Hello and welcome to this presentation of the STM32 System Memories Protection. It will cover the different means for protecting code and/or data from external and/or internal attacks.

Overview

- Purpose

Provides read and write protection of internally embedded software and/or data in:

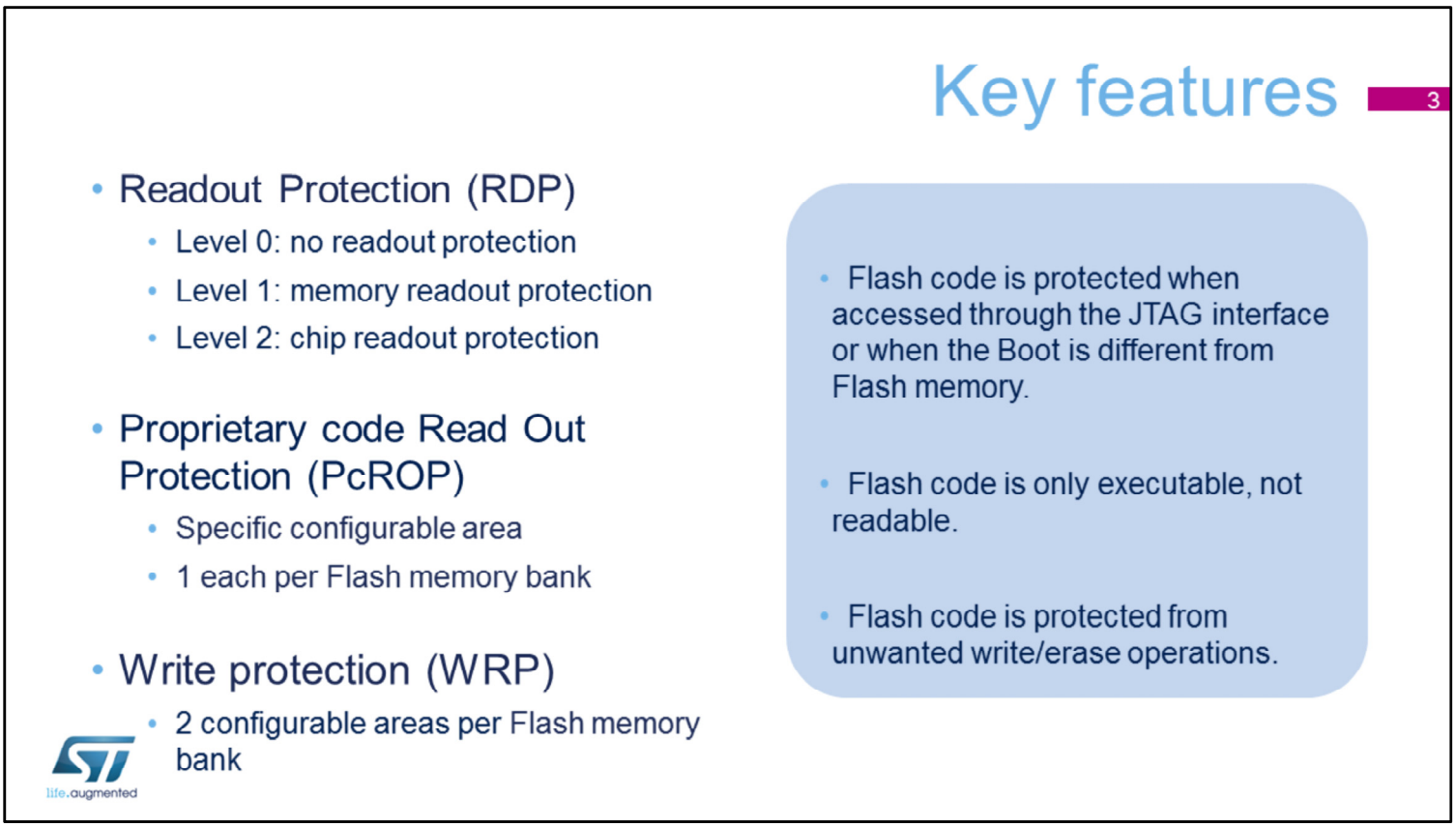
- Flash memory
- SRAM2 (new)
- Backup registers

Application benefits

- Protection of STM32 internally embedded software intellectual property
- Prevents hacking code or dumping code through JTAG interface or other possible means of external attack
- Protects code/data from unwanted/accidental erasure (i.e loader, calibration data)

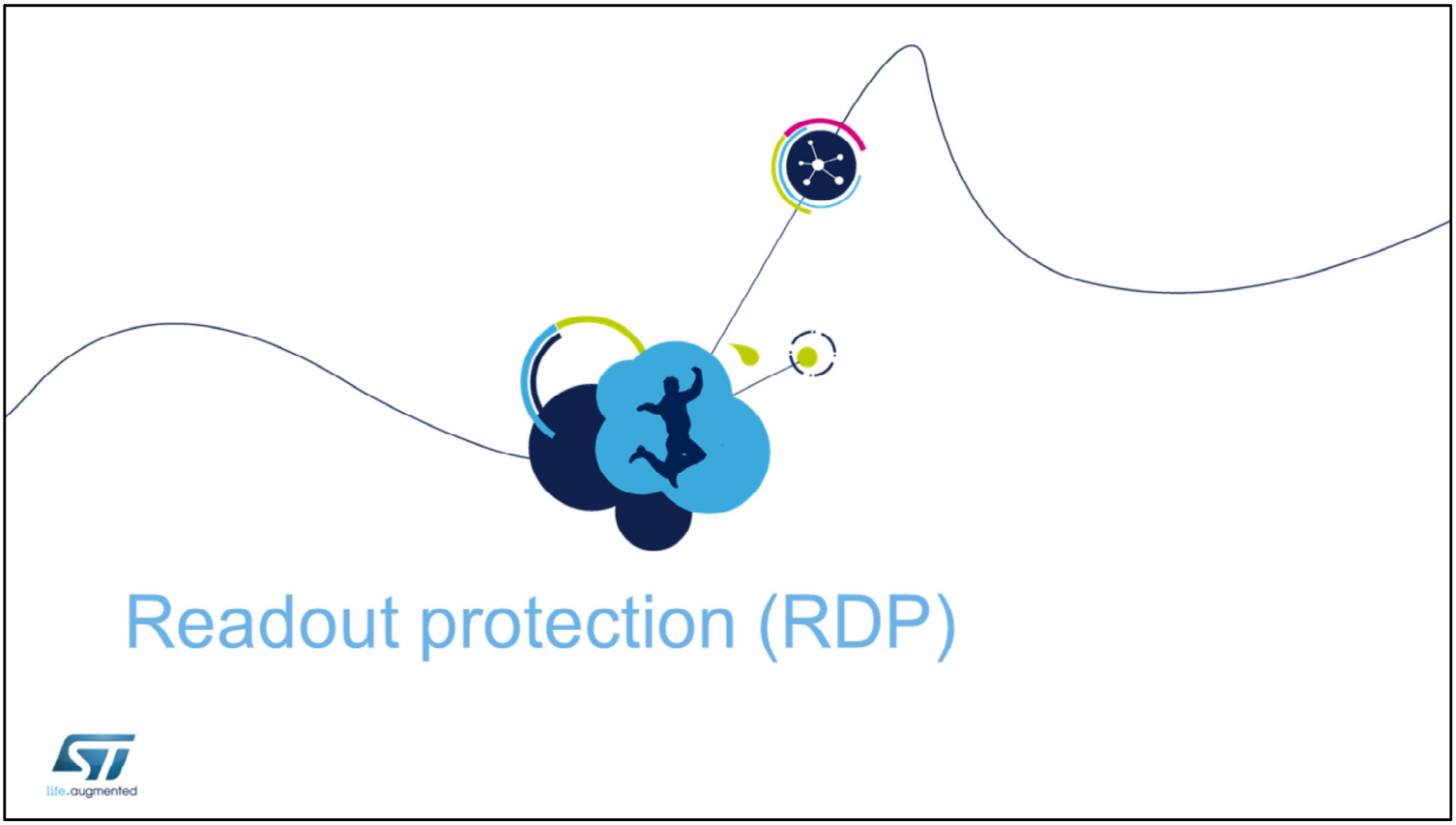
life.augmented

Software providers may need to protect their software intellectual propriety from malicious users or from intrusive attacks.
For this purpose, STM32L4 microcontrollers provide a couple of features for protecting code and/or data located in either Flash memory, SRAM2 or Backup registers.
These features can prevent the reading or writing of code and/or data through the JTAG debugger, end-user code, or SRAM Trojan code.



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

These features are configurable via the STM32L4 option bytes:
RDP: Prevents Flash memory access through the JTAG for ALL Flash memory.
PcROP: Prevents Read access of configurable Flash memory/SRAM areas performed by the CPU executing malicious 3rd-party code (Trojan horse).
WRP: Prevents accidental or malicious write/erase operations.



Let’s take a closer look at the details of the readout protection feature.

Readout protection (1/2)

- Readout protection Level 0 (no protection, factory default)
  - All operations (R/W/Erase) are permitted on Flash memory, SRAM2 (new), and Backup registers.
  - Option bytes can be modified.
- Readout protection Level 1
  - If the selected boot mode is user Flash (Boot0 = 0), and if no debugger access is detected (no JTAG):
    - All operations (R/W/Erase) are permitted on the Flash memory, SRAM2 (new), and Backup registers. Option bytes can be modified.
  - If the selected boot mode is not user Flash (Boot0 = 1), or if a debugger access is detected (JTAG):
    - ALL operations (R/W/Erase) to Flash memory, SRAM2 (new), and Backup registers are blocked (hard fault generated). Option bytes can be modified.

life.augmented

The STM32L4 readout protection feature offers three levels of protection for all SRAM2 and Flash memory as well as the backup registers:
- Level 0 means “no protection”. This is the factory defaultRead, Write and Erase operations are permitted in the SRAM2 and Flash memory as well as the backup registers. Option bytes are changeable in Level 0.
- Level 1 ensures total read protection of the chip’s memories which includes the Flash memory and the backup registers as well as a new feature to the STM32 family, the SRAM2 content.

Whenever a debugger access is detected or Boot mode is not set to a Flash memory area, any access to the Flash memory, the backup registers or to the SRAM2 generates a system hard fault which blocks all code execution until the next power-on reset. Please note that option bytes can still be modified in Level 1.

Readout protection (2/2)

- Readout protection Level 2 (JTAG fuse)
  - All protections provided by Level 1 are active.
  - Boot from RAM or System memory (boot loader) is no longer possible (only from User Flash memory).
  - The JTAG interface is disabled, debugging/programming via the JTAG/SWD is no longer available (JTAG killed).
    - Factory FARs are limited, ensuring there is no backdoor.
  - If the selected boot mode is User Flash memory
    - All operations (R/W/Erase) are permitted on the Flash memory, backup registers and SRAM2
  - Option bytes can no longer be changed, internal or external (Level 2 forever)
- Un-protection (Level 1 only)
  - The protection regression is only possible for the RDP transition from Level 1 to Level 0. The resulting consequence is the complete erase of the Flash memory, backup registers and SRAM2.

life.augmented

Level 2 provides the same protection features for the SRAM2, Flash memory and Backup registers as described for Level 1. However, there are three major differences.
The JTAG/SWD debugger connection is disabled (even at the ST factory, to ensure that there are no backdoors), the Boot mode is forced to User Flash memory REGARDLESS of what the boot 0/1 settings are, and Level 2 is permanent. Once set to Level 2, there is no going back; RDP/WRP option bytes can no longer be changed, as well as ALL the other option bytes.
Changing the level of RDP protection is only permitted when the current protection level is ‘1’. Changing the protection level from ‘1’ to ‘0’ will automatically erase the entire user flash memory, SRAM2 and backup registers.

Access status vs. readout protection level

7

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	-
	System memory	1	R	R
		2	R	-
	Option bytes	1	R/W/E	R/W/E
		2	R	-
	Backup registers	1	R/W	No Access
		2	R/W	-
	SRAM2	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 SRAM2 according to the readout protection (RDP) level, configured boot mode and debug access, as previously discussed. In summary:

- When RDP is set to Level 0, no protection mechanism is active an all memories can be read and modified.

- When RDP is other than level 0:

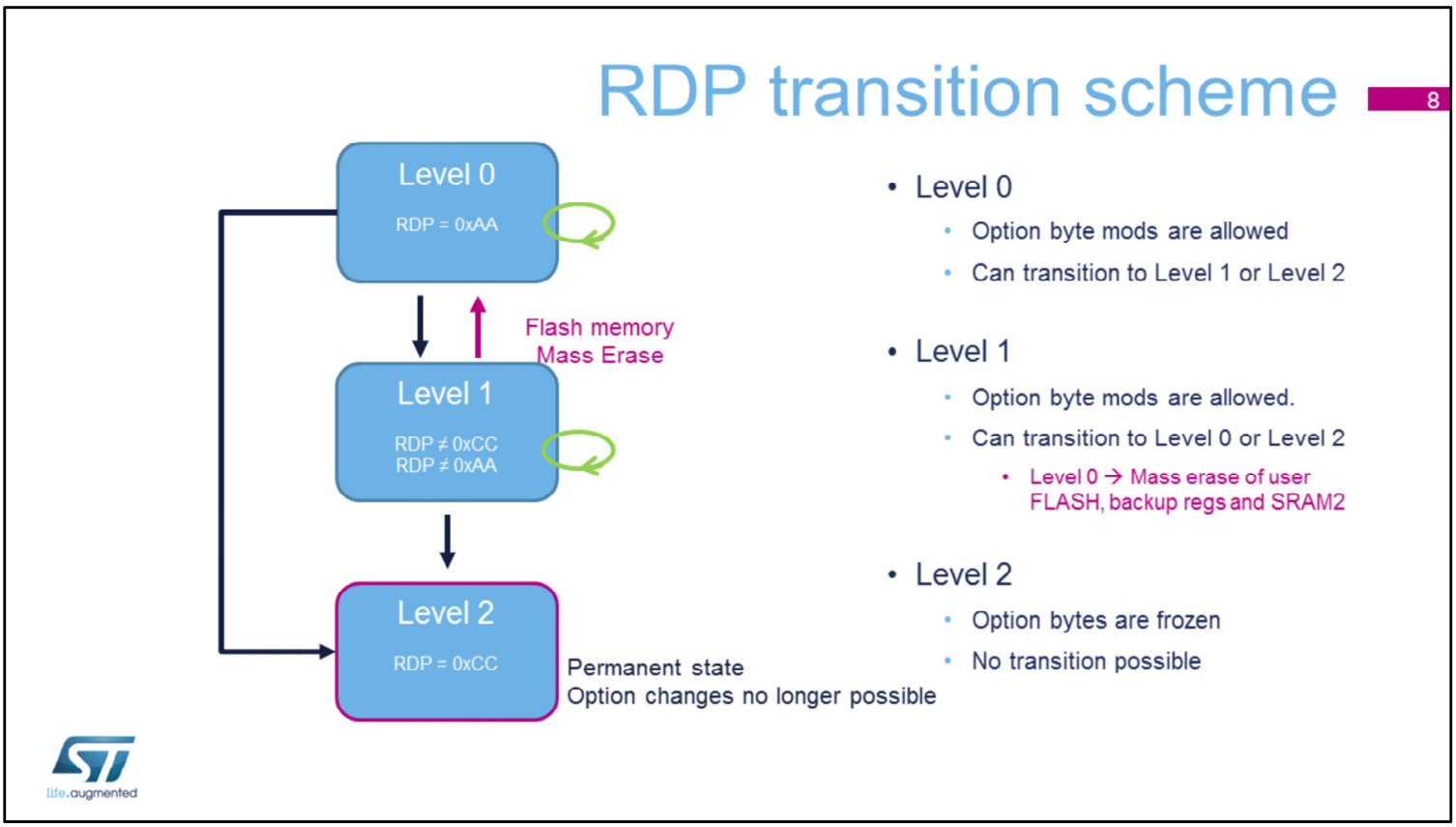
If the device is configured to boot from the User Flash memory, THEN:

=> The User Flash memory, backup registers and SRAM2 can be read or modified regardless of the RDP level.

=> The System Flash memory can be read only.

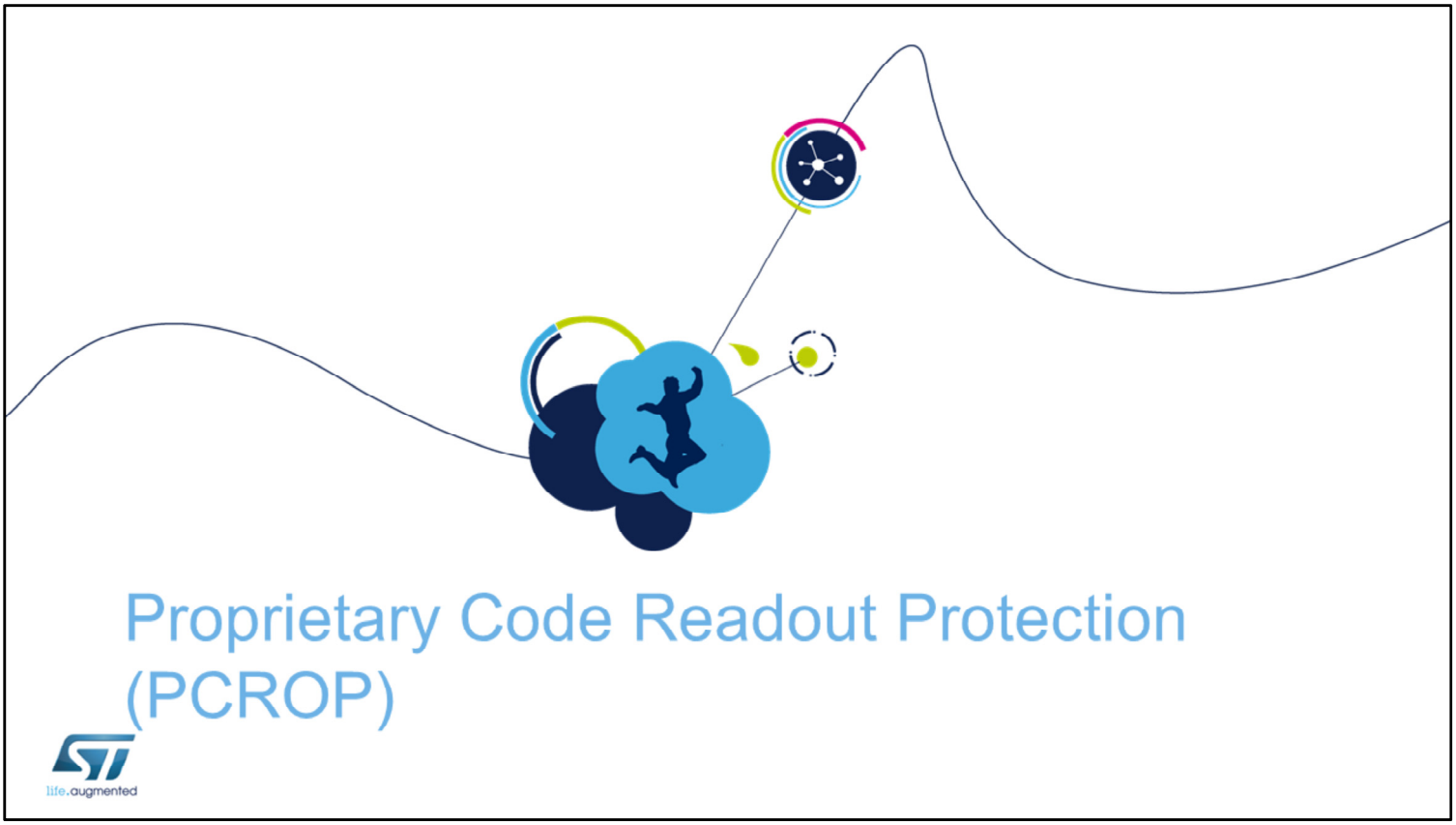
=> The Option bytes can be read only when the RDP is set to Level 2.

Otherwise, if the device is not configured to boot from the User Flash memory or if a debugger access is detected, THEN:
=> Almost all memories are not accessible excepted the System Flash memory, which can only be read in Level 1, and Option bytes which can be read or modified in Level 1.

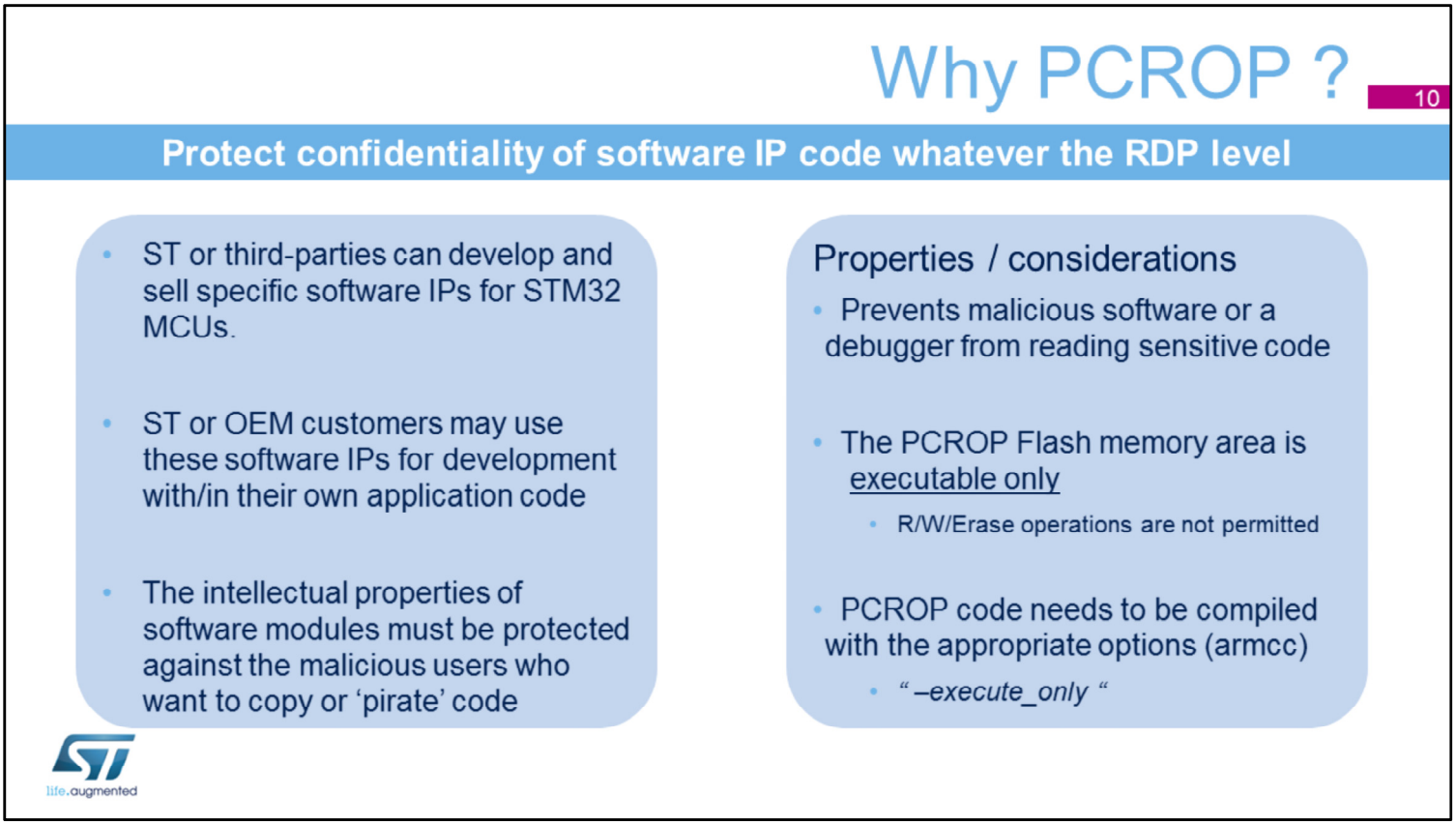


Let's look at the transitions possible between each readout protection level.
As already mentioned, STM32L4 MCUs have three RDP levels:
- Level 0 means there is no memory protection and option bytes can be modified.
- From Level 0, the device can move to Level 1 or Level 2.
- Level 1 ensures the memory protection while keeping debug access enabled.
- From Level 1, the device can move to Level 0 or Level 2. Regression to Level 0 will cause a Flash memory Mass Erase.
- Level 2 ensures the memory protection the same as Level 1, but completely disables JTAG/SWD debug access.
- Level 2 is a permanent state, and moving to another

RDP level is not possible.



Let’s take a closer look at the details of the Proprietary Code Readout Protection (PCROP) and how it’s different from RDP.



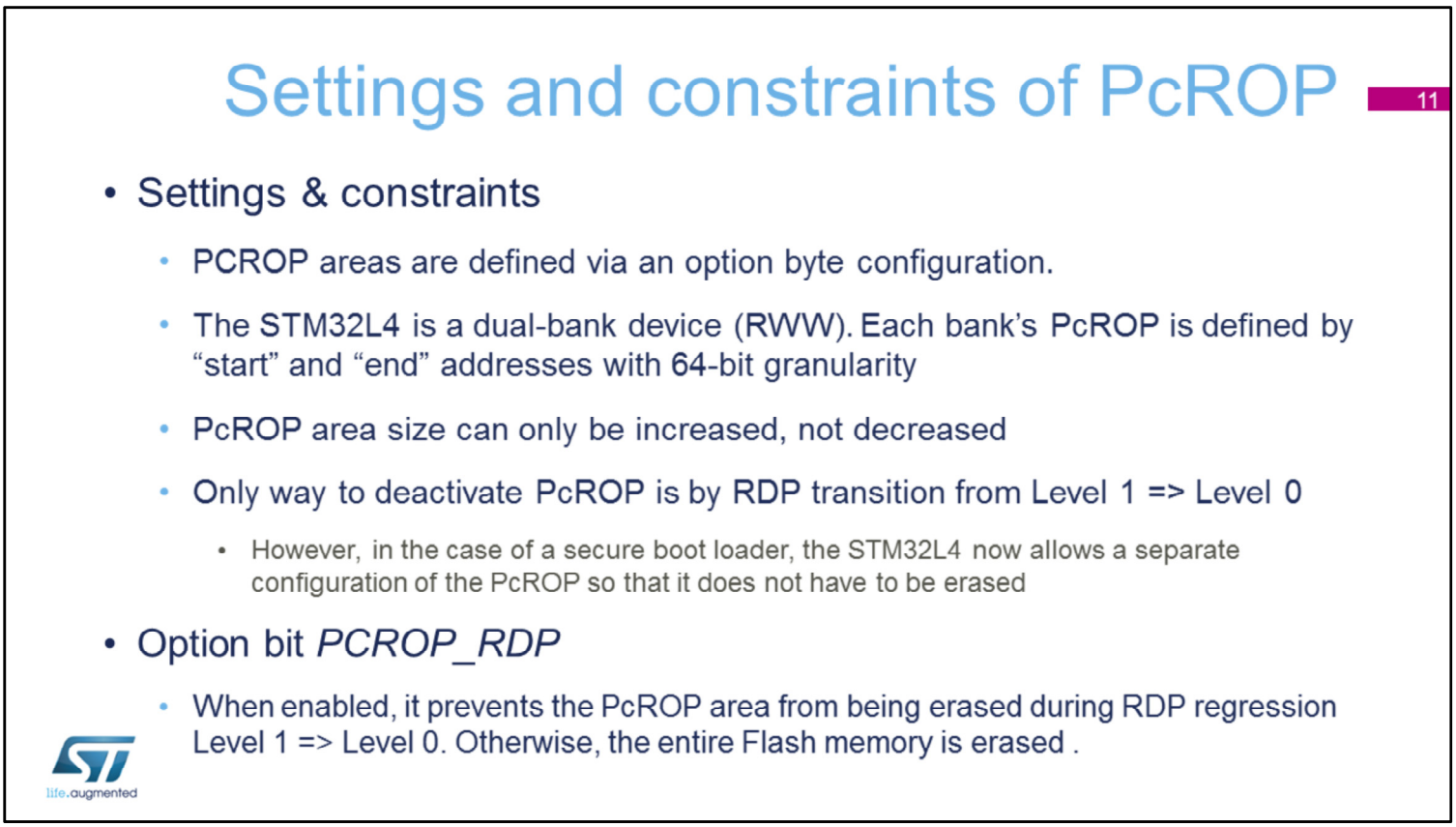
PcROP means : Proprietary code readout protection

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)

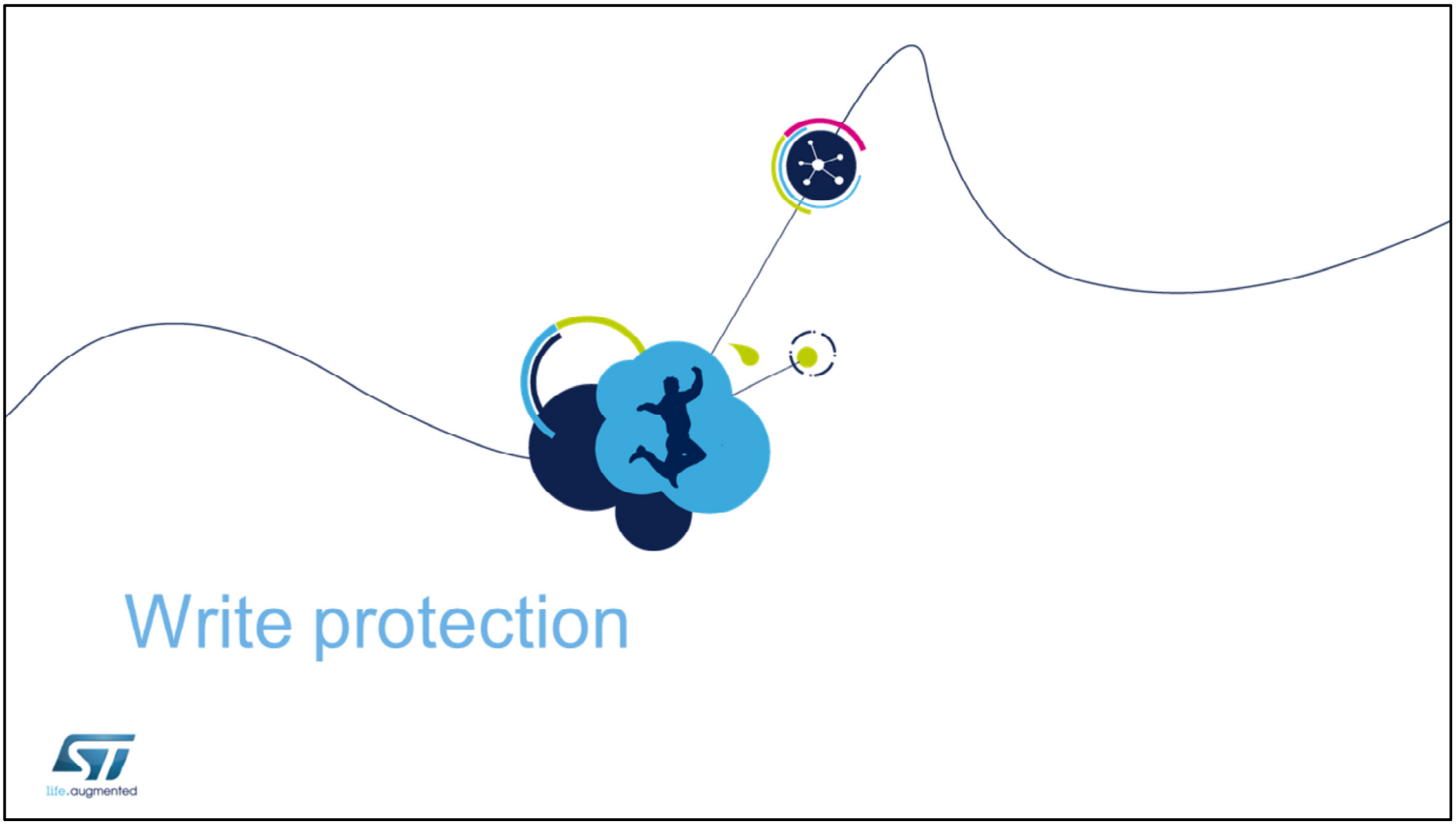


The proprietary code readout protected areas in Flash memory is defined through the option bytes.
The PcROP feature is improved on the STM32L4 devices. Two separate PcROP areas can now be set independently (one per bank), each one defined by a start and end address with a granularity of 64 bits. Note that once a PcROP area is configured, its size can only be increased.
Once the PcROP areas have been defined, the only way to disable this protection feature is to change the RDP protection level from '1' to '0', which erases the entire Flash memory

STM32L4 microcontrollers have a new feature that prevents the code in the PcROP areas from being erased during the regression operation. By setting the PCROP_RDP bit in the option bytes, the code in the

PcROP areas will NOT be lost.

To further explain the ‘execute only’ meaning of the PcROP:
- The PcROP is a sub-state of the RDP. The PcROP is designed to prohibit other code executing on the STM32 from reading the Flash memory. This is not the same as the RDP, where the protection targets external worlds. When the PcROP is enabled, the AHB only allows the Instruction bus to work, so code can only be executed. The Data bus can’t access that Flash memory.
- Once the development phase is completed, the PCROP can then be turned into a RDP setting, Level 1. In this case, the external world is limited to read-only. But the PcROP settings for specific sectors stills applies to all masters trying to read that code.



Now, let’s take a closer look at the details of the write protection settings of the STM32L4.

Flash write protection

- Settings & constraints
  - The write-protected area is defined through the option bytes
  - The STM32L4 allows 2 WRP areas per bank to be configured (4 total areas).
    - Each WRP area is defined by “start” & “end” addresses with a granularity of 2 Kbytes
      Other STM32 devices allow WRP on a per sector basis.
  - The WRP area size can be modified (option byte changed) whenever the RDP is not Level 2.
- Properties
  - When a WRP area is defined/enabled, write/erase operations are not permitted on this area.

life.augmented

The Flash memory write protection mechanism is designed to prevent unwanted write access to defined areas in Flash memory, such as boot loader or calibration constants that do not change.
The write protection areas are defined through the option bytes. The user can define up to four different write-protected Flash memory areas independently (two per bank). Each of the four Flash memory areas are defined by a start and end address with a granularity of 2 Kbytes. The size of the write areas can be modified whenever the RDP level is not set to Level 2.
Erase operations are treated as write operations on write protected areas, meaning they are not allowed.

SRAM write protection

- Settings & constraints
  - The SRAM 2 write-protected area is configured through the system configuration registers. The write-protection feature for the SRAM is new to the STM32 devices.
  - The STM32L4 allows 1 WRP area for the entire SRAM2..
    - As with the Flash memory WRP area, the SRAM2 is defined by “start” & “end” addresses with the granularity of 2 Kbytes.
- Properties
  - When the SRAM2 write-protection area is defined/enabled, write operations to the area are not permitted.
  - When regression occurs (RDP Level 1 → Level 0) with the SRAM2 WRP area defined, the SRAM2 WRP content is erased.

life.augmented

The write protection area of the SRAM2 is configured through the system configuration registers. Only one area can be set using the Start and End address registers. The address granularity is 2 Kbytes.
As with the Flash memory, write operations on the protected area is not permitted.
When regressing from RDP Level 1 to Level 0, the entire content of SRAM2 is erased.