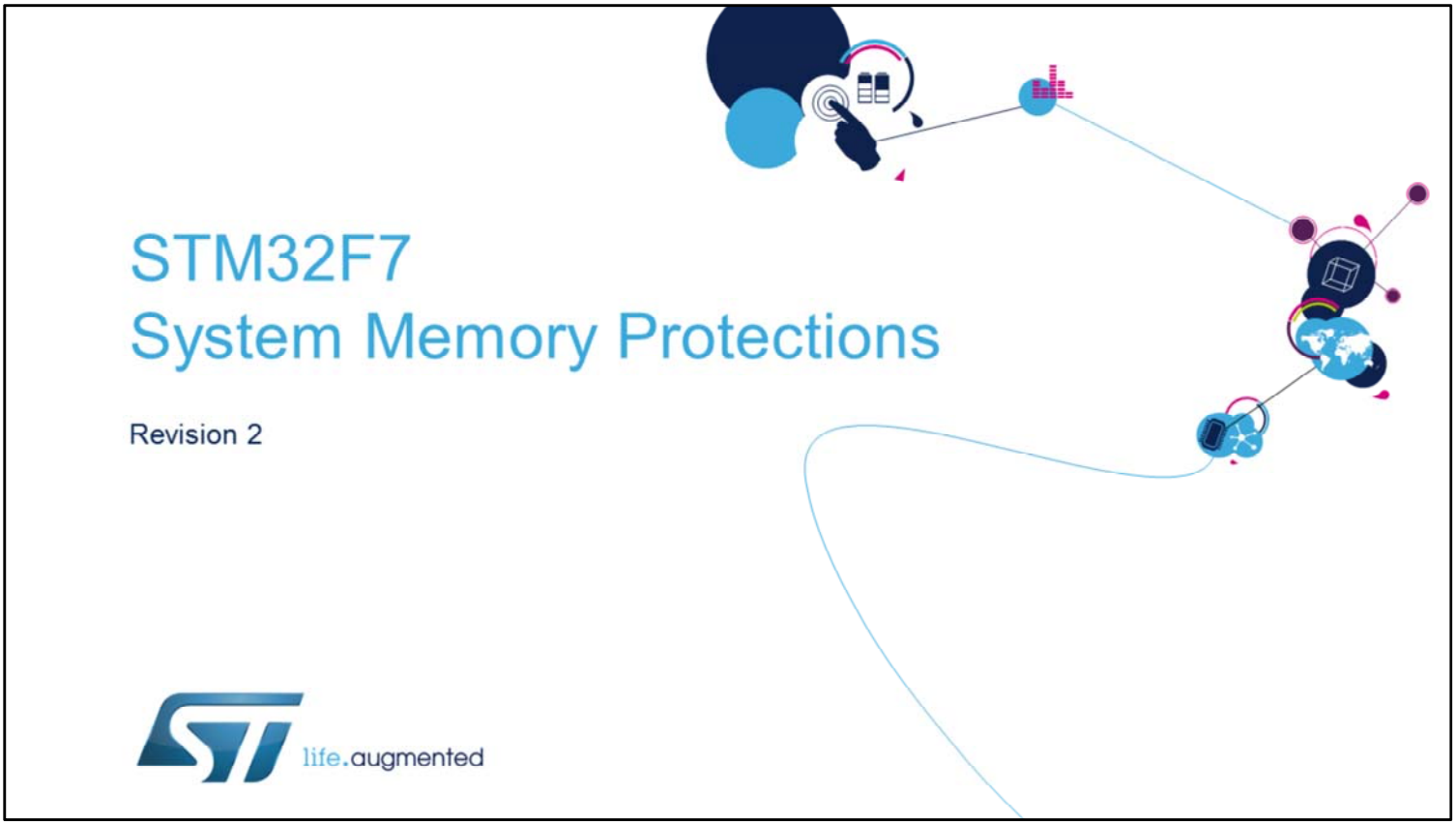
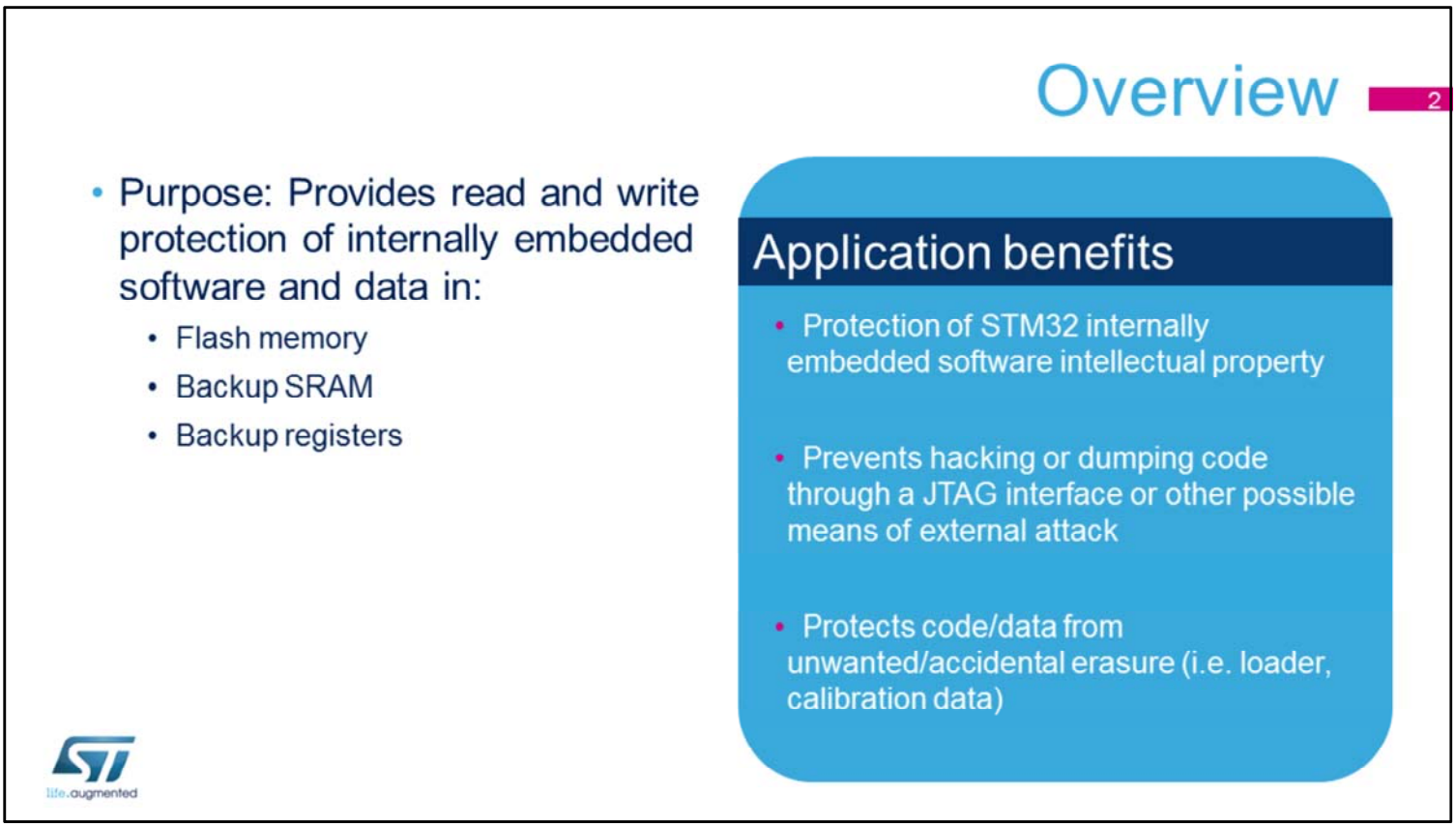
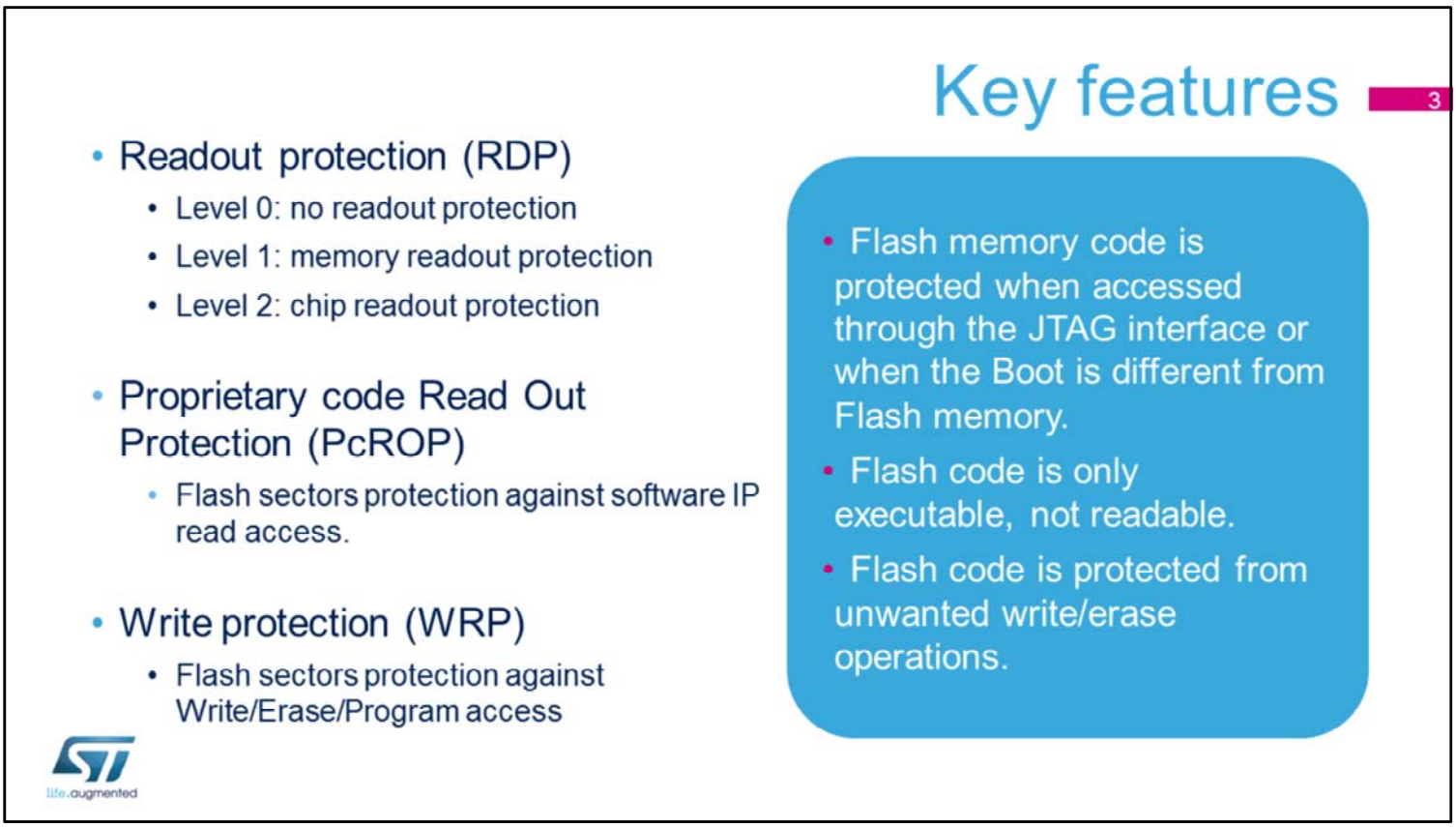


Hello and welcome to this presentation of the STM32 System Memories Protection. It will cover the different means for protecting code and data.



Memory protections have been designed for different purposes.
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 areas from being accidentally erased by a load overflow in a software or data update procedure.

STM32F7 microcontrollers provide several features for protecting code and data located in Flash memory, backup SRAM and backup registers.
The following slides will describe the read and write protection features.



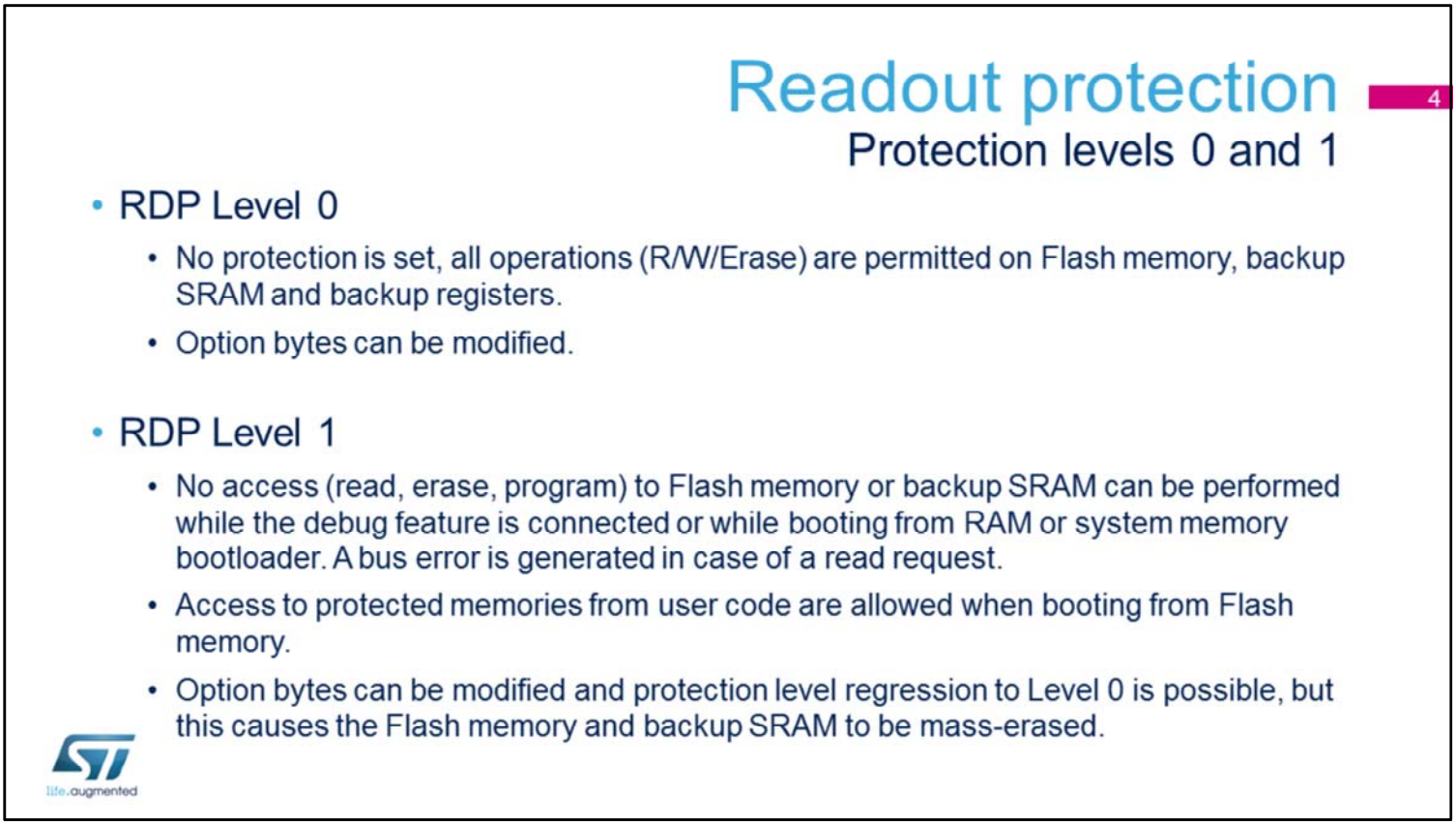
The following means are provided for code protection purposes:
RDP: ReaDout Protection
PcROP: Proprietary code readout protection
WRP: Write protection

Readout Protection, or RDP is a global mechanism that prevents external read access to Flash memory, backup SRAM and registers.
An external access can be gained by using a JTAG connector, a Serial Wire port or 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.

The second kind of memory protection available in STM32F7 is the PcROP.
PcROP prevents Read access of configurable Flash memory areas performed by the CPU executing malicious 3rd-party code (Trojan horse).
This protection can be set by Flash memory sectors of 16Kbytes, 64Kbytes or 128Kbytes.

Finally, the STM32F7 offers a write protection mechanism.
This protection prevents accidental or malicious write/erase operations.
As for PcROP, Write protection is set on specific memory sectors of the Flash memory.

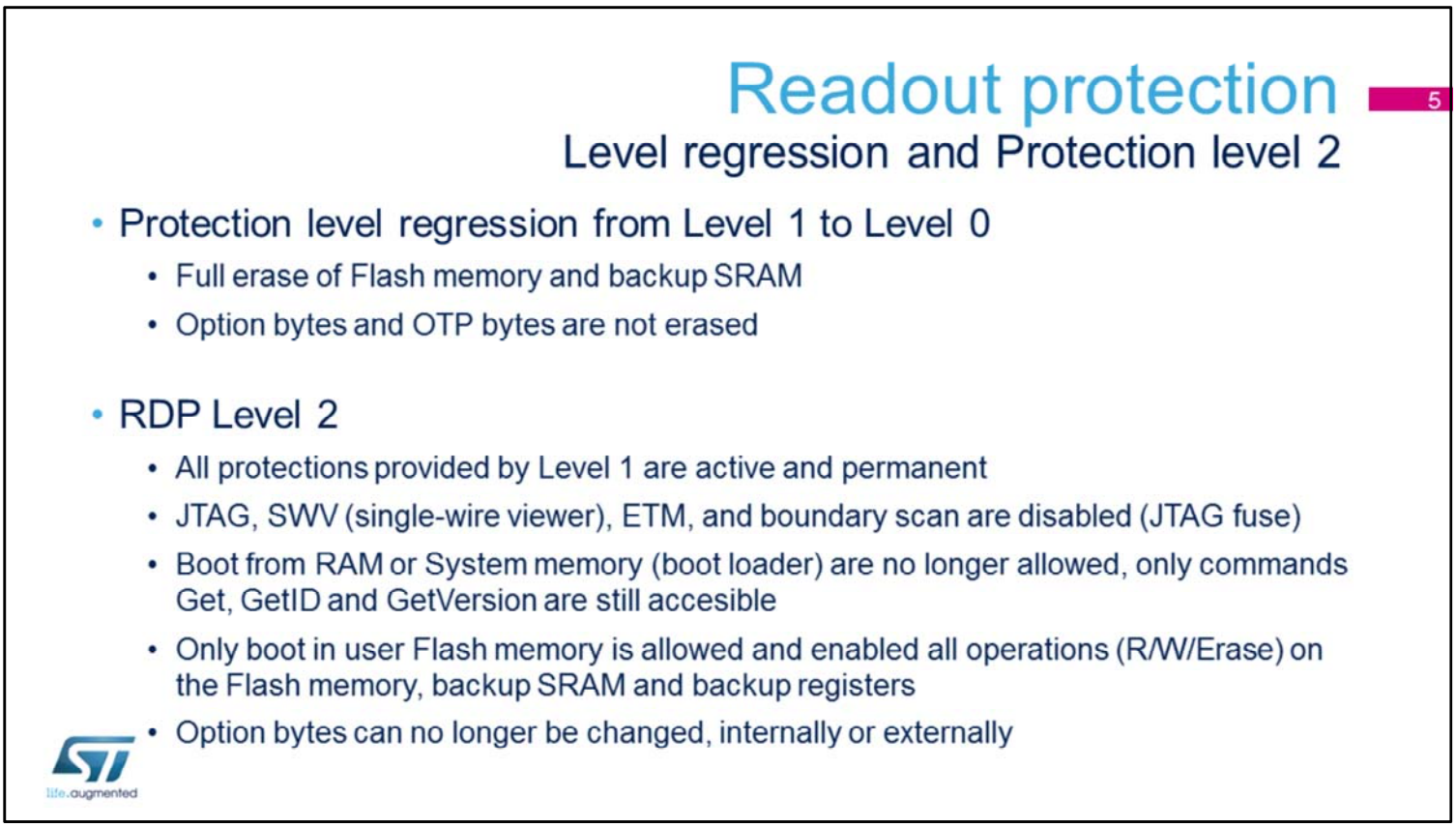
All protection mechanisms are configurable via the STM32F7 option bytes.



When first 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 or the backup SRAM are possible in all boot configurations (Flash user boot, debug or boot from RAM).
Option bytes are also changeable in this level.
Level 0 is is the factory default level.

In level 1, read protection is set for the Flash memory, the backup SRAM and the backup registers is set.
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 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.



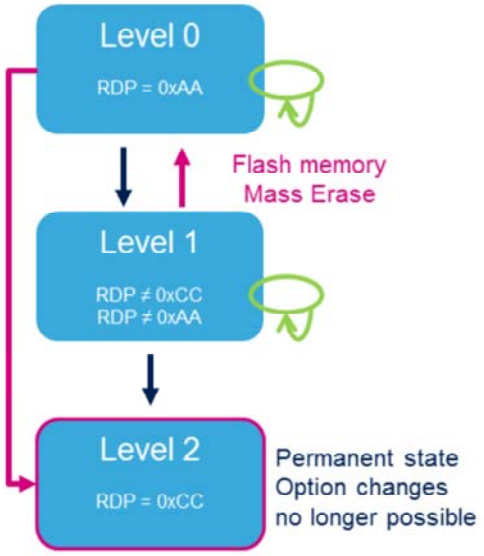
We have seen in the previous slide that it is possible to modify option bytes in Level 1. It is then possible to remove the protection by changing the protection level to Level 0. This protection level regression will cause the Flash memory and the backup SRAM to be mass-erased. Hence, no sensitive data can be retrieved.

Readout protection Level 2 provides the same protection as in Level 1 but the protection becomes permanent. Once the RDP protection is set to this level, there is no way to modify it. No level regression and mass-erase mechanism is 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 even 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 backup 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 with the consequence of a full User Flash Erase operation.
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 different other than 0xAA or 0xCC.

Readout protection

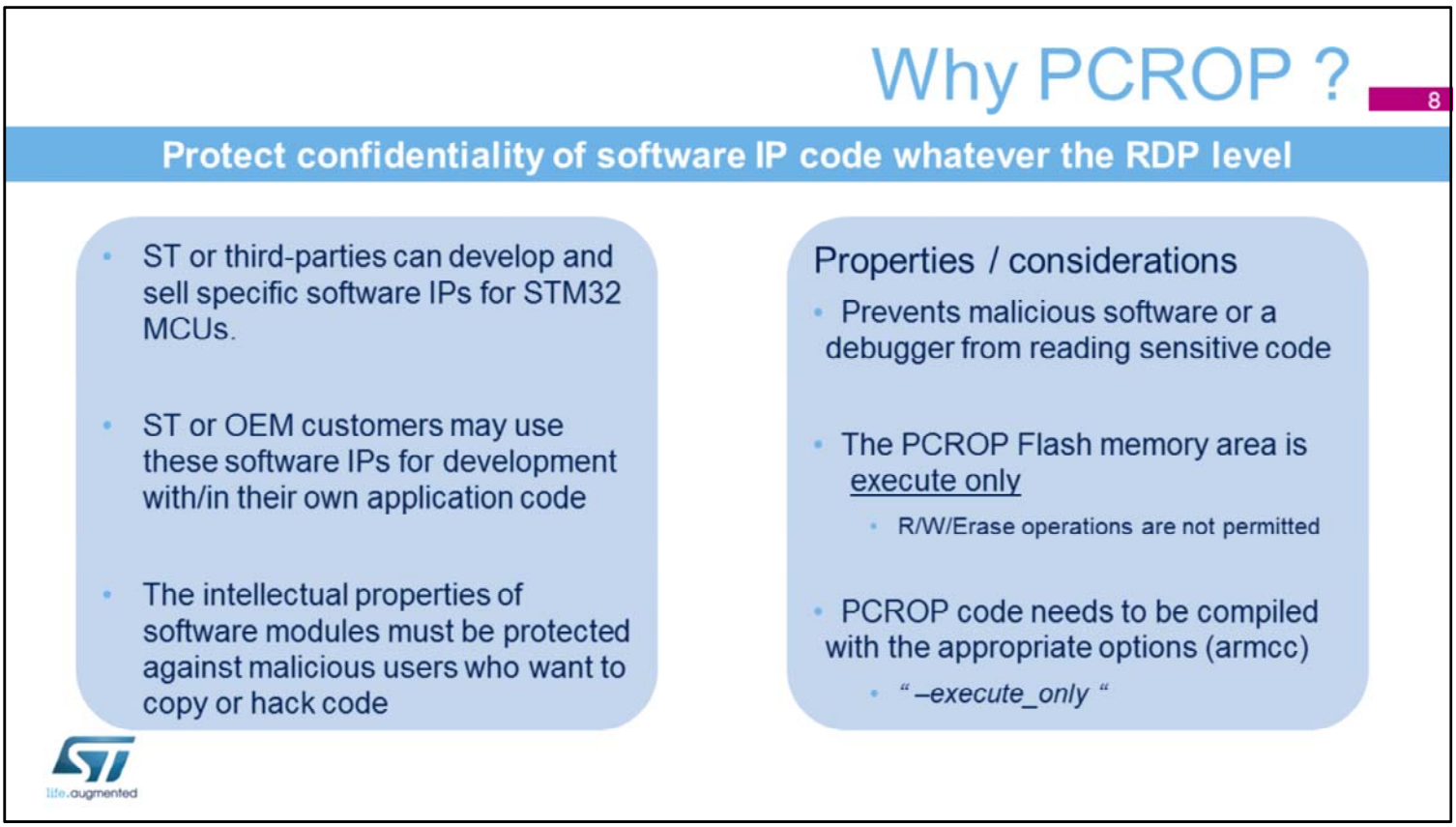
Summary

Area		Protection level (RDP)	Access rights when Boot = User Flash	Access rights when Boot ≠ User Flash or Debug Access detected
Flash memory	Main memory	1	R/W/E	No Access
		2	R/W/E	-
	Option bytes	1	R/W/E	R/W/E
		2	R	-
	OTP	1	R/W	No Access
		2	R/W	-
	Backup SRAM & backup registers	1	R/W	No Access
		2	R/W	-

W: Write R: Read E: Erase

life.augmented

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



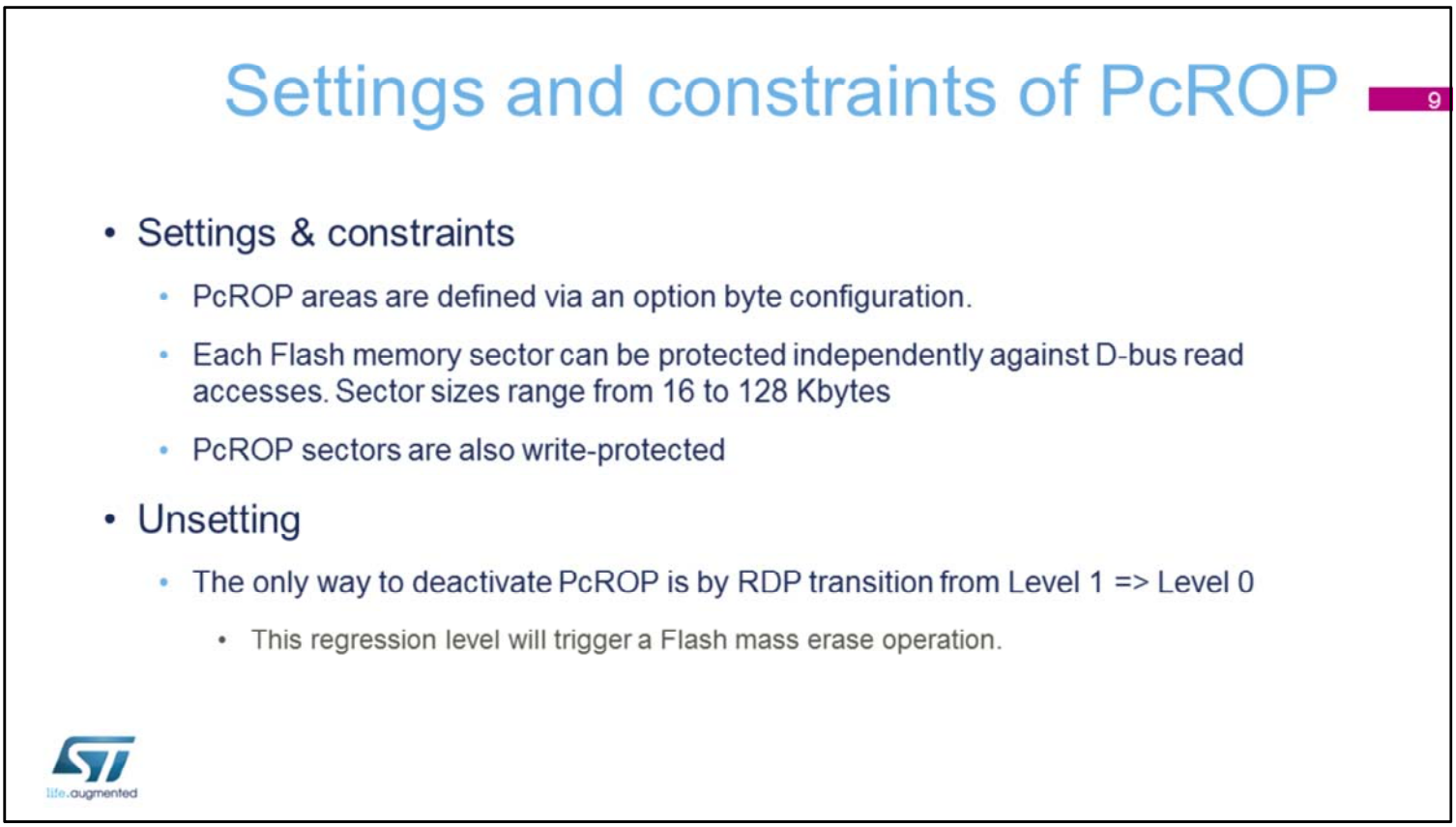
PcROP means : Proprietary code readout protection

Why PcROP ?

Proprietary code readout protection is basically a way to protect the confidentiality of 3rd-party software intellectual property code independently of the RDP level setting. 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. Proprietary code readout protection helps protect the confidentiality of 3rd-party IPs and protects software intellectual property against malicious users.

In other words, PcROP consists in preventing malicious software or debuggers from reading sensitive code. The protected area is execute-only and can only be reached by the STM32 CPU, as an instruction code, while all other accesses (DMA, debug and CPU data

read, write and erase) are strictly prohibited. This means that the code to be protected must be compiled using a specific compiler option:
For example: “–execute_only” (for Keil tools)



The proprietary code readout protected areas in Flash memory are defined through the option bytes.
Sectors of Flash memory can be independently protected against read access through the data-bus. Only an instruction bus can access the protected sector for code execution.
Note that sectors protected with the PCROP feature are also protected against Write access, offering protection against unwanted sector write or erase operations.

Removing PCROP protection can only be done by a RDP regression level from level 1 to level 0. When executed, this mechanism triggers a full mass erase of the Flash memory.

Flash write protection

10

- Protects code and data from unwanted or accidental erasure
- Protection available on Flash memory sectors.
  - Protection granularity is the sectors size (16, 64 or 128 Kbytes)
- Protected sectors cannot be erased or programmed
- If any sector is write-protected, the level regression mechanism does not work.
  - Write protection must be removed prior to a level regression and a Mass Flash 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. Unlike Readout protection, the write protection can be set on a selection of Flash memory sectors only.
There are 8 sectors defined in STM32F7: 4 sectors of 16Kbytes, 1 sector of 64Kbytes and 3 sectors of 128 Kbytes.

When a sector 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 sector is write-protected, a mass-erase of the Flash memory cannot be performed. The protection needs to be removed first.

Related peripherals

11

- Refer to this training related to this peripheral:
  - STM32F7 Flash memory

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