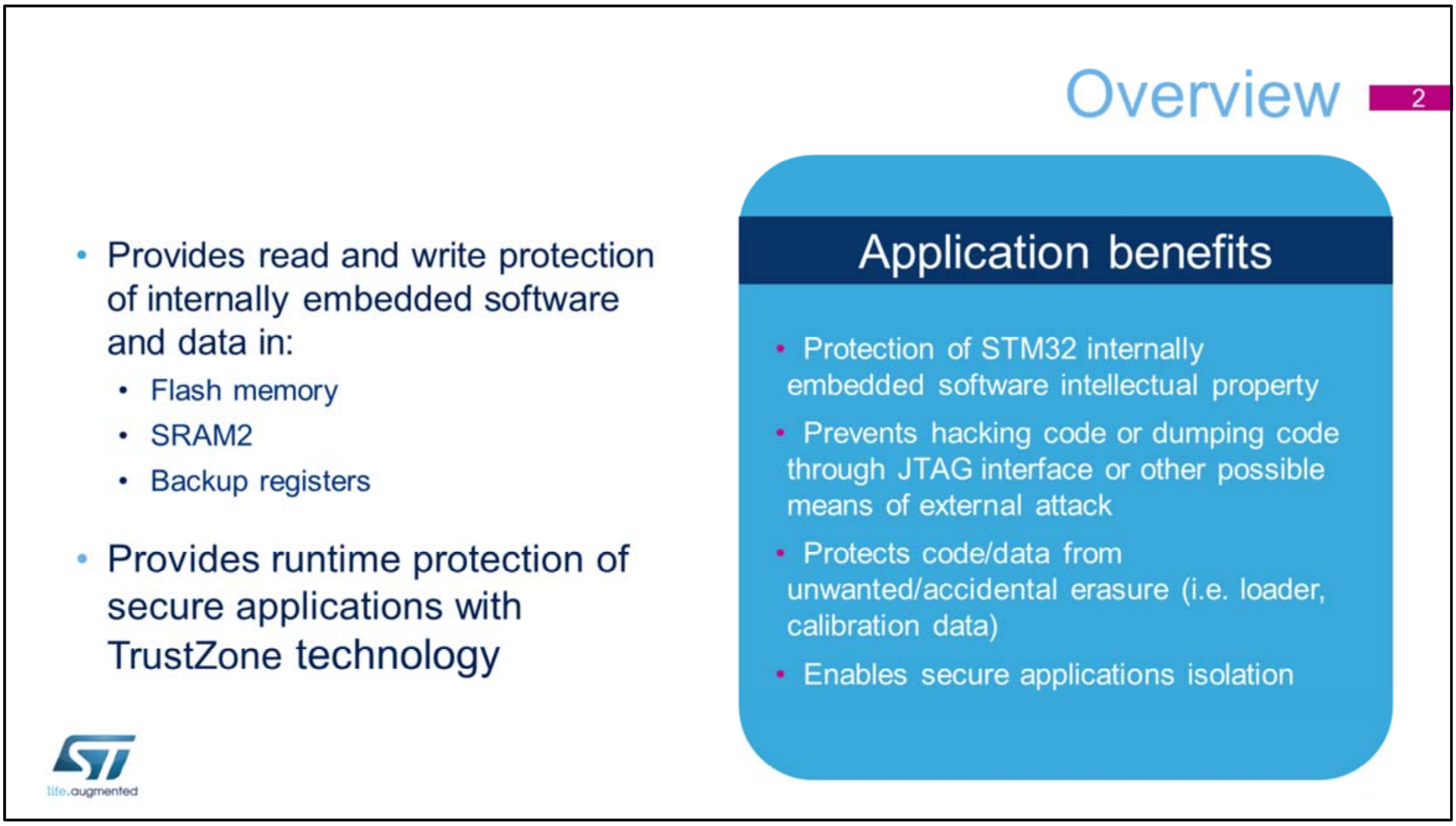
STM32L5 MEMPROTECT

Memory Protection features

Revision 1.0

life.augmented

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

2

- Provides read and write protection of internally embedded software and data in:
  - Flash memory
  - SRAM2
  - Backup registers
- Provides runtime protection of secure applications with TrustZone technology

Application benefits

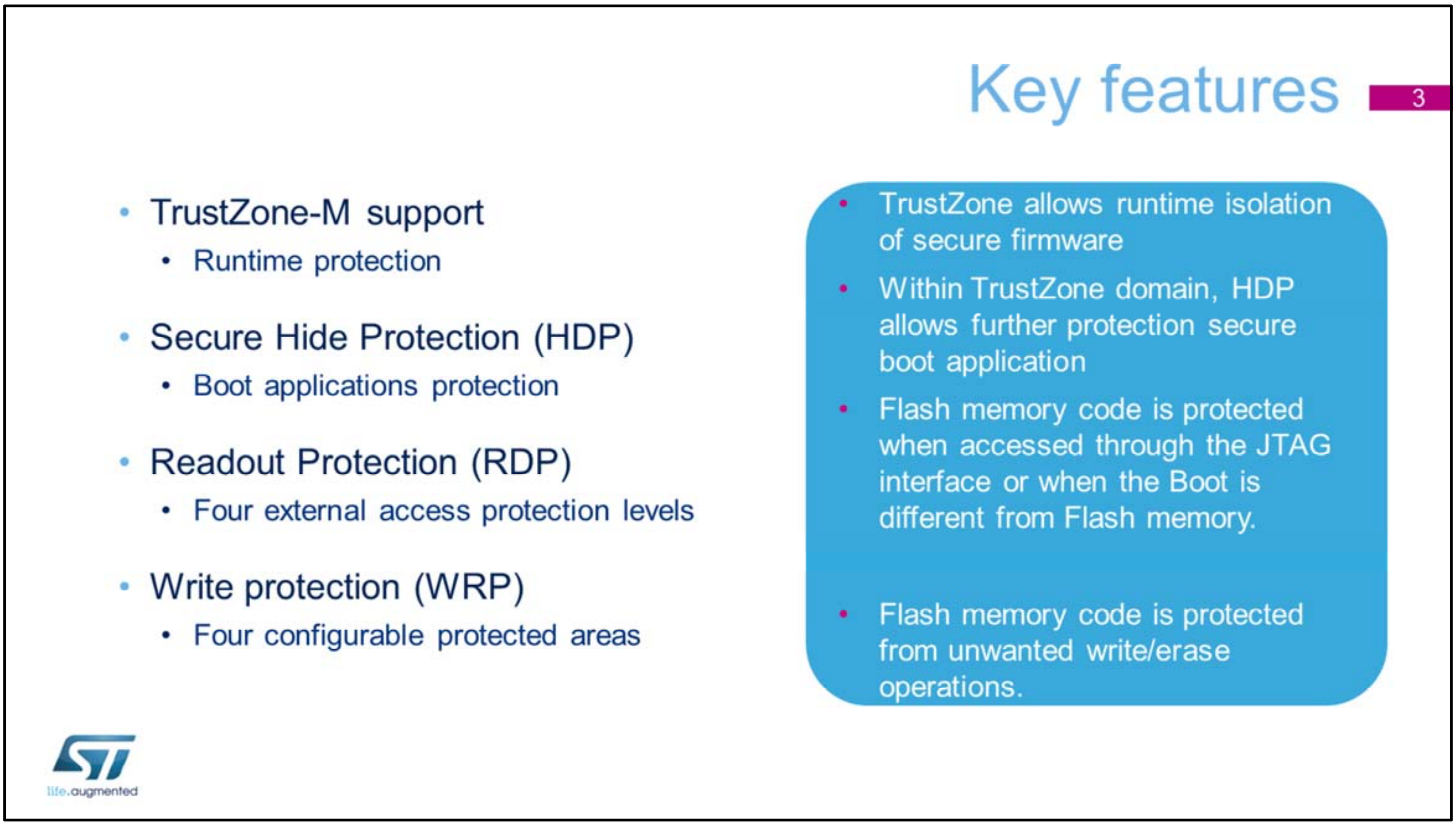
- Protection of STM32 internally embedded software intellectual property
- Prevents hacking code or dumping code through JTAG interface or other possible means of external attack
- Protects code/data from unwanted/accidental erasure (i.e. loader, calibration data)
- Enables secure applications isolation

Software providers may need to protect their software intellectual propriety from malicious users or from intrusive attacks.

For this purpose, STM32L5 microcontrollers provide several 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.

In addition to these static memory protections, STM32L5 introduces the support of TrustZone-M technology that provides runtime protections between secure and non-secure applications.



Key features

- TrustZone-M support
  - Runtime protection
- Secure Hide Protection (HDP)
  - Boot applications protection
- Readout Protection (RDP)
  - Four external access protection levels
- Write protection (WRP)
  - Four configurable protected areas

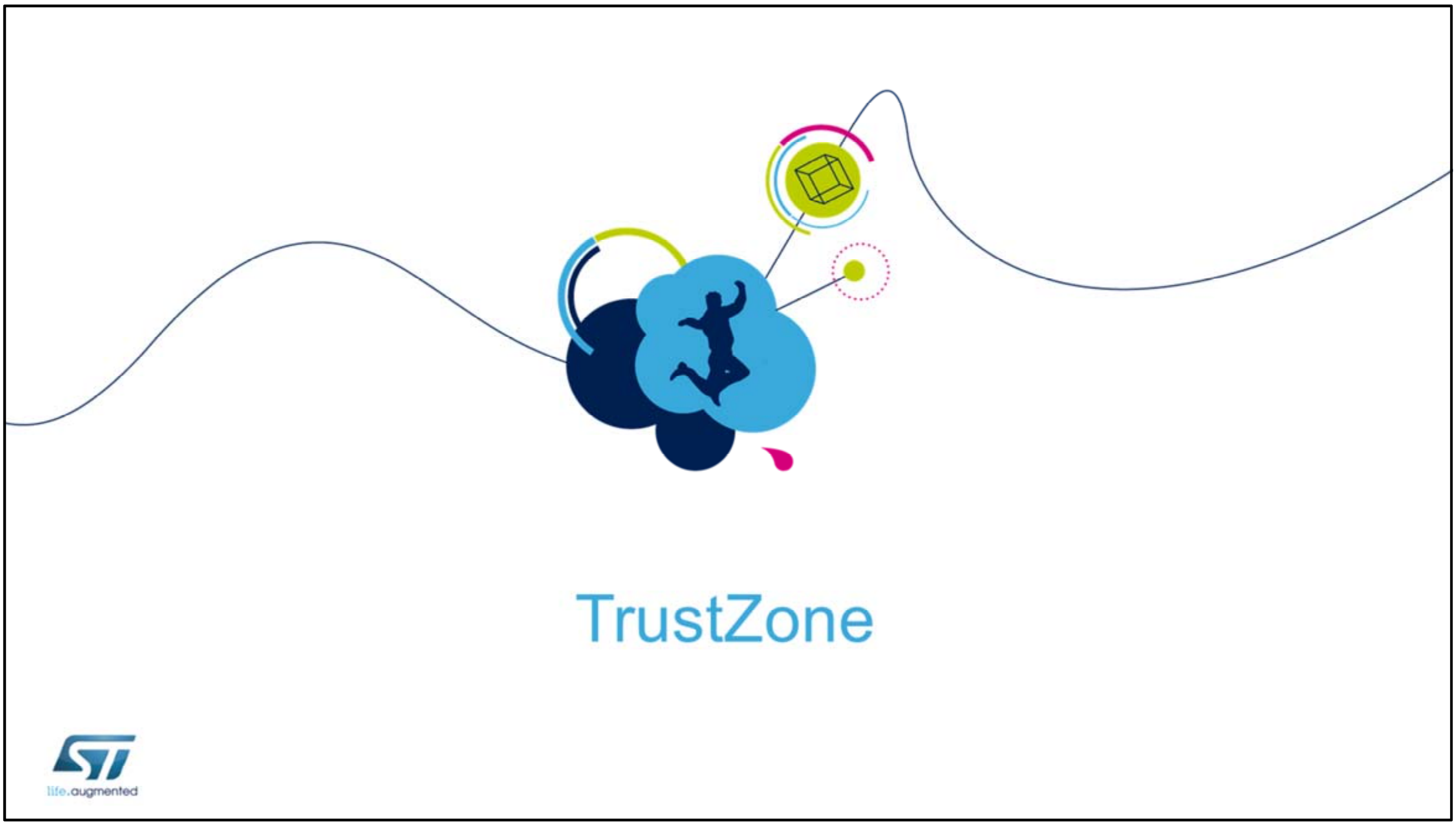
- TrustZone allows runtime isolation of secure firmware
- Within TrustZone domain, HDP allows further protection secure boot application
- Flash memory code is protected when accessed through the JTAG interface or when the Boot is different from Flash memory.

- Flash memory code is protected from unwanted write/erase operations.

This slides summarizes the protection mechanisms available in STM32L5

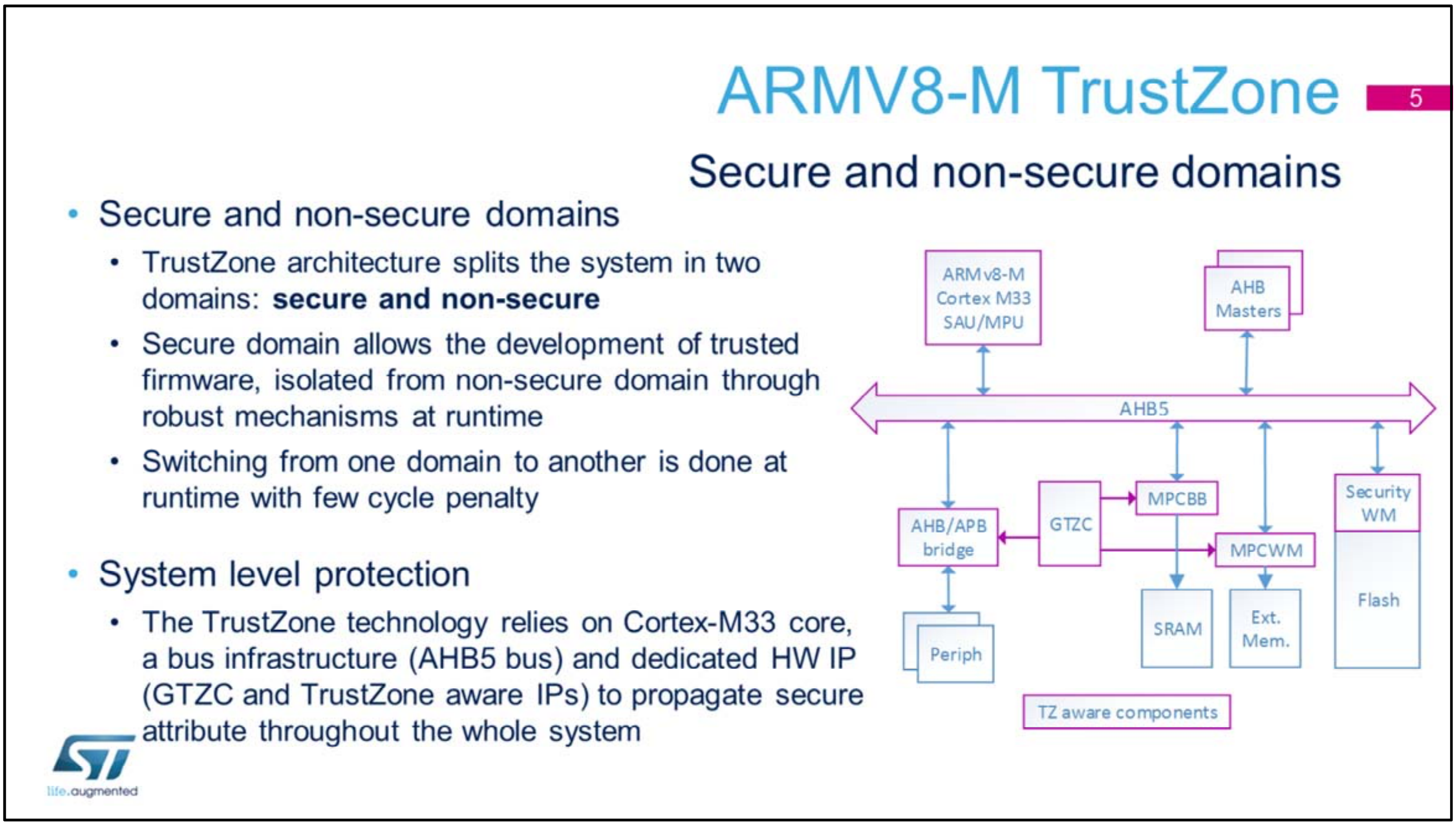
- TrustZone-M provides runtime protection between secure and non-secure domains
- Secure Hide Protection area, or HDP, is an additional protection level within secure domain that enables the implementation of a secure boot application for example
- Readout protection, or RDP, is a global Flash memory protection against external access through the JTAG.
- Write protection, or WRP, prevents accidental or malicious write/erase operations.

All these protections are configurable via the STM32L5 option bytes.



TrustZone

Let’s take a closer look at the details of the TrustZone-M technology.



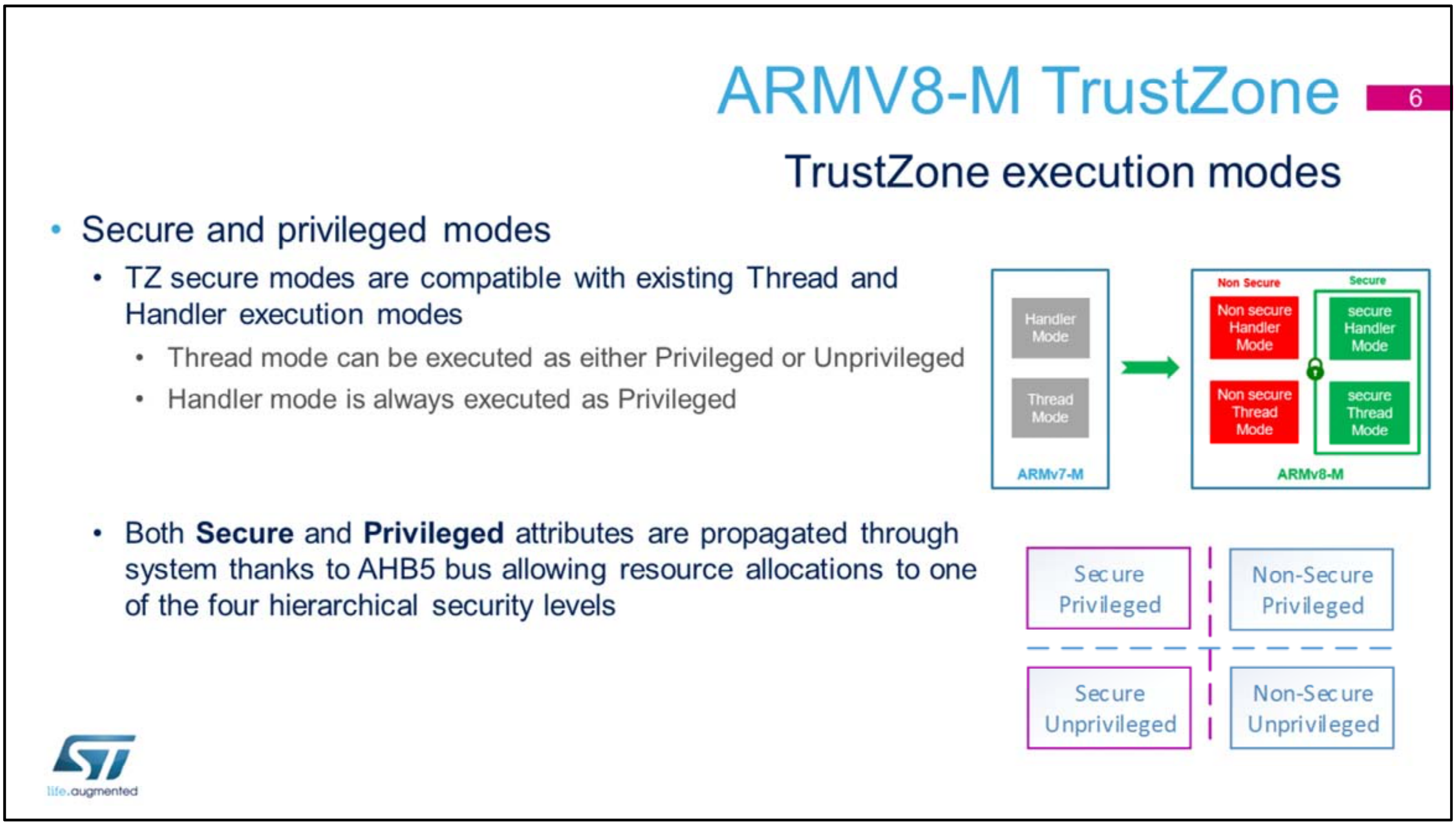
ARMV8-M TrustZone

Secure and non-secure domains

- Secure and non-secure domains
  - TrustZone architecture splits the system in two domains: **secure and non-secure**
  - Secure domain allows the development of trusted firmware, isolated from non-secure domain through robust mechanisms at runtime
  - Switching from one domain to another is done at runtime with few cycle penalty
- System level protection
  - The TrustZone technology relies on Cortex-M33 core, a bus infrastructure (AHB5 bus) and dedicated HW IP (GTZC and TrustZone aware IPs) to propagate secure attribute throughout the whole system

ArmV8-M architecture introduces the TrustZone-M technology that allows the split of firmware in secure and non-secure domains at runtime level. Switching form one domain to the other is done with few cycle penalty. As an example, secure domain may provide secure services based on cryptography to the user application running in non-secure domain.

TrustZone is a system level protection relying on Cortex-M33 core, AHB5 bus infrastructure and some dedicated HW blocs.



ARMV8-M TrustZone

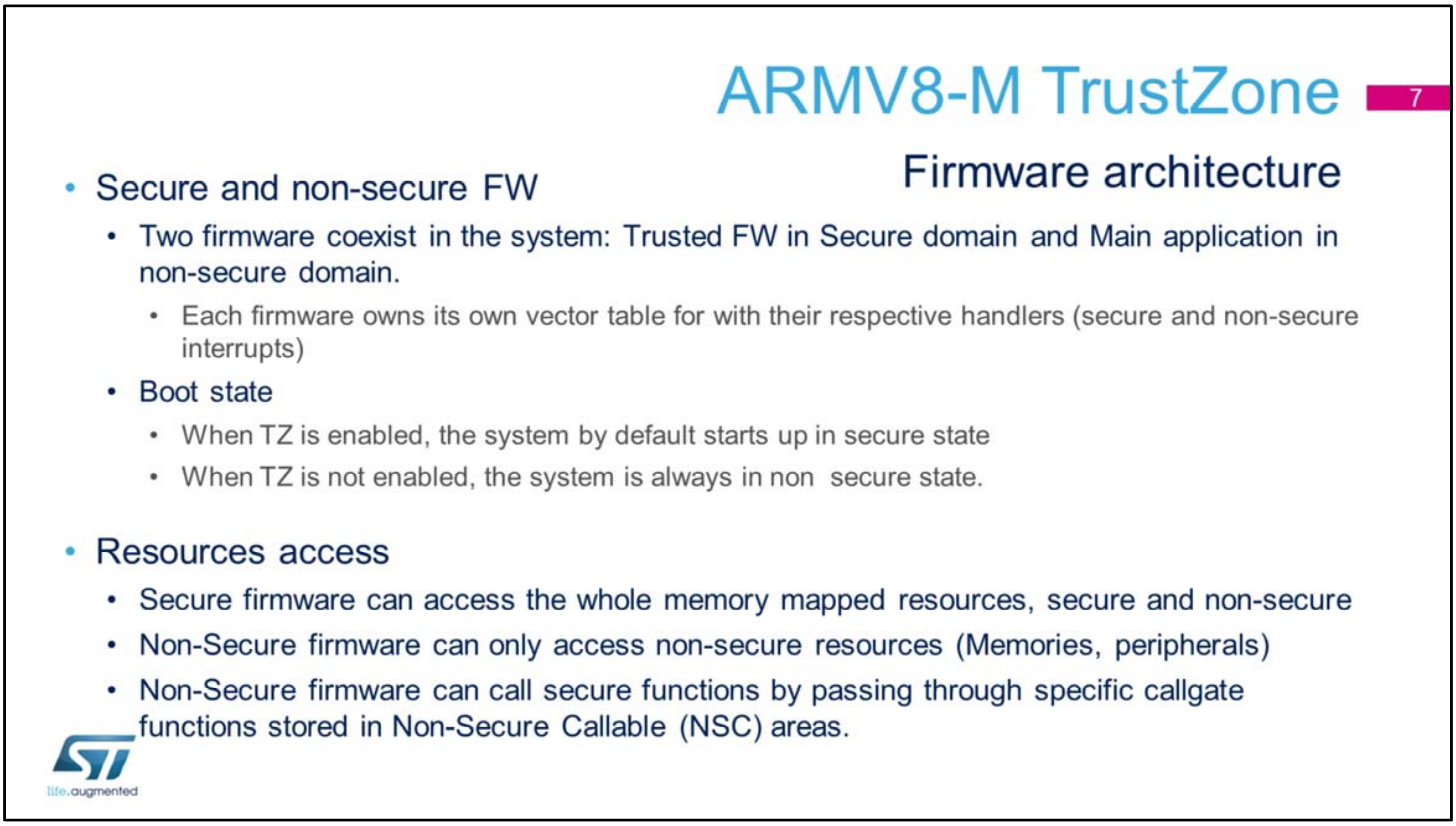
6

TrustZone execution modes

- Secure and privileged modes
  - TZ secure modes are compatible with existing Thread and Handler execution modes
    - Thread mode can be executed as either Privileged or Unprivileged
    - Handler mode is always executed as Privileged
  - Both **Secure** and **Privileged** attributes are propagated through system thanks to AHB5 bus allowing resource allocations to one of the four hierarchical security levels

TrustZone technology is compatible with thread and handler execution modes. In ARMV6 and ARMV7, two execution modes were supported, In ArmV8-M, four executions modes are now available.

Thread and handler modes support privileged/non-privileged access to memory-mapped resources. Privilege attribute, as secure attribute, is propagated at system level through bus infrastructure.
Hence, it is possible to consider four security levels for different part of firmware, from secure-privilege level to non-secure/ non privilege level.



ARMV8-M TrustZone

Firmware architecture

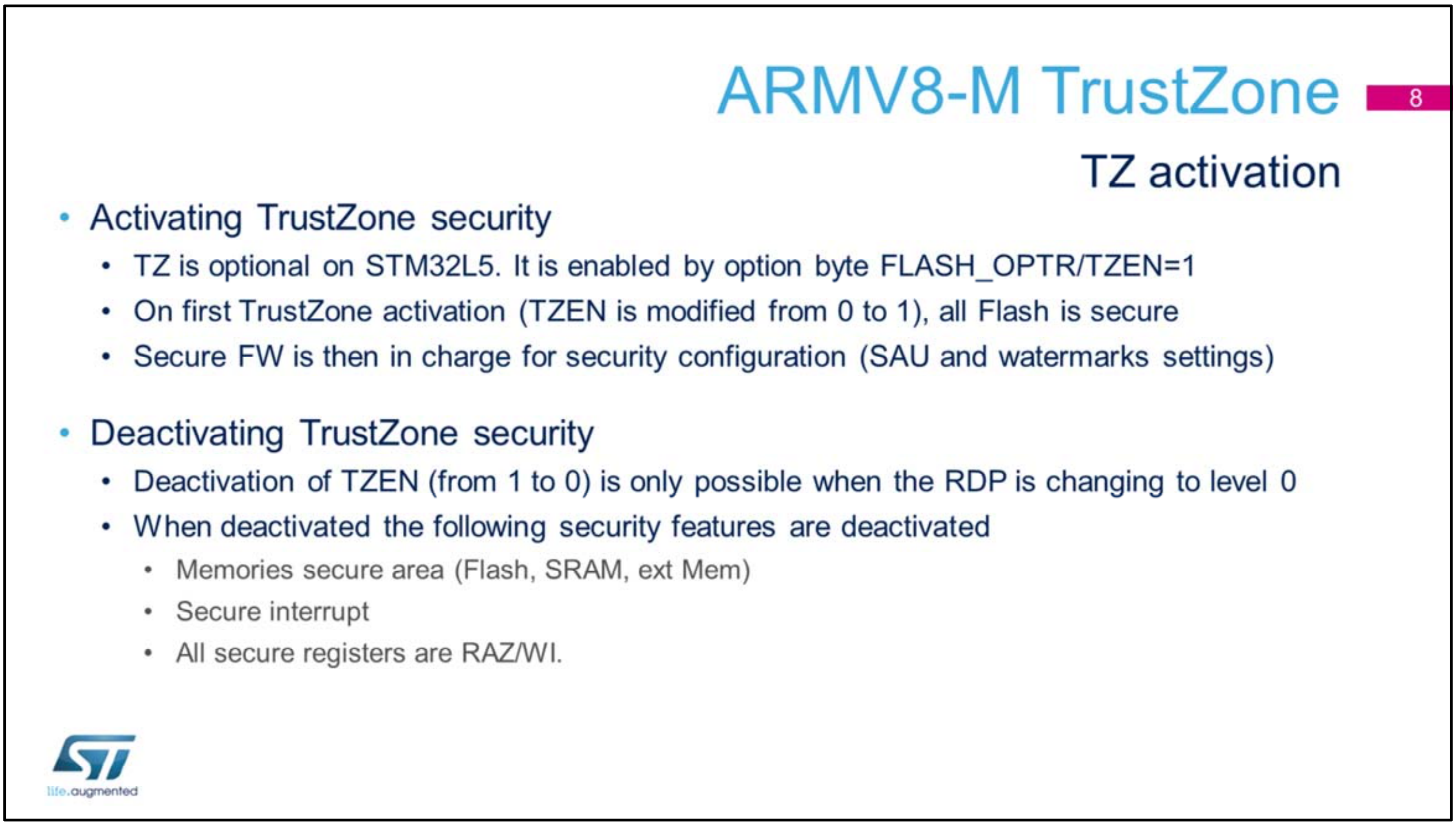
- Secure and non-secure FW
  - Two firmware coexist in the system: Trusted FW in Secure domain and Main application in non-secure domain.
    - Each firmware owns its own vector table for with their respective handlers (secure and non-secure interrupts)
  - Boot state
    - When TZ is enabled, the system by default starts up in secure state
    - When TZ is not enabled, the system is always in non secure state.
- Resources access
  - Secure firmware can access the whole memory mapped resources, secure and non-secure
  - Non-Secure firmware can only access non-secure resources (Memories, peripherals)
  - Non-Secure firmware can call secure functions by passing through specific callgate functions stored in Non-Secure Callable (NSC) areas.

With TrustZone technology, two domains coexist at runtime. There are two firmware, one per domain, with their own vector tables. At boot, when TrustZone is enabled, the system starts in secure state.

Secure firmware can access the whole memory mapped resources from either secure and non-secure domain.

Non-secure firmware can only access to non-secure resources.

Non-secure firmware can access to secure services only through specific callgate entry point stored in Non-secure callable (NSC) areas.



ARMV8-M TrustZone

TZ activation

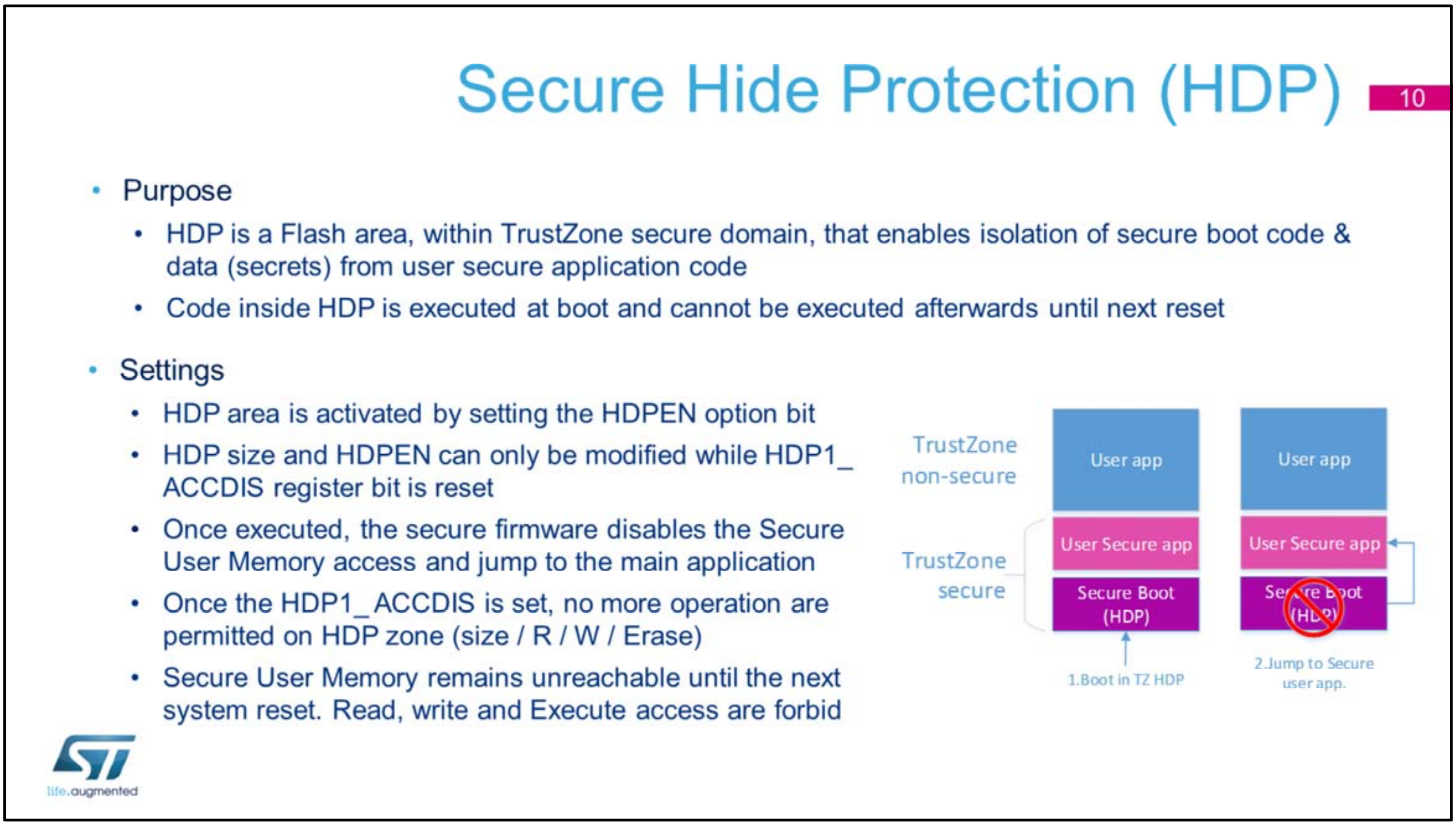
- Activating TrustZone security
  - TZ is optional on STM32L5. It is enabled by option byte FLASH_OPTR/TZEN=1
  - On first TrustZone activation (TZEN is modified from 0 to 1), all Flash is secure
  - Secure FW is then in charge for security configuration (SAU and watermarks settings)
- Deactivating TrustZone security
  - Deactivation of TZEN (from 1 to 0) is only possible when the RDP is changing to level 0
  - When deactivated the following security features are deactivated
    - Memories secure area (Flash, SRAM, ext Mem)
    - Secure interrupt
    - All secure registers are RAZ/WI.

life.augmented

TrustZone security is optional and can be activated with an option byte. Once set, the Flash is full secure. Further split between secure and non-secure domain is defined by secure firmware through the configuration of Secure Attribute Unit (or SAU) and other watermarks registers. Deactivation of TrustZone can only be done during the RDP level regression to level 0 with a Flash mass erase.

Secure Hide Protection (HDP)

Let’s take a closer look at the Secure Hide Protection feature.



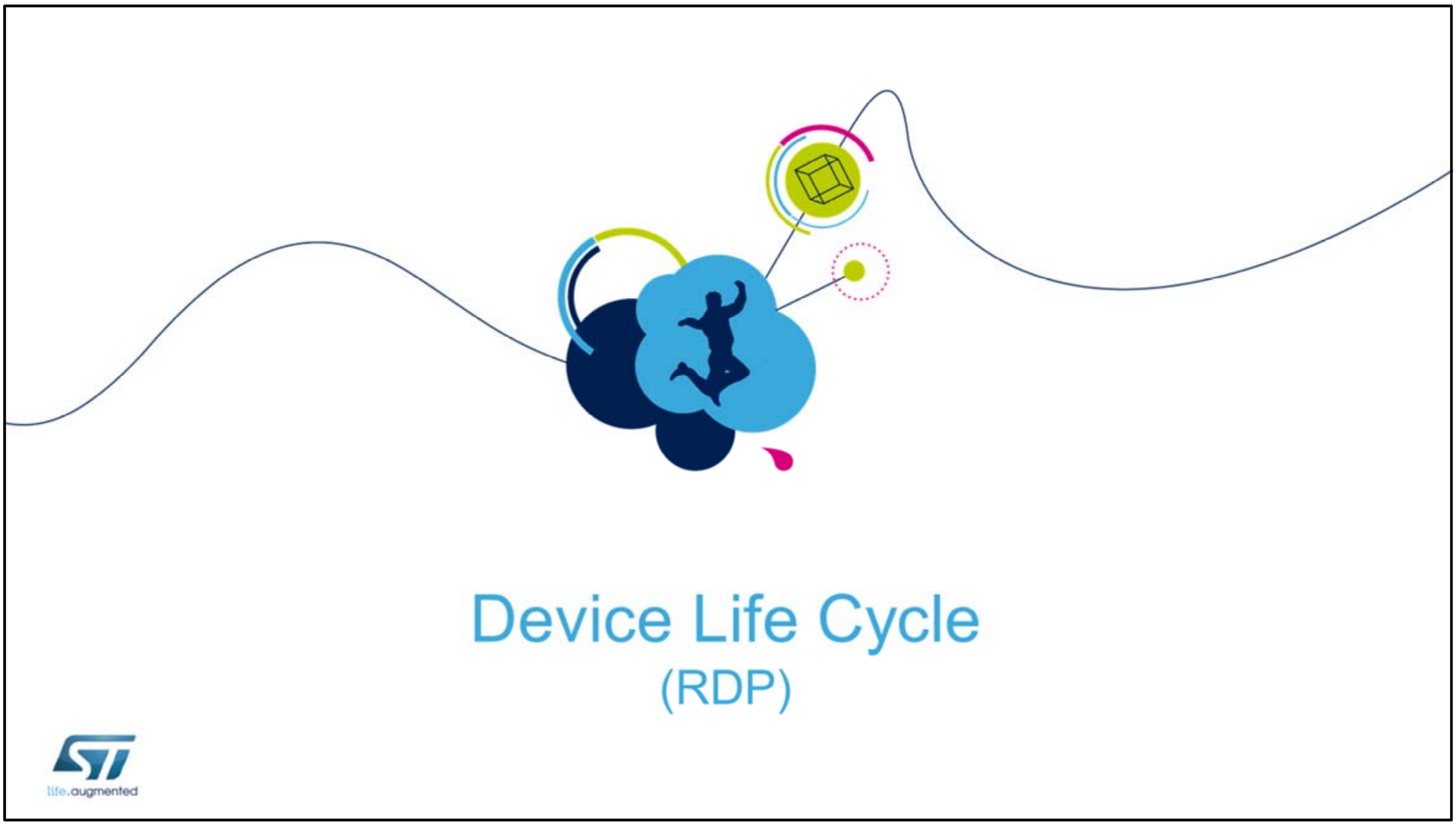
Secure Hide Protection (HDP)

10

- Purpose
  - HDP is a Flash area, within TrustZone secure domain, that enables isolation of secure boot code & data (secrets) from user secure application code
  - Code inside HDP is executed at boot and cannot be executed afterwards until next reset
- Settings
  - HDP area is activated by setting the HDPEN option bit
  - HDP size and HDPEN can only be modified while HDP1_ ACCDIS register bit is reset
  - Once executed, the secure firmware disables the Secure User Memory access and jump to the main application
  - Once the HDP1_ACCDIS is set, no more operation are permitted on HDP zone (size / R / W / Erase)
  - Secure User Memory remains unreachable until the next system reset. Read, write and Execute access are forbid

Secure Hide protection, or HDP is an additional protection mechanism within the TrustZone secure domain. It allows the development of secure application running only once after reset before jumping to user secure application. A typical use-case is to provide a secure boot application isolated from the rest of the main application (secure and non-secure).

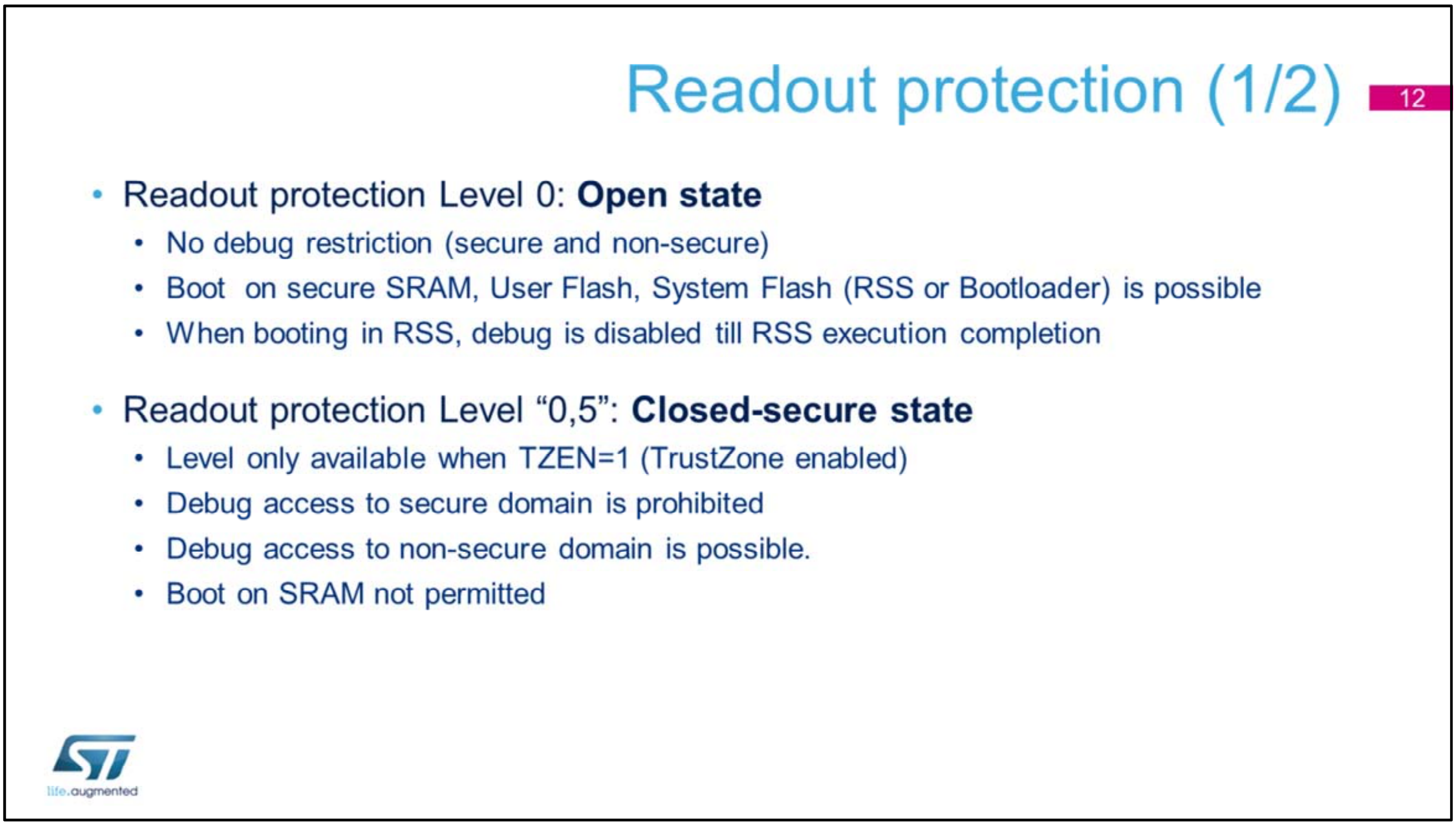
The code embedded in HDP is executed first. At the end of its execution, it jumps to secure user application. The code and data protected can no longer be accessed until the next system reset.



Device Life Cycle

(RDP)

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

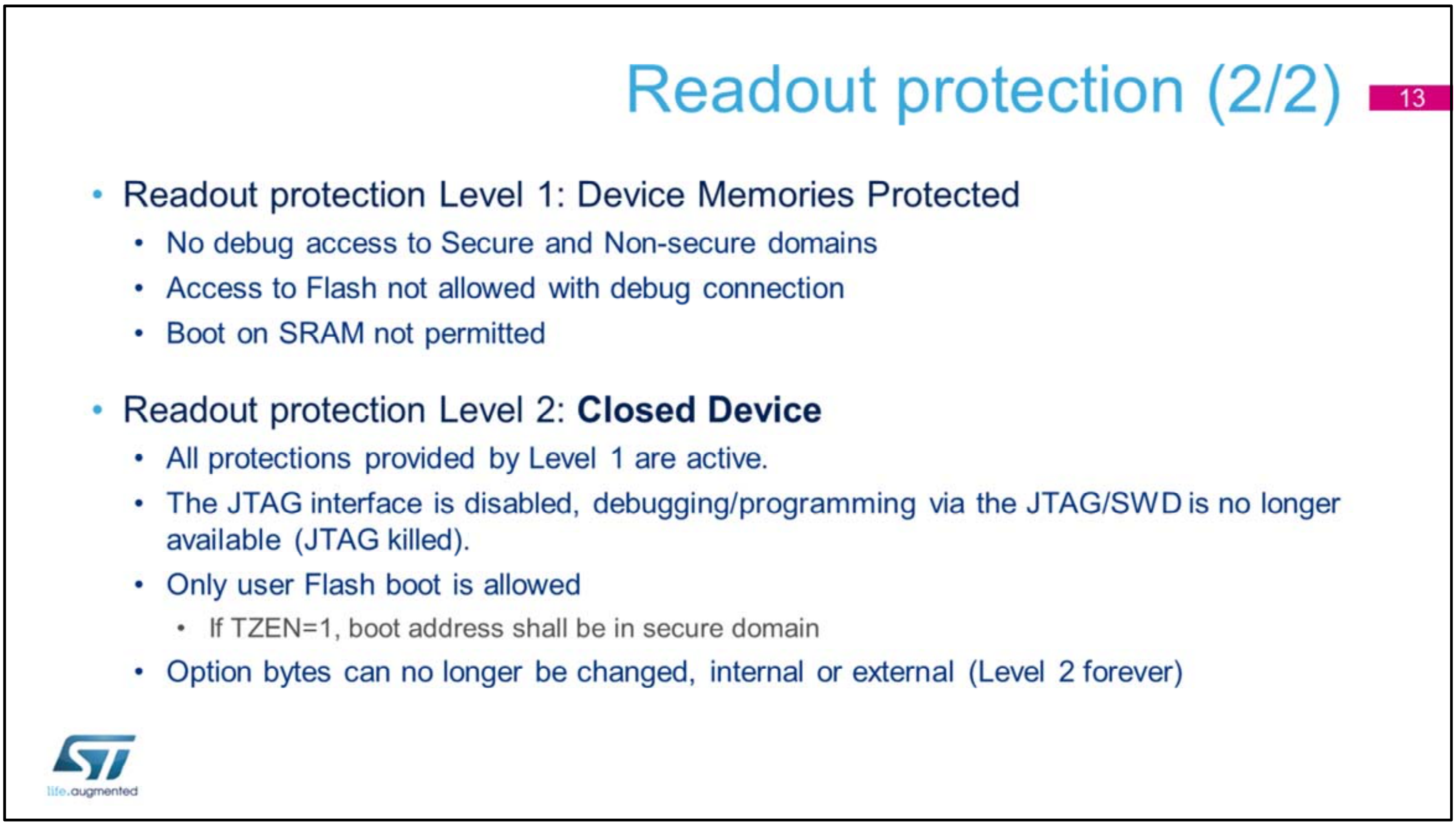


Readout protection (1/2)

- Readout protection Level 0: **Open state**
  - No debug restriction (secure and non-secure)
  - Boot on secure SRAM, User Flash, System Flash (RSS or Bootloader) is possible
  - When booting in RSS, debug is disabled till RSS execution completion
- Readout protection Level “0,5”: **Closed-secure state**
  - Level only available when TZEN=1 (TrustZone enabled)
  - Debug access to secure domain is prohibited
  - Debug access to non-secure domain is possible.
  - Boot on SRAM not permitted

The STM32L5 readout protection feature offers four levels of protection for all SRAM2 and Flash memory as well as the backup registers:

- Level 0 means “no protection”. This is the factory default. Read, 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 0.5 is an additional protection level associated with TrustZone. RDP 0.5 is available only when TrustZone is enabled. Debug of secure domain is forbidden, only non-secure domain can be accessed for debug.



Readout protection (2/2)

- Readout protection Level 1: Device Memories Protected
  - No debug access to Secure and Non-secure domains
  - Access to Flash not allowed with debug connection
  - Boot on SRAM not permitted
- Readout protection Level 2: **Closed Device**
  - All protections provided by Level 1 are active.
  - The JTAG interface is disabled, debugging/programming via the JTAG/SWD is no longer available (JTAG killed).
  - Only user Flash boot is allowed
    - If TZEN=1, boot address shall be in secure domain
  - Option bytes can no longer be changed, internal or external (Level 2 forever)

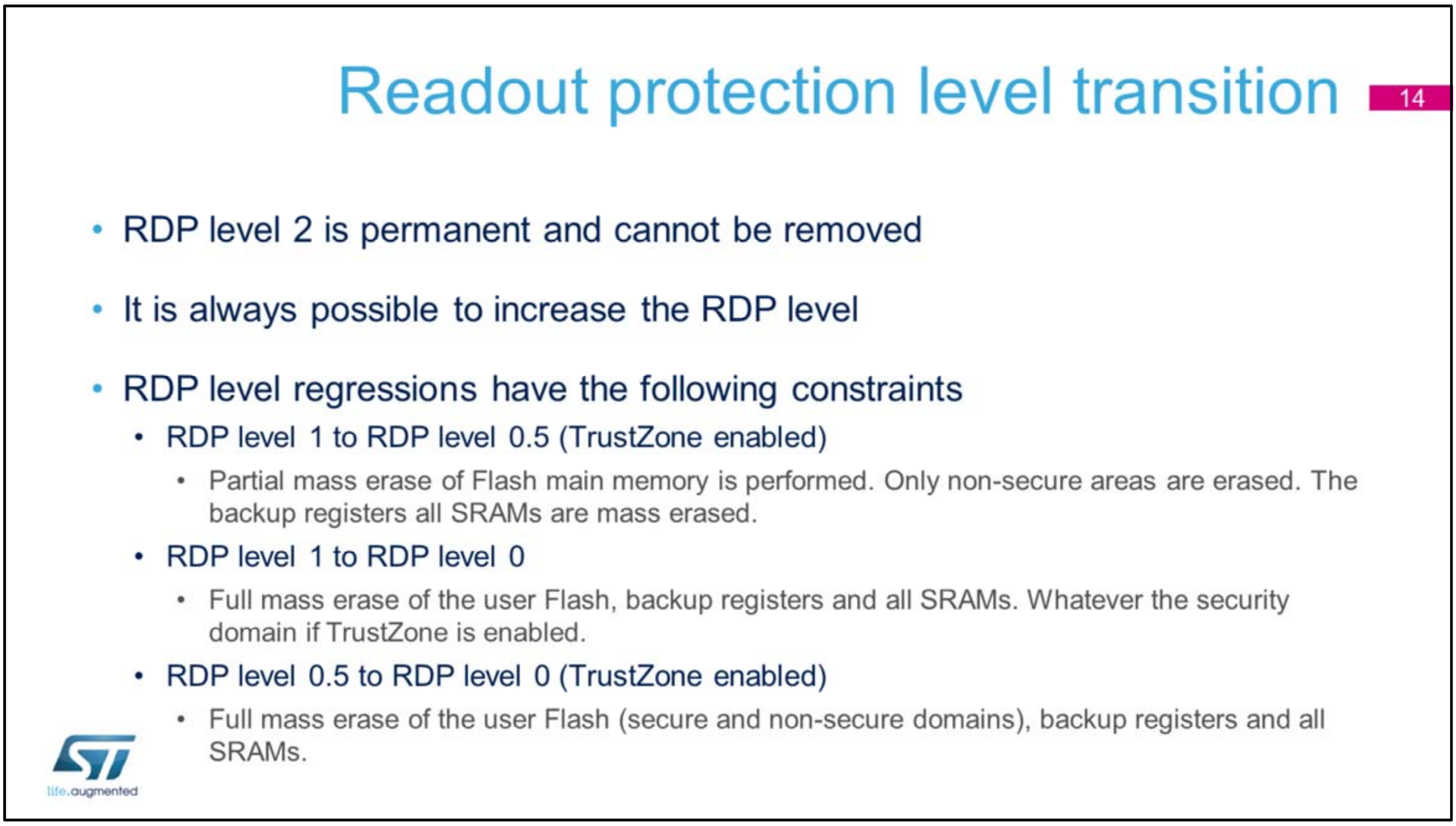
Level 1 ensures total read protection of the chip’s memories which includes the Flash memory and the backup registers as well as a new feature to the STM32 family, the SRAM2 content.
Whenever a debugger access is detected or Boot mode is not set to a Flash memory area, any access to the Flash memory, 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.

Level 2 provides the same protection features for the SRAM2, Flash memory and Backup registers as described for Level 1. However, there are two major differences.

1. The JTAG/SWD debugger connection is disabled (even at the ST factory, to ensure that there are no

backdoors);

2. RDP/WRP option bytes can no longer be changed, as well as all the other option bytes.



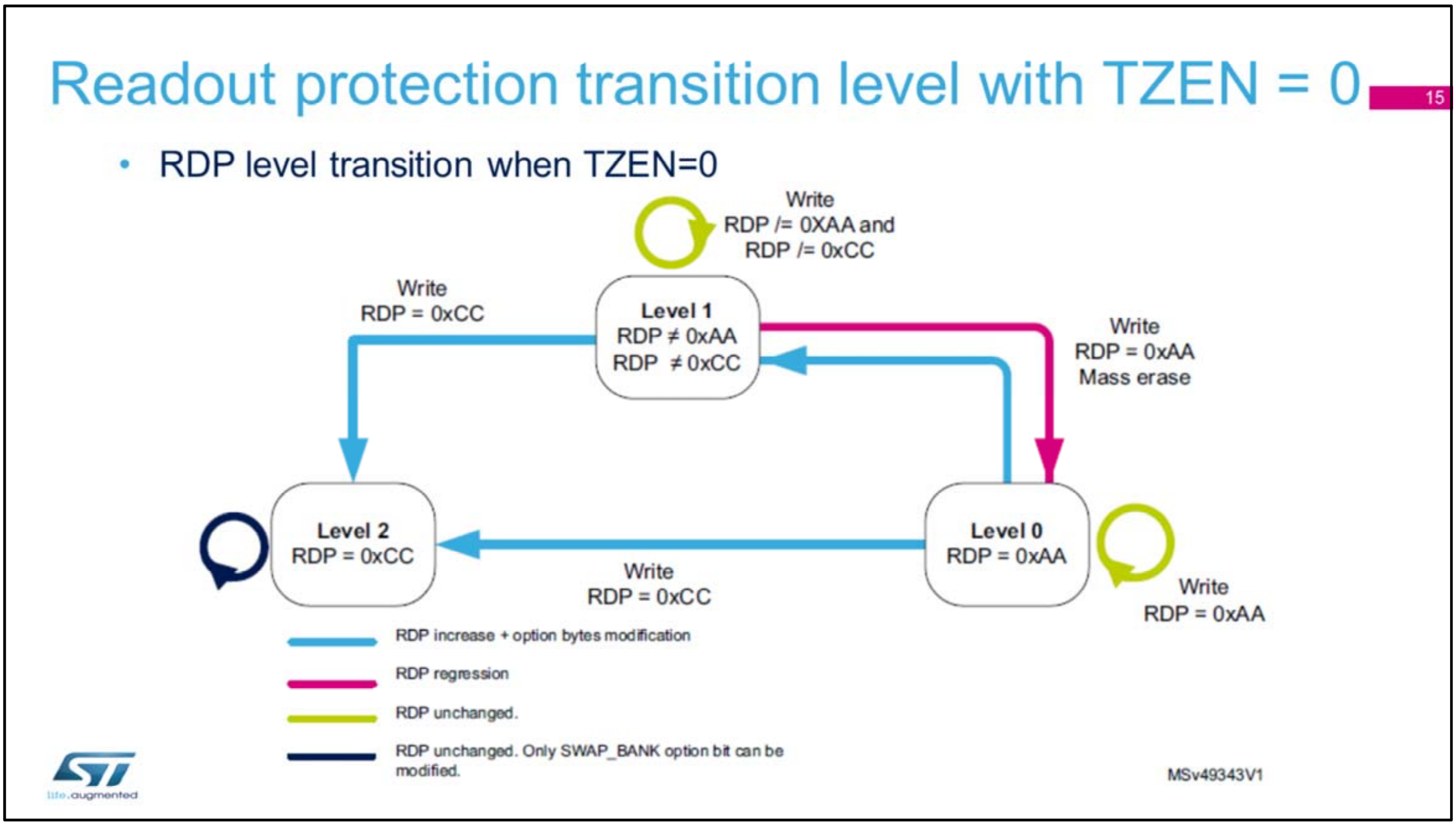
Readout protection level transition

- RDP level 2 is permanent and cannot be removed
- It is always possible to increase the RDP level
- RDP level regressions have the following constraints
  - RDP level 1 to RDP level 0.5 (TrustZone enabled)
    - Partial mass erase of Flash main memory is performed. Only non-secure areas are erased. The backup registers all SRAMs are mass erased.
  - RDP level 1 to RDP level 0
    - Full mass erase of the user Flash, backup registers and all SRAMs. Whatever the security domain if TrustZone is enabled.
  - RDP level 0.5 to RDP level 0 (TrustZone enabled)
    - Full mass erase of the user Flash (secure and non-secure domains), backup registers and all SRAMs.

RDP level regression is only possible in levels 1 and 0.5. Level 2 is permanent and cannot be modified.

Regression from level 1 or level 0.5 to level 0 triggers a Flash mass erase, as well as backup registers and all SRAMs.

Regression from level 1 to level 0.5 , when TrustZone is enabled, triggers an erase of the non-secure domain. Backup registers and SRAMs are fully erased.



Readout protection transition level with TZEN = 0

- RDP level transition when TZEN=0

Write
RDP /= 0XAA and
RDP /= 0xCC

Write
RDP = 0xCC

Level 1
RDP ≠ 0xAA
RDP ≠ 0xCC

Write
RDP = 0xAA
Mass erase

Level 2
RDP = 0xCC

Level 0
RDP = 0xAA

Write
RDP = 0xCC

Write
RDP = 0xAA

RDP increase + option bytes modification

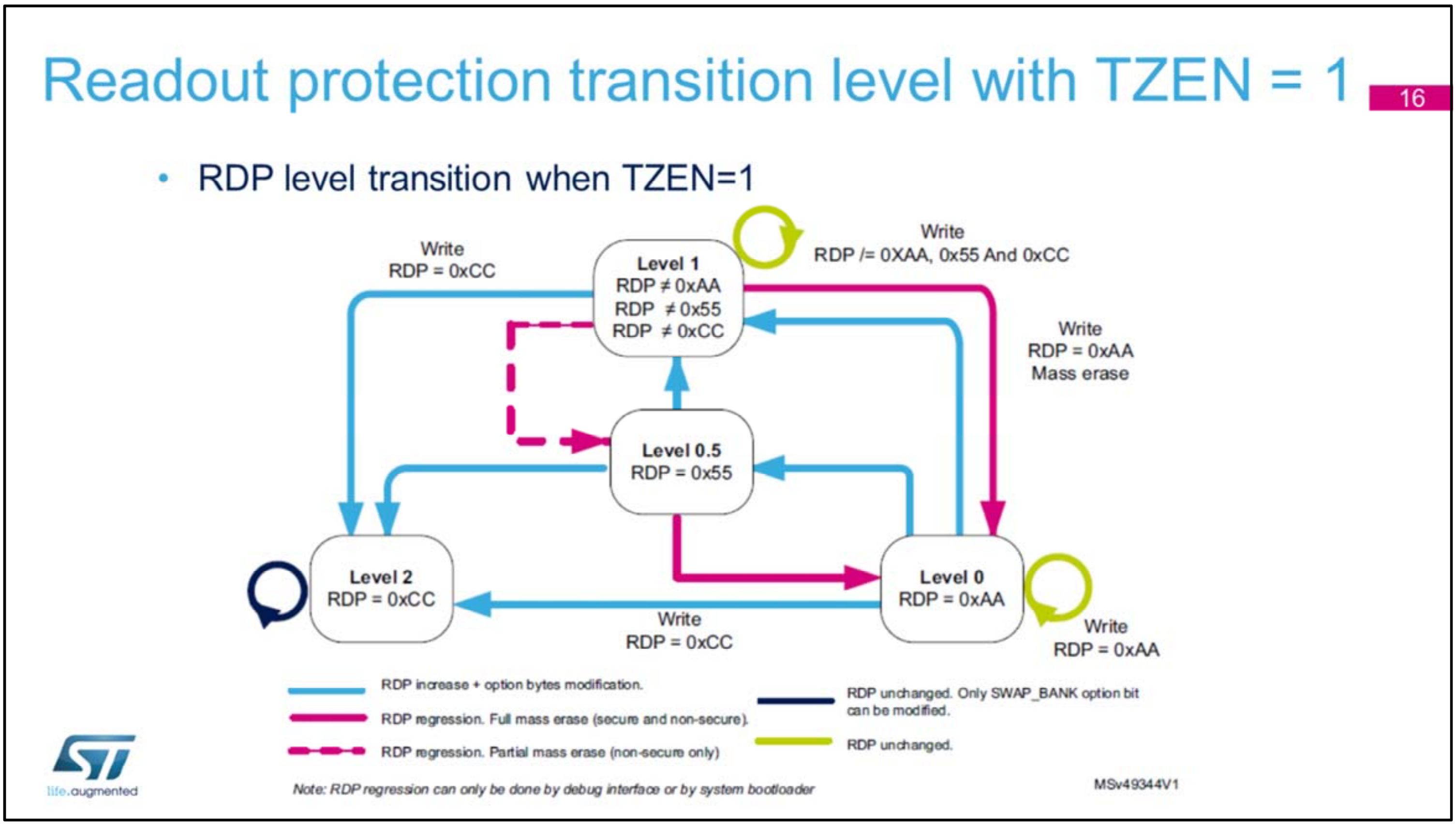
RDP regression

RDP unchanged.

RDP unchanged. Only SWAP_BANK option bit can be modified.

MSv49343V1

This slide is a summary of RDP level transitions when TrustZone is not enabled. This is the traditional scheme active in all STM32 products based on ARMV6 and ARMV7 architectures.



Readout protection transition level with TZEN = 1

16

- RDP level transition when TZEN=1

RDP increase + option bytes modification.

RDP regression. Full mass erase (secure and non-secure).

RDP regression. Partial mass erase (non-secure only)

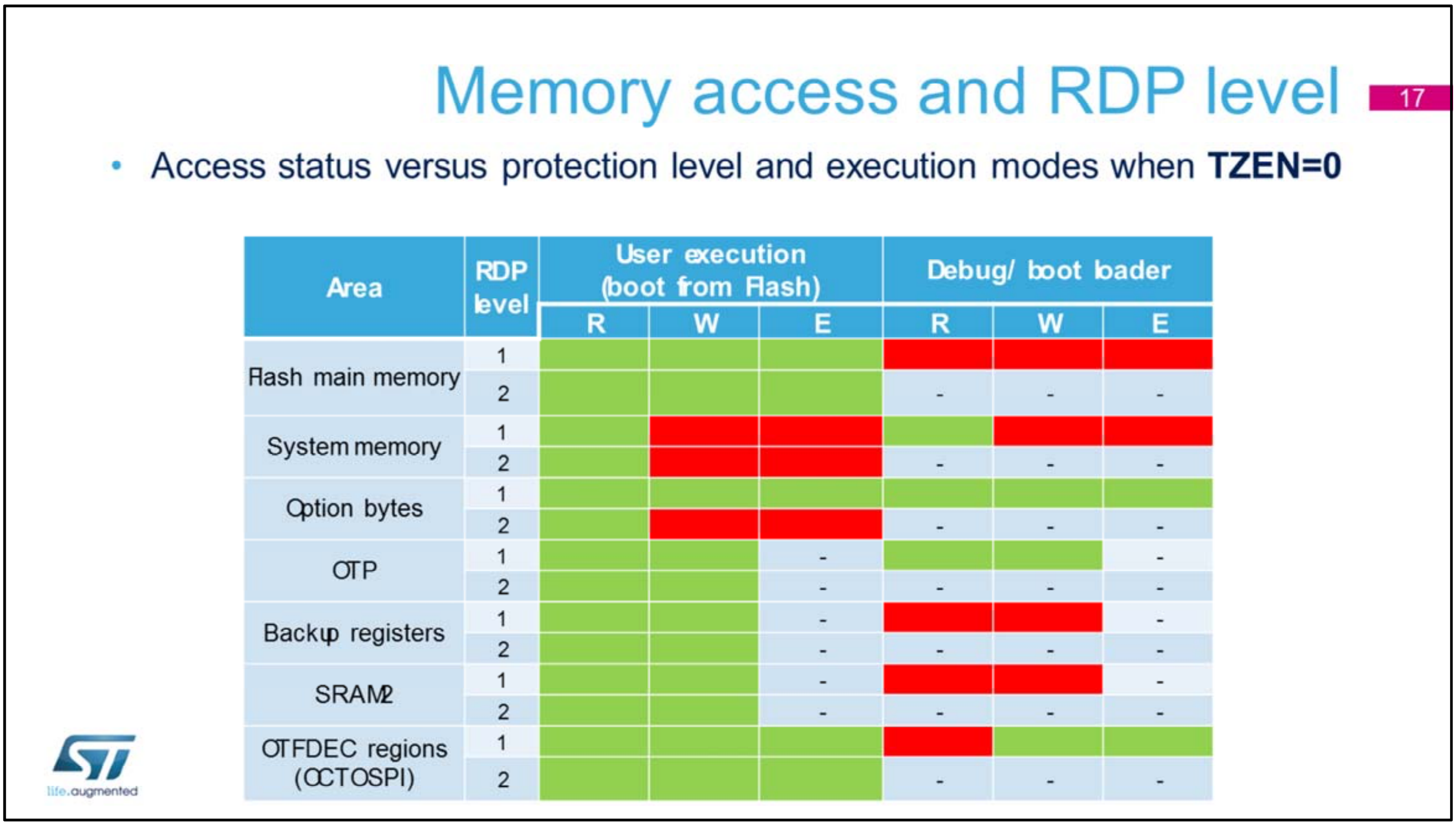
RDP unchanged. Only SWAP_BANK option bit can be modified.

RDP unchanged.

Note: RDP regression can only be done by debug interface or by system bootloader

MSv49344V1

This slide is a summary of RDP level transitions when TrustZone is enabled. In addition to levels 0, 1 and 2, there is a “0.5” level for secure –only protection against external access.



Memory access and RDP level

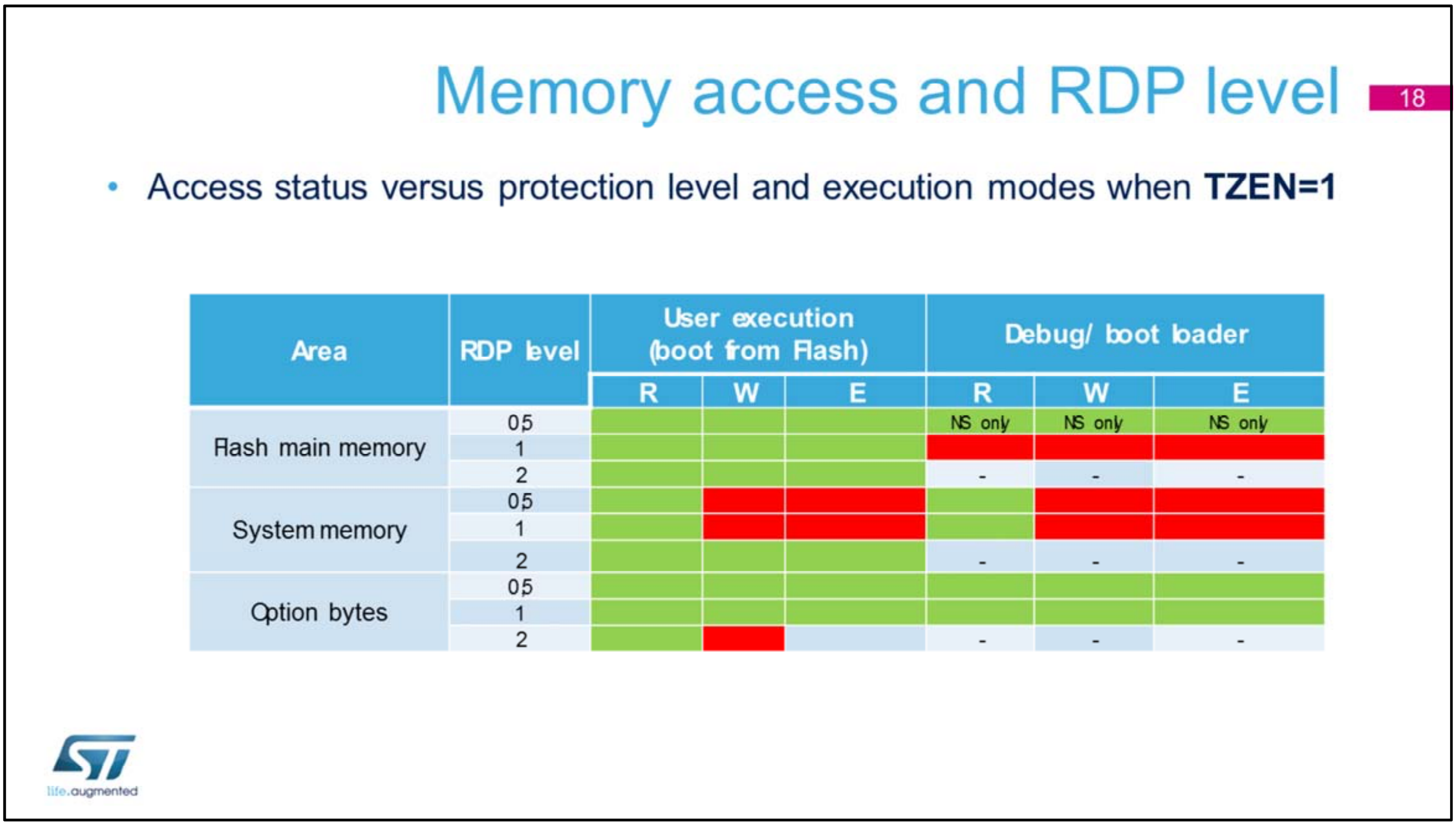
17

- Access status versus protection level and execution modes when **TZEN=0**

Area	RDP level	User execution (boot from Flash)			Debug/ boot loader		
		R	W	E	R	W	E
Flash main memory	1	🟩	🟩	🟩	🟥	🟥	🟥
	2	🟩	🟩	🟩	-	-	-
System memory	1	🟩	🟥	🟥	🟩	🟥	🟥
	2	🟩	🟥	🟥	-	-	-
Option bytes	1	🟩	🟩	🟩	🟩	🟩	🟩
	2	🟩	🟥	🟥	-	-	-
OTP	1	🟩	🟩	-	🟩	🟩	-
	2	🟩	🟩	-	-	-	-
Backup registers	1	🟩	🟩	-	🟥	🟥	-
	2	🟩	🟩	-	-	-	-
SRAM2	1	🟩	🟩	-	🟥	🟥	-
	2	🟩	🟩	-	-	-	-
OTFDEC regions (OCTOSPI)	1	🟩	🟩	🟩	🟥	🟩	🟩
	2	🟩	🟩	🟩	-	-	-

life.augmented

This table summarizes the different types of access authorized when TrustZone is not enabled for the different memory types according to the readout protection (RDP) level, configured boot mode and debug access, as previously discussed.



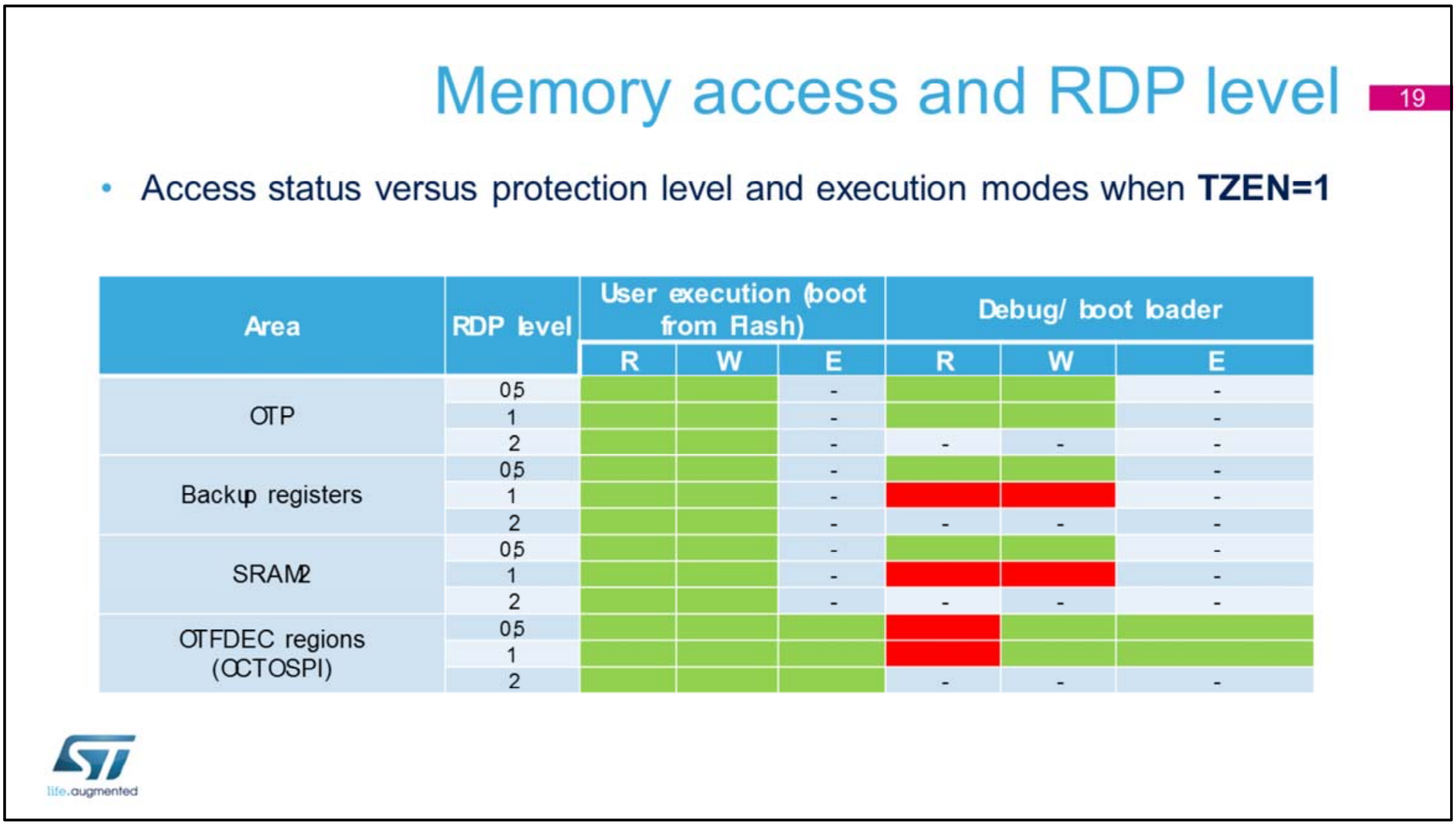
Memory access and RDP level

- Access status versus protection level and execution modes when **TZEN=1**

Area	RDP level	User execution (boot from Flash)			Debug/ boot loader		
		R	W	E	R	W	E
Flash main memory	0,5	🟩	🟩	🟩	🟩 NS only	🟩 NS only	🟩 NS only
	1	🟩	🟩	🟩	🟥	🟥	🟥
	2	🟩	🟩	🟩	-	-	-
System memory	0,5	🟩	🟥	🟥	🟩	🟥	🟥
	1	🟩	🟥	🟥	🟩	🟥	🟥
	2	🟩	🟩	🟩	-	-	-
Option bytes	0,5	🟩	🟩	🟩	🟩	🟩	🟩
	1	🟩	🟩	🟩	🟩	🟩	🟩
	2	🟩	🟥		-	-	-

life.augmented

This table summarizes the different types of access authorized when TrustZone is enabled for the Flash memory and the option bytes according to the readout protection (RDP) level, configured boot mode and debug access.



Memory access and RDP level

- Access status versus protection level and execution modes when **TZEN=1**

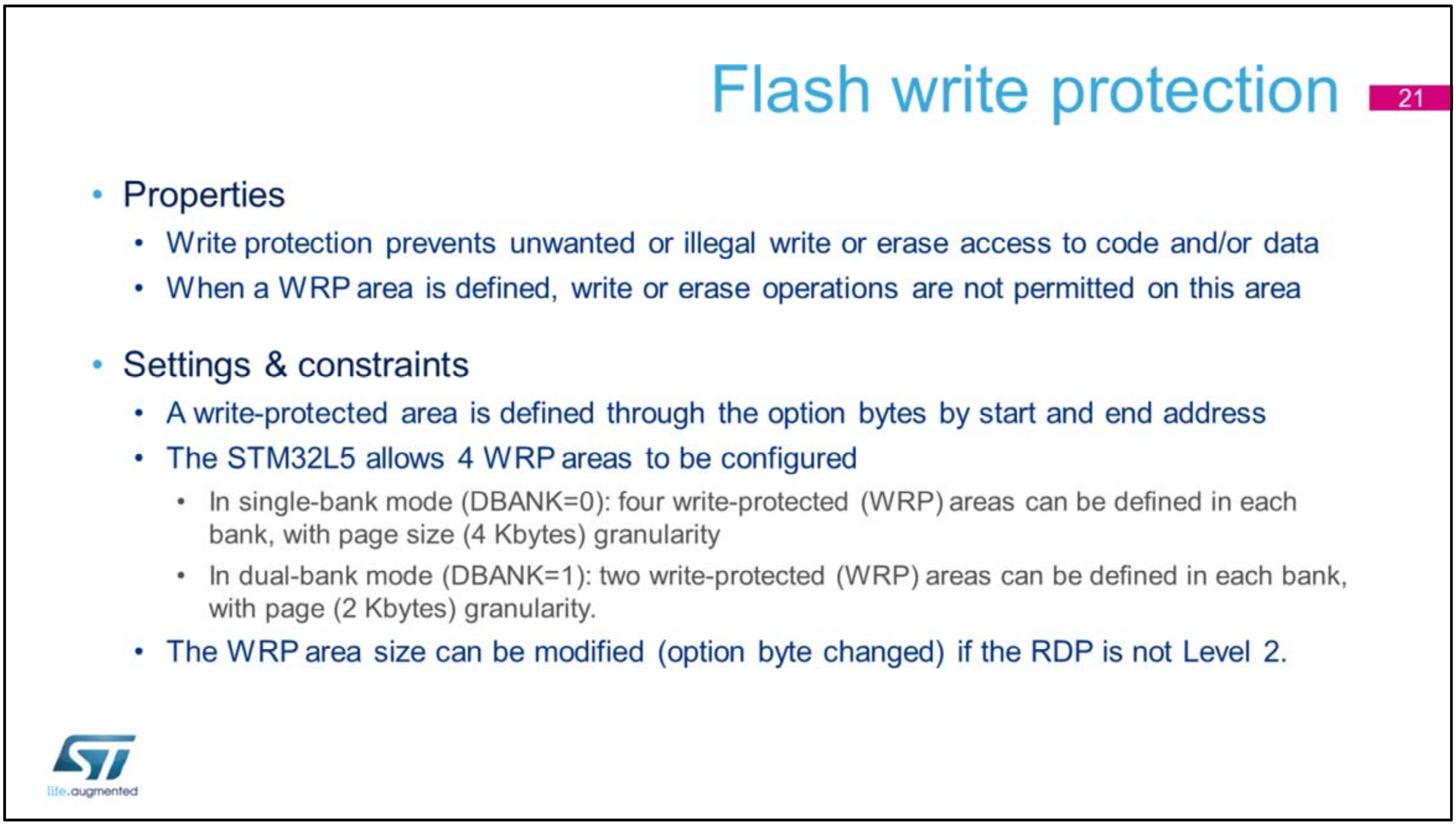
Area	RDP level	User execution (boot from Flash)			Debug/ boot loader		
		R	W	E	R	W	E
OTP	0,5	🟩	🟩	-	🟩	🟩	-
	1	🟩	🟩	-	🟩	🟩	-
	2	🟩	🟩	-	-	-	-
Backup registers	0,5	🟩	🟩	-	🟩	🟩	-
	1	🟩	🟩	-	🟥	🟥	-
	2	🟩	🟩	-	-	-	-
SRAM2	0,5	🟩	🟩	-	🟩	🟩	-
	1	🟩	🟩	-	🟥	🟥	-
	2	🟩	🟩	-	-	-	-
OTFDEC regions (OCTOSPI)	0,5	🟩	🟩	🟩	🟥	🟩	🟩
	1	🟩	🟩	🟩	🟥	🟩	🟩
	2	🟩	🟩	🟩	-	-	-

life.augmented

This table summarizes the different types of access authorized when TrustZone is enabled for the OTP, the backup registers, SRAM2 and external memory according to the readout protection (RDP) level, configured boot mode and debug access.

Write protection

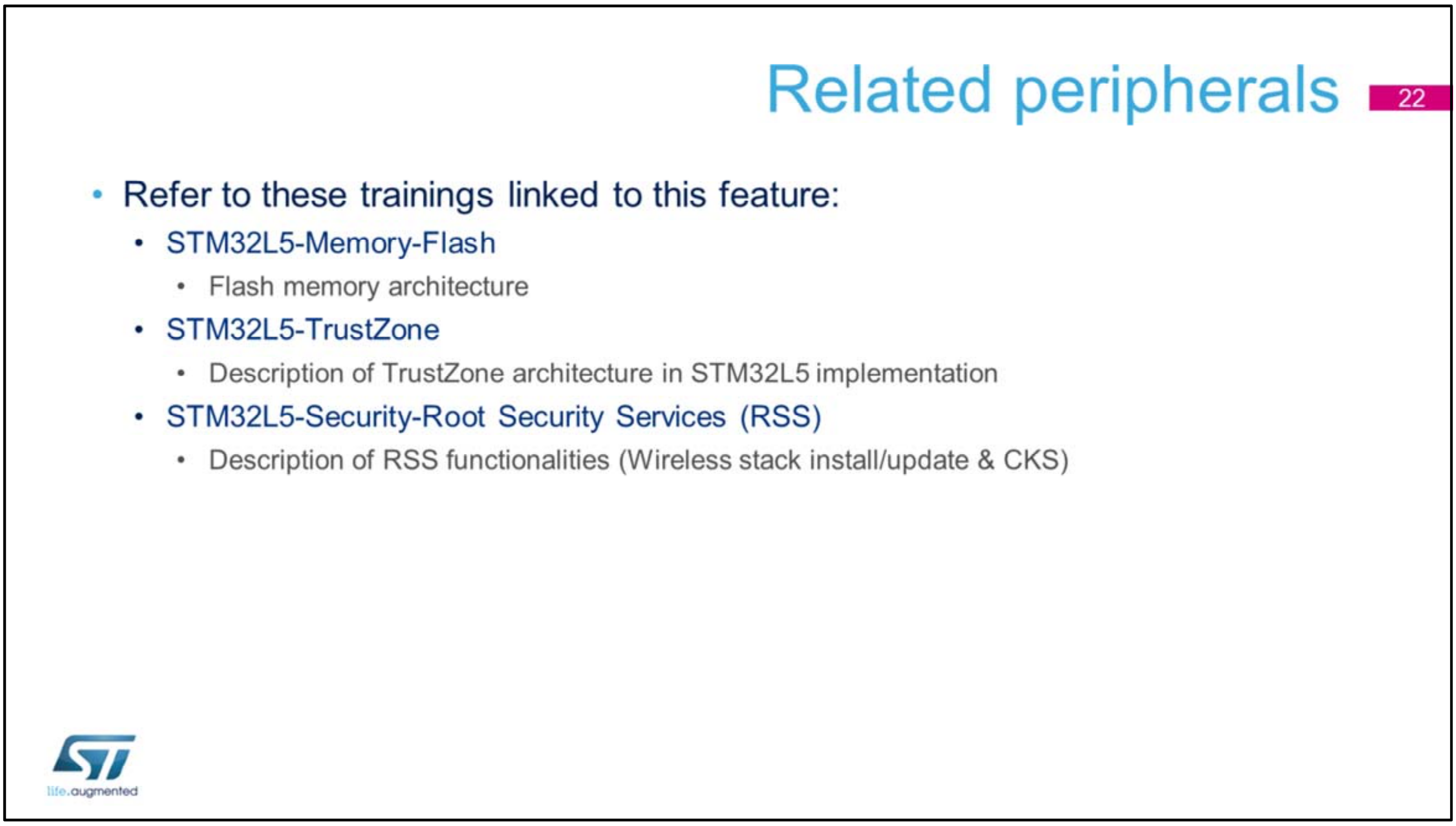
Now, let’s take a closer look at the details of the write protection settings of the STM32L5.



Flash write protection

- Properties
  - Write protection prevents unwanted or illegal write or erase access to code and/or data
  - When a WRP area is defined, write or erase operations are not permitted on this area
- Settings & constraints
  - A write-protected area is defined through the option bytes by start and end address
  - The STM32L5 allows 4 WRP areas to be configured
    - In single-bank mode (DBANK=0): four write-protected (WRP) areas can be defined in each bank, with page size (4 Kbytes) granularity
    - In dual-bank mode (DBANK=1): two write-protected (WRP) areas can be defined in each bank, with page (2 Kbytes) granularity.
  - The WRP area size can be modified (option byte changed) if the RDP is not Level 2.

The Flash memory write protection mechanism is designed to prevent unwanted write access to defined areas in Flash memory, such as the bootloader 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 page granularity (4 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.



Related peripherals

22

- Refer to these trainings linked to this feature:
  - STM32L5-Memory-Flash
    - Flash memory architecture
  - STM32L5-TrustZone
    - Description of TrustZone architecture in STM32L5 implementation
  - STM32L5-Security-Root Security Services (RSS)
    - Description of RSS functionalities (Wireless stack install/update & CKS)

life.augmented

In addition to this training, you may find these three modules useful.