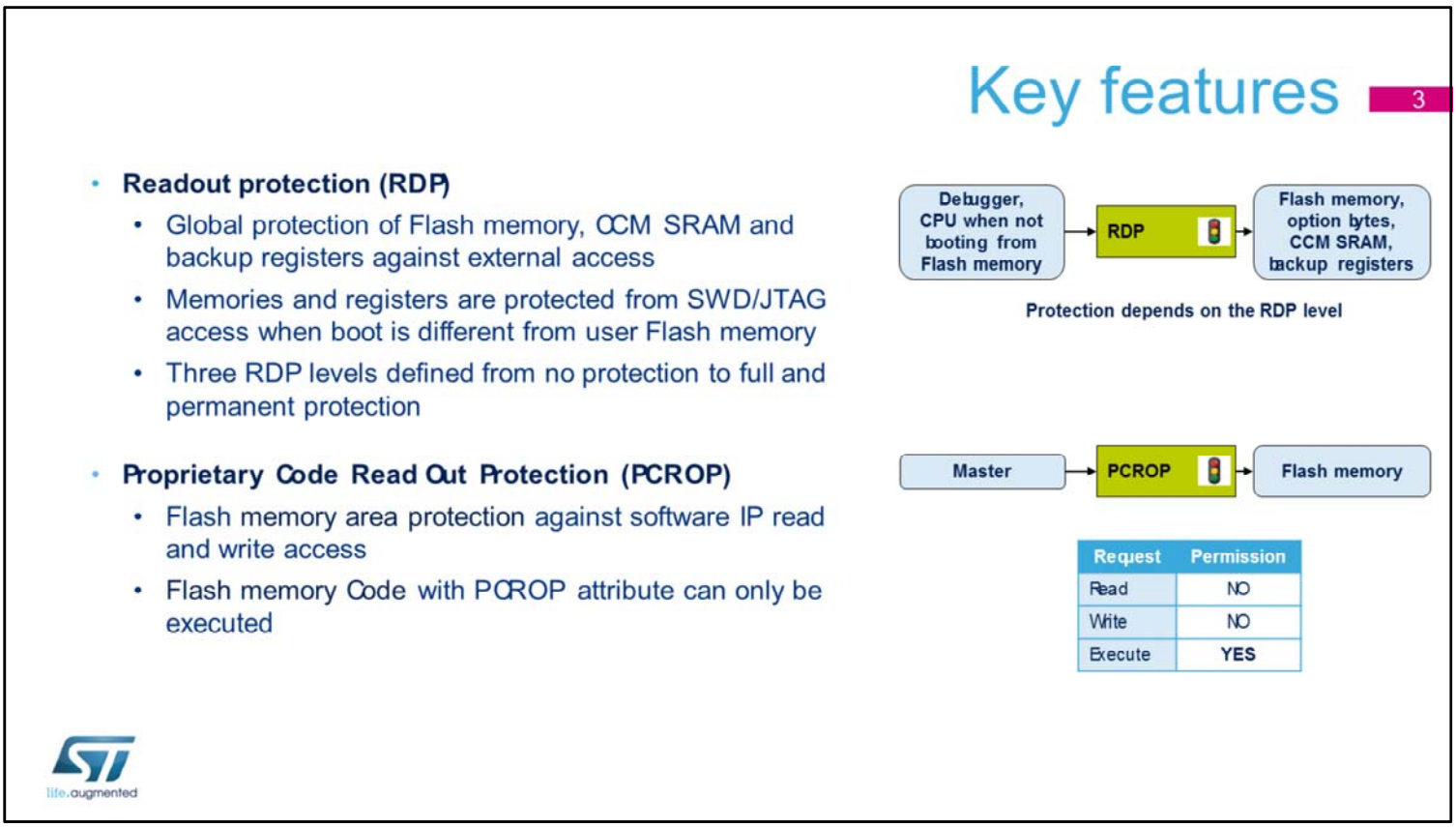
life.augmented

Hello and welcome to this presentation of the STM32G4 System Memories Protection. It will cover the different means for protecting code and data.



Memory protections have been designed for different purposes.
Protected memories are the flash memory, the Core-Coupled Memory (or CCM) SRAM and the backup registers.
A read protection, for example, will prevent the dumping of embedded software code through an external access and will protect the developer's intellectual property.
A write protection will prevent certain Flash sectors from being accidentally erased by a load overflow in a software or data update procedure.
STM32G4 microcontrollers provide several features for protecting code and data located in Flash memory and backup registers.
In addition to these typical memory protections, the STM32G4 also introduces a new mechanism to ensure the safe execution of sensitive firmware.

The following slides will describe all these protection features.



The following means are provided for code protection purposes:
RDP: ReaDout Protection
PCROP: Proprietary code readout protection
WRP: Write protection
Secure User Memory protection is a new feature of STM32G4 microcontrollers. It ensures the safe execution of sensitive applications in addition to code and data protection.
Readout Protection, or RDP is a global mechanism that prevents external read access to Flash memory, option bytes, CCM SRAM and backup registers.
An external access can be gained by using a JTAG connector, a Serial Wire port or the boot software embedded in SRAM.
Three levels of RDP protection are defined from Level 0, which offers no protection at all, to Level 2 which has full

and permanent protection.
Protection levels will be described in the following slides.
PCROP is a memory access protection against code dumping. It is used to protect the intellectual property of the code.
The protected firmware remains executable but read and write access performed by the CPU executing malicious 3rd-party code (such as Trojan horse) are prohibited.

Key features

- **Write protection (WRP)**
  - Flash memory sectors protection against Write/Erase/Program access
  - Flash memory code with write protection attribute is protected against unwanted write or erase operations

Request	Permission
Read	YES
Write	NO
Execute	YES

- **Secure User Memory protection**
  - Flash memory area protection with specific access mechanisms for sensitive firmware execution
  - Code and data in this area are only accessible after reset
  - Code is executed prior to any other process
  - Once executed, the area is closed and cannot be access until the next reset

Request	Permission
Secure Read	YES
Non-Secure read	NO
Secure Write	YES
Non-Secure Write	NO
Secure Execute	YES
Non-Secure Execute	NO

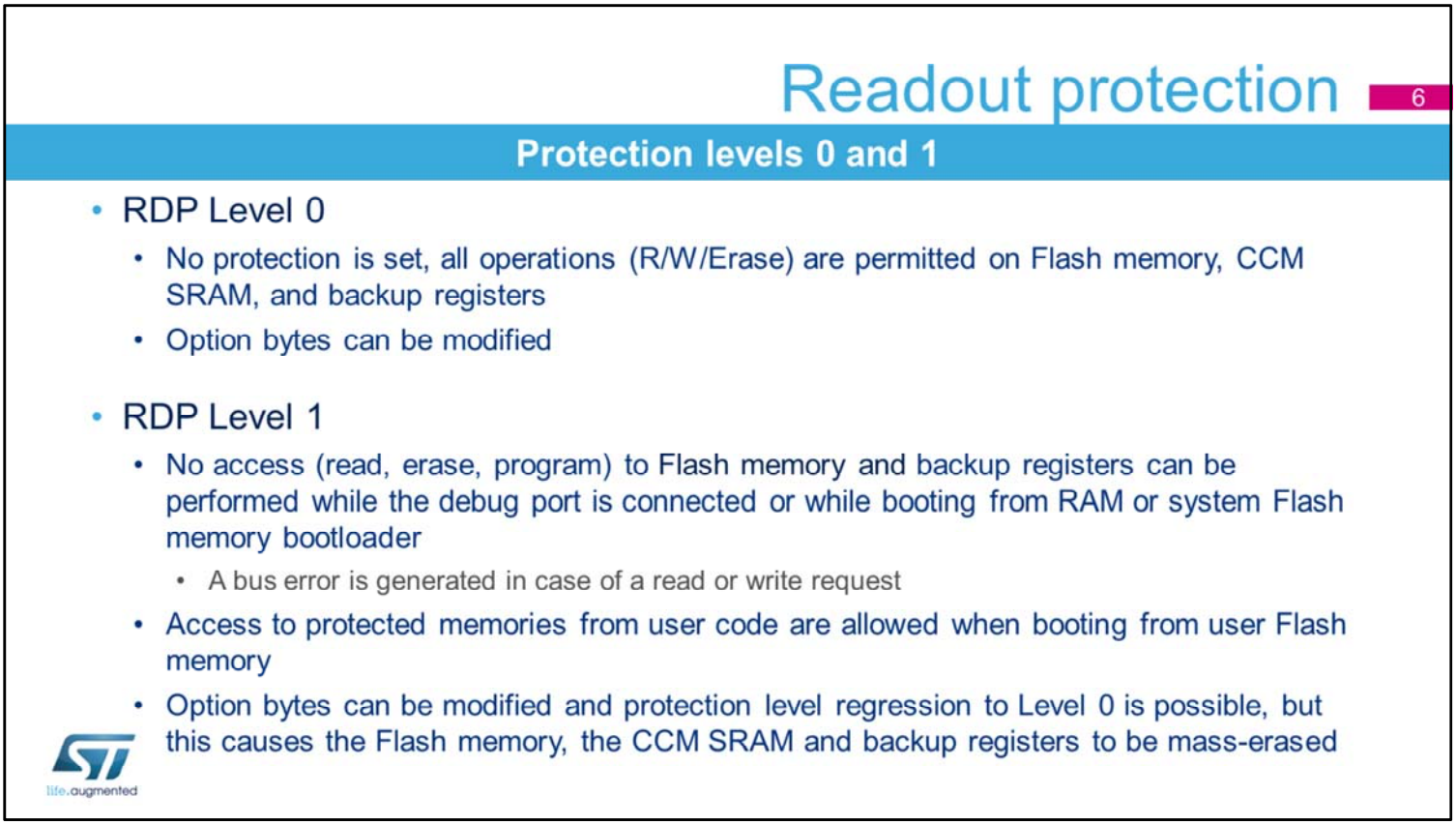
life.augmented

The write protection mechanism prevents accidental or malicious write/erase operations.
Secure User memory is a Flash memory area with a specific protection mechanism to ensure the safe execution of sensitive firmware in addition to code and data protection.
All protection mechanisms are configurable via the STM32G4 option bytes. Note that once the secure boot has been executed, the Secure User Memory is no longer accessible until the next reset.

Differences between STMG43X/4X and STM32G47X/8X

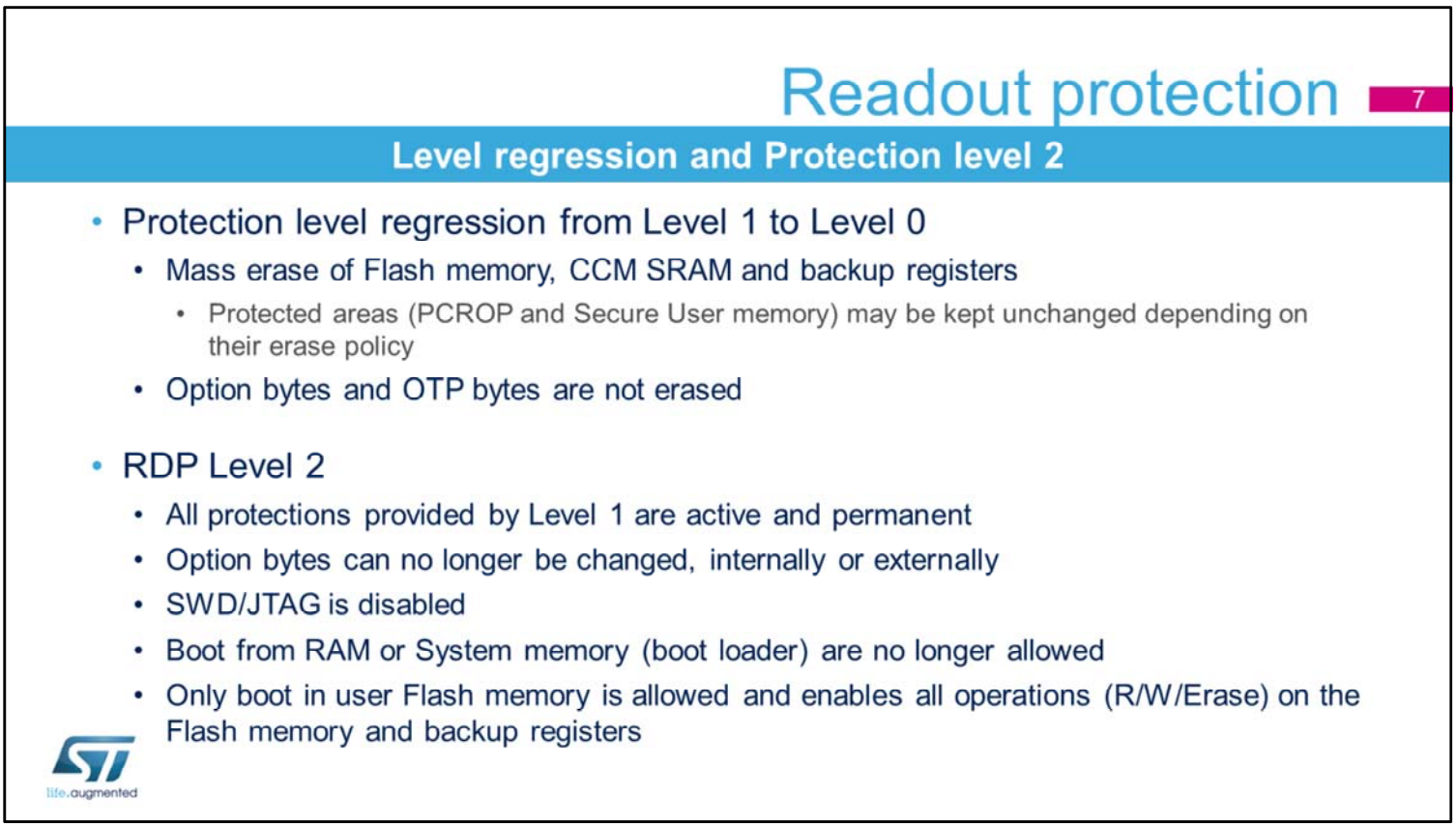
	STM32G43X/4X (Category 2)	STM32G47X/8X (Category 3)	
		FLASH_OPTR[DBANK]=0 (Single bank)	FLASH_OPTR[DBANK]=1 (Dual bank)
Number of banks	1	1	2
Page size	2-KB	4-KB	2-KB
Write Protect areas (WRPs)	2	4	2 per bank
Proprietary Code Read Protection Areas (PCROPs)	1	2	1 per bank
Securable memory area	1	2	1 per bank

This slide highlights the differences regarding the flash memory implementation between STM32G43X/4X, called category 2 microcontrollers, and STM32G47X/8X, called category 3 microcontrollers:
Number of banks is 1 for category 2, 1 or 2 for category 3, depending on the DBANK option bit.
The page size which provides the minimum erase granularity is 2 KB for category 2, 4 KB for category 3 with single bank and 2 KB for category 3 with dual bank.
Regarding protection features, the category 2 microcontrollers have 1 Write Protect area, 1 PCROP and 1 securable memory area while category 3 microcontrollers have 2 write protect areas, 2 PCROPs and two securable memory areas.



When the lowest RDP level, Level 0, is set, the device has no protection. All read or write operations (if no write protection is set) on the Flash memory, the CCM SRAM and the backup registers are possible in all boot configurations (such as Flash user boot, debug or boot from RAM).
Option bytes are also changeable in this level.
Level 0 is the factory default level.
In Level 1, read protection is set for the Flash memory, CCM SRAM and the backup registers.
In this level, protected memories are only accessible when booting from User Flash memory.
Whenever a debugger access is detected or boot is not set to a user Flash memory area, any access to the protected memories generates a system hard fault which blocks all code execution until the next power-on reset.
Note that option bytes can still be modified in this level,

making it possible to remove the protection. This mechanism is explained in the next slide.



We have seen in the previous slide that it is possible to modify option bytes in Level 1. It is then possible to remove the protection by changing the protection level to Level 0.

This protection level regression will cause the Flash memory, the CCM SRAM and the backup registers to be mass-erased. Flash areas protected by PCROP or configured as Secure User Memory can be erased or left unchanged depending on their erase policy configuration.

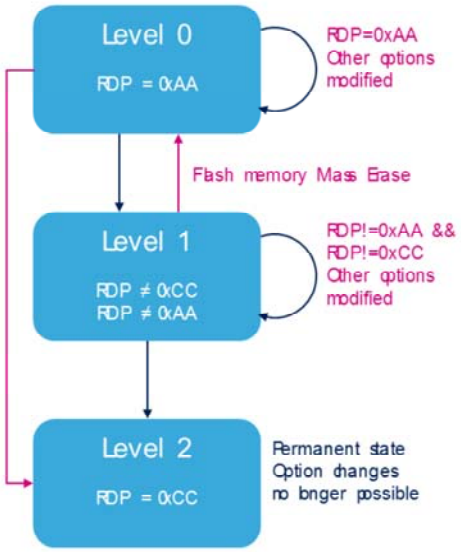
Readout protection Level 2 provides the same protection as in Level 1 but the protection becomes permanent. Option bytes cannot be modified, so once the RDP protection is set to this level, there is no way to modify it and level regression with mass-erase mechanism is no longer possible. This level must only be considered in the final product when the development stage is

completed.
Note that to ensure that there are no backdoors, this protection cannot be bypassed even at ST factory.

Readout protection

Transition scheme

- Level 0 / RDP= 0xAA
  - Option byte change is allowed
  - Transition to Level 1 or Level 2 possible
- Level 1 / RDP != (0xAA | 0xCC)
  - Option byte change is allowed
  - Transition to Level 0 with mass erase of user Flash memory, backup registers and CCM SRAM
  - Transition to permanent protection (Level 2) possible
- Level 2 / RDP = 0xCC
  - Option bytes are frozen
  - No transition possible



This slide shows the possible transitions between each readout protection level. It is always possible to raise the protection level but regression is only possible between Level 1 and Level 0.

When the RDP is reprogrammed to the value 0xAA to move from Level 1 to Level 0, a mass erase of the Flash main memory is performed. Backup registers and CCM SRAM are also erased. The OTP area is not affected by mass erase and remains unchanged.

If the bit PCROP_RDP is cleared in the FLASH_PCROP1ER register, the full mass erase is replaced by a partial mass erase that is successive page erases in the bank where PCROP is active, except for the pages protected by PCROP. This is done in order to keep the PCROP code.

Note that the RDP level is coded in one option byte; Level 0 is coded by a 0xAA value, Level 2 is coded by a

0xCC value and Level 1 is coded by any value other than 0xAA or 0xCC.

Readout protection

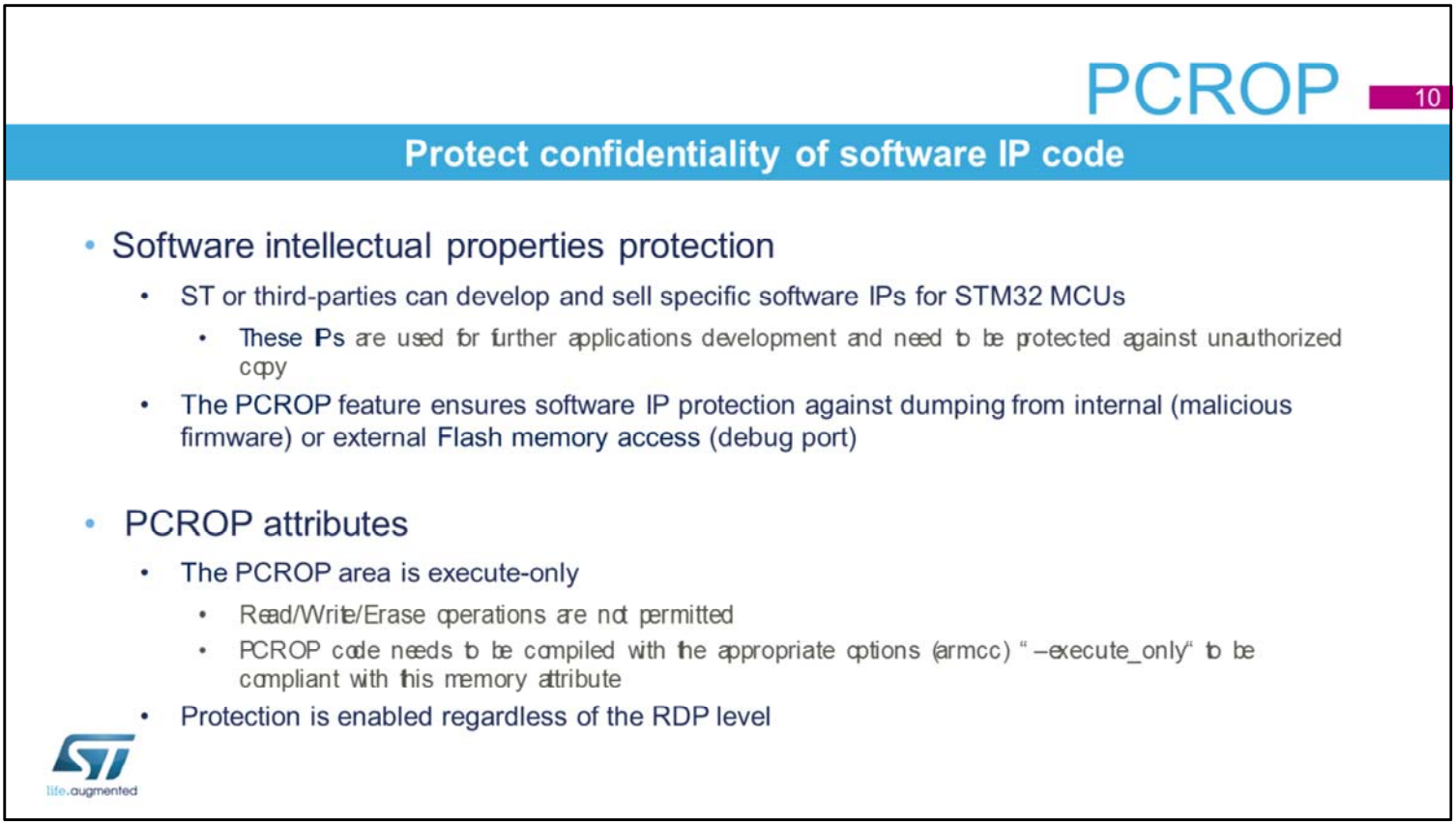
Summary

Area	Protection level (RDP)	Access rights when Boot in User Flash memory	Access rights when Boot from RAM or from bootloader or Debug Access detected
Main Flash memory	1	R/W/E	No Access
	2	R/W/E	NA, only boot in user flash memory is allowed
System Flash memory (Boot loader)	1	R	R
	2	R	NA, only boot in user flash memory is allowed
Option bytes	1	R/W/E	R/W/E
	2	R	NA, only boot in user flash memory is allowed
Backup registers	1	R/W	No Access
	2	R/W	NA, only boot in user flash memory is allowed
CCM SRAM	1	R/W	No Access
	2	R/W	NA, only boot in user flash memory is allowed
OTP	1	R/W	No Access
	2	R/W	NA, only boot in user flash memory is allowed

W: Write R: Read E: Erase

life.augmented

This table summarizes the different types of access authorized for the Flash memory and backup registers according to the readout protection (or RDP) level, configured boot mode and with debug access, as seen in previous slides.



PCROP means Proprietary code readout protection
Third-parties may develop and sell specific software IPs for STM32 microcontrollers and original equipment manufacturers may use them when developing their own application code. In order to protect the software intellectual property (or IP), the code must not be copied or read. The PCROP's purpose is to protect the confidentiality of 3rd-party software intellectual property code against malicious users independent of the RDP level setting.
The protected firmware can only be executed by the Cortex®-M4 core. Any other access (like DMA, debug and data read, write and erase) is strictly prohibited.
To be compliant with this constraint, the firmware must be compiled with the appropriate compilation option. For example: "–execute_only" (for Keil tools). Without this option, constants are interleaved with functions in the

read-only section, called the literal pool.
The Cortex-M4 MPU does not support execute-only access permissions.

Setting/Unsetting

- Setting
  - Each PCROP area is defined by a start page offset and an end page offset related to the physical Flash bank base address from 16 bytes or 32 bytes up to the full bank
  - PCROP areas are defined through option byte registers
- Resetting
  - The only way to deactivate PCROP is by RDP level regression from Level 1 to Level 0
    - This regression level will trigger a Flash memory mass erase operation
  - An additional option bit (PCROP_RDP) allows the selection of the PCROP areas to erase when the RDP protection is changed from Level 1 to Level 0

life.augmented

The proprietary code readout protected areas in Flash memory are defined through the option bytes.
Each PCROP area is defined by a start page offset and an end page offset related to the physical Flash bank base address from 16 bytes or 32 bytes up to the full bank, 16 bytes for category 2 devices and category 3 devices with dual bank, 32 bytes for category 3 devices with single bank.
The areas are protected against data accesses.
Note that sectors protected with the PCROP feature are also protected against Write access, offering protection against unwanted sector write or erase operations.
The PCROP protection can only be removed by a RDP level regression from Level 1 to Level 0. When executed, this mechanism triggers a full mass erase of the Flash memory.
Depending on the PCROP_RDP option bit, the PCROP

areas are erased when the RDP protection is changed from Level 1 to Level 0.

Flash memory write protection

12

Protects code and data from unwanted or accidental erasure

- Write protection attributes
  - Protected sectors cannot be erased or programmed
- Setting/Resetting
  - Protection is set independently for each page of the Flash memory
  - Protection is set in option byte registers
  - Write protection can be reset in RDP Level 0 and Level 1
    - It cannot be modified in RDP Level 2
  - If any page is write-protected, the level regression mechanism does not work
    - Write protection must be removed prior to a level regression and a Flash memory Mass Erase

life.augmented

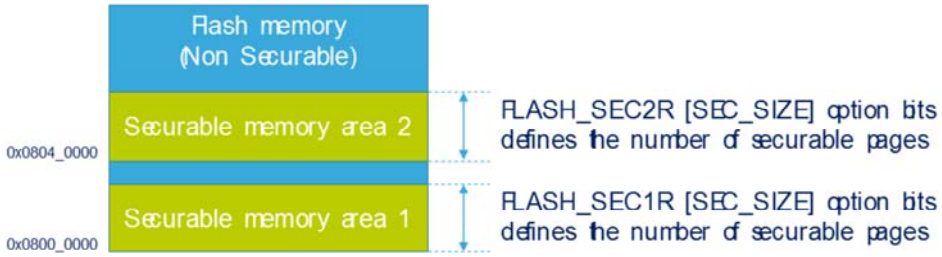
The write protection protects code and non-volatile data from unwanted or accidental erasure.
This protection is only available on the Flash memory.
The write protection can be set on a selection of Flash memory pages only.
When a page is protected, it cannot be erased or programmed. Any attempt to write-access the sector will cause a Flash memory error.
If at least one page is write-protected, a mass-erase of the Flash memory cannot be performed. The protection needs to be removed first.

Securable memory area

13

Introduction

- The main purpose of the securable memory area is to protect a specific part of Flash memory against undesired access
  - This allows implementing software security services such as secure key storage or safe boot



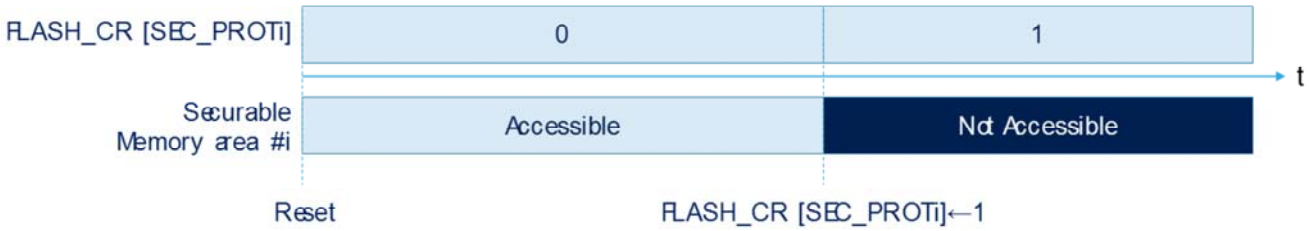
  - When FLASH_SECiR[SEC_SIZE] option bits are equal to zero, securable memory is not implemented
    - This field can only be modified in RDP Level 0

life.augmented

The purpose of the securable memory is to store code and data, available during the boot time, that become inaccessible once the boot program sets a control bit.
The typical use case consists in performing an authentication and possibly decryption of the software image present in the flash memory by using cryptographic keys contained in the securable memory.
The authentication and decryption programs are also stored in the securable memory.
Option bits are used to set the size of the securable memory in page units. Base address is always 0x0800_0000 for Securable memory area 1, which corresponds to Cortex-M4 reset vectors.
Securable memory area 2 starts at address 0x0804_0000.
When the SEC_SIZE field in the option bytes is equal to zero, securable memory is not implemented.

This field can only be modified in RDP Level 0.

Securable memory area



- By default, after a reset, the securable memory is accessible
  - Once the SEC_PROTi bit is set in FLASH_CR register, the securable memory number i becomes inaccessible until the next reset
  - Only a reset can clear the SEC_PROTi bit

life.augmented

When software sets the SEC_PROTi bit in the FLASH_CR register, the securable memory number i is no longer accessible.
In case of secure boot, used to perform image authentication and decryption, the SEC_PROTi bit is set to one when the authentication is successful, just before branching to the first instruction of the image.
Once the SEC_PROTi bit is set, it cannot be cleared by software. The only way to clear this bit is to apply a reset.

Securable memory area

- The content of the securable memory is erased upon changing from RDP Level 1 to Level 0, even if it overlaps with PCROP pages

Securable memory size (SEC_SIZE[6:0])	Securable memory ?	PCROP_RDP	Erased pages
0	NO	1	All (mass erase)
0		0	All but PCROP
>0	YES	1	All (mass erase)
>0		0	All but PCROP outside the securable memory area

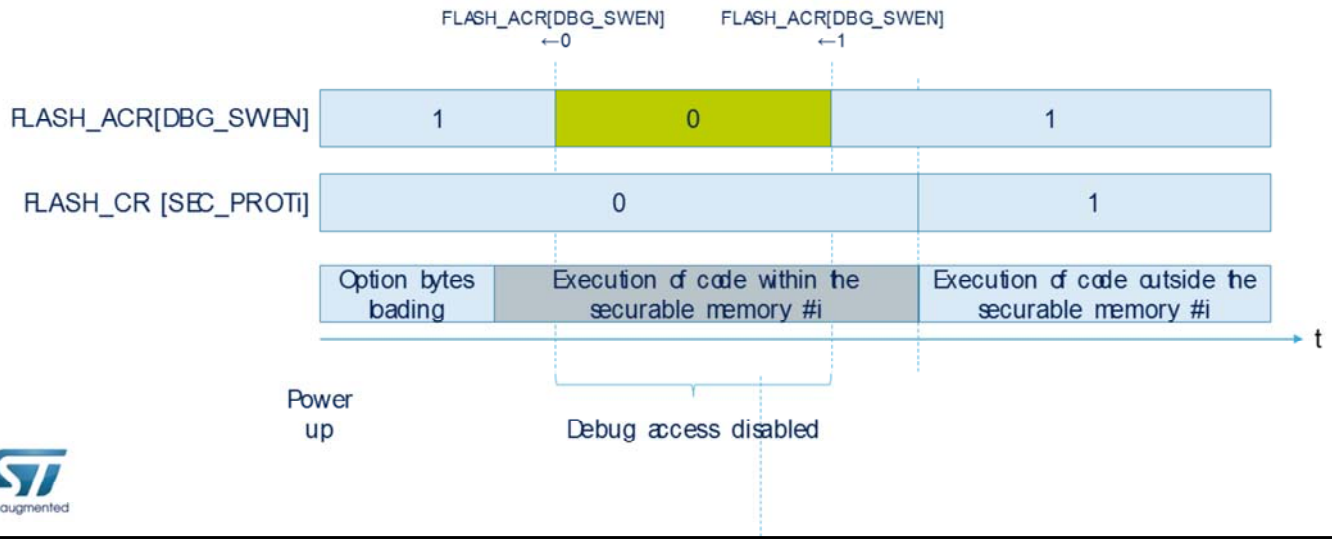
  - PCROP_RDP bit controls whether PCROP is preserved when RDP level decreases from Level 1 to Level 0:
    - =0: PCROP is not erased
    - =1: PCROP is erased

life.augmented

Of course code present in the securable memory may decide to erase a part or the securable memory. Furthermore, changing the Flash Read Protection level from Level 1 to Level 0 triggers the erasure of the securable memory.
Note that the code present in the securable areas can also be protected against read and write accesses, by mapping it into Proprietary Code Read Out Protection (or PCROP) areas.
Changing the RDP level from Level 1 to Level 0 will erase these PCROP areas, whatever the value of the PCROP_RDP bit. Only the contents of PCROP areas outside the securable memory address range will be preserved.

Disabling core debug access

- For executing sensitive code or manipulating sensitive data in securable memory area, the debug access to the core can temporarily be disabled



Taking control of the Cortex-M4 by using invasive debug can be temporarily disabled by programming appropriately the DBG_SWEN control bit.
For instance, the secure boot can decide to clear this bit before performing authentication/decryption and then to set this bit to one to re-enable invasive debug once the authentication is successful.

Forcing boot from Flash memory

- STM32G4 boot memories:
  - Embedded SRAM
  - System memory (bootloader)
  - Main Flash memory
- To increase the security and establish a chain of trust, the BOOT_LOCK option bit of the FLASH_SECR register allows forcing the system to boot from the Main Flash memory regardless the other boot options
  - It is always possible to set the BOOT_LOCK bit
  - Conditions to reset this bit:
    - RDP is set to Level 0, or
    - RDP is set to Level 1, while Level 0 is requested and a full mass-erase is performed

life.augmented

In the STM32G4, three different boot modes can be selected: boot from embedded SRAM, boot from system memory and boot from main Flash memory.
Executing a secure boot from securable memory implies that the boot area is the Flash memory. To disable the other boot areas, the BOOT_LOCK option bit has to be set in the FLASH_SECR register.
This option bit can be set unconditionally. However resetting is possible only when RDP level is zero or RDP is changed from Level 1 to Level 0, which causes a full mass-erase.

Related peripherals

- Refer to this training related to this peripheral:
  - STM32G4- Flash memory

life.augmented

Please refer to the Flash memory training to learn more about the memory architecture, option bytes and Flash memory operations.