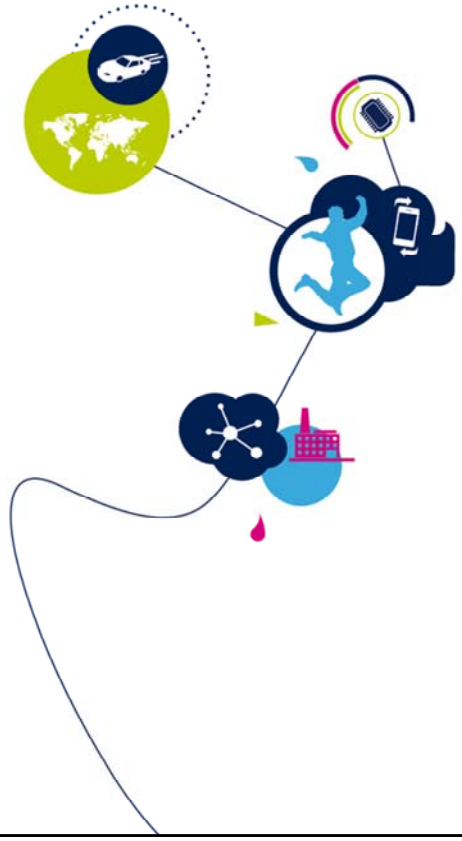
STM32L5 - GTZC

Global TrustZone® Controller

Revision 1.0

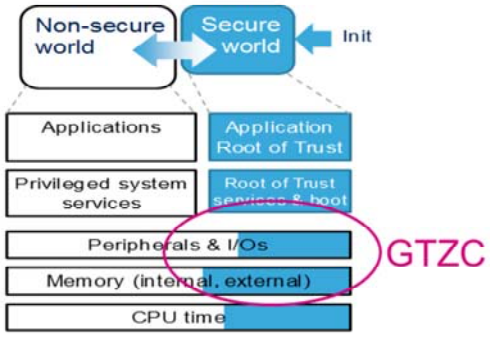


life.augmented

Hello, and welcome to this presentation of the Global TrustZone Controller, which is included in all products of the STM32L5 microcontroller family.

Overview

- STM32L5 global partitioning between secure and non-secure for securable peripherals & memories
  - The GTZC is composed of three components:
    - TrustZone® security controller (TZSC)
    - Block-based memory protection controller (MPCBB)
    - TrustZone® illegal access controller (TZIC)



Application benefits

- Reinforce in a flexible way the isolation between the secure and the non-secure worlds
- Illegal access signaling
- Either static setting or dynamic re-programming

In addition to the ARMv8-M TrustZone security extension in Cortex M33, the STM32L5 microcontroller series comes with complementary security features that reinforce in a flexible way the isolation between the secure and the non-secure worlds. It also provides a second level of security for the Cortex-M33 after the SAU/IDAU TrustZone protection.

This GTZC training module is composed of three sub-units, corresponding to each component inside GTZC.

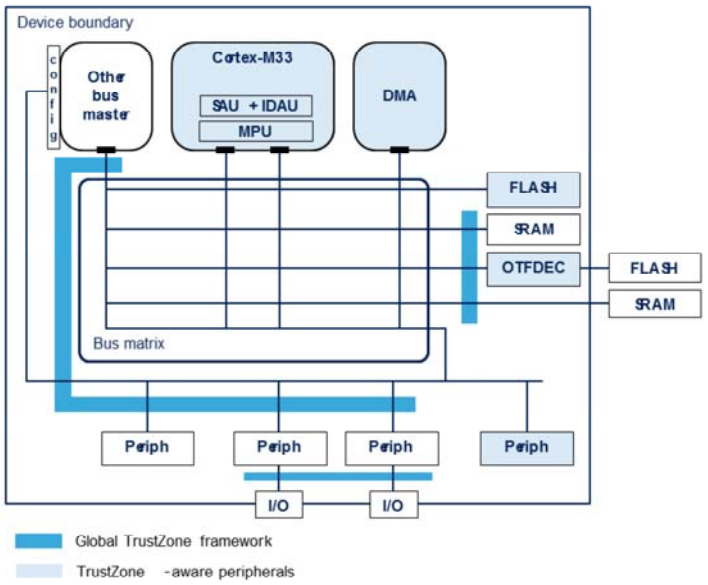
- The TrustZone Security Controller (TZSC)
- The block-based memory protection controller (MPCBB)
- The TrustZone illegal access controller (TZIC)

In addition to assigning a secure attribute, the GTZC also controls the privilege attribute that can be used even when TrustZone is disabled.

The setting of the secure attribute can be performed at any time by the secure boot firmware, unless the configuration is locked.

Global TrustZone framework architecture

3



- Complements memory and peripheral TrustZone allocation within Cortex-M33 (SAU+IDAU)
- GTZC can make non-TrustZone aware peripherals secure-only
  - If this peripheral is master on the interconnect it will issue secure transactions if it is secured with GTZC
- GTZC can make portions of embedded or external memories secure-only

Two types of peripherals are implemented in the STM32L5:

- Securable peripherals, which are protected by an AHB/APB firewall gate, controlled by GTZC
- TrustZone-aware peripherals, which implement a specific TrustZone behavior such as a subset of registers being secure.

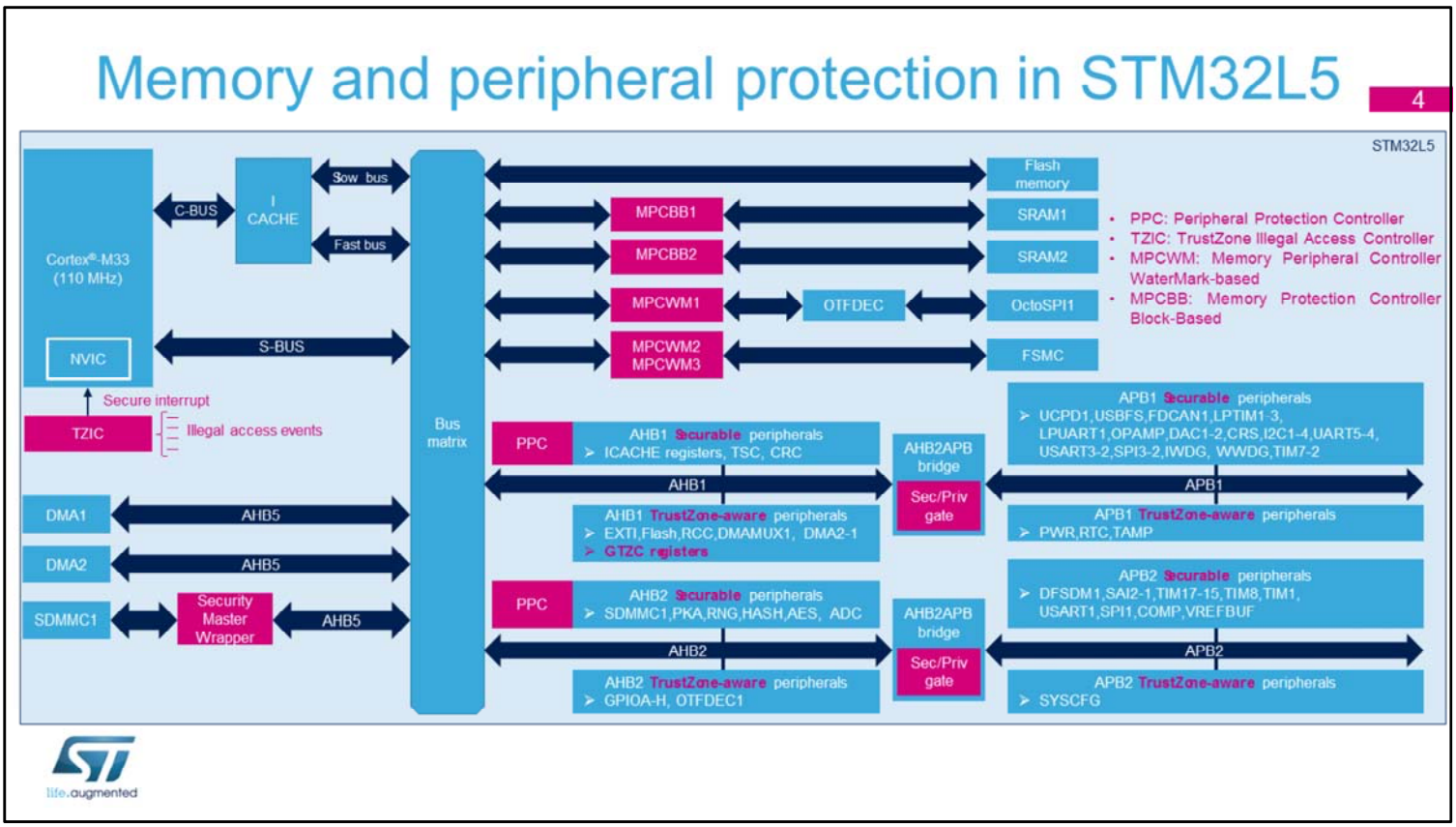
TrustZone-aware AHB masters always drive the AHB5 HNONSEC signal according to their security mode (as Cortex-M33 core and DMA).

Securable peripherals drive their (optional) AHB5 HNONSEC signal according to the security mode set in GTZC

Like with TrustZone a peripheral can be made privileged-only with GTZC. In this case, if this peripheral is master on the interconnect it automatically issues privileged transactions.

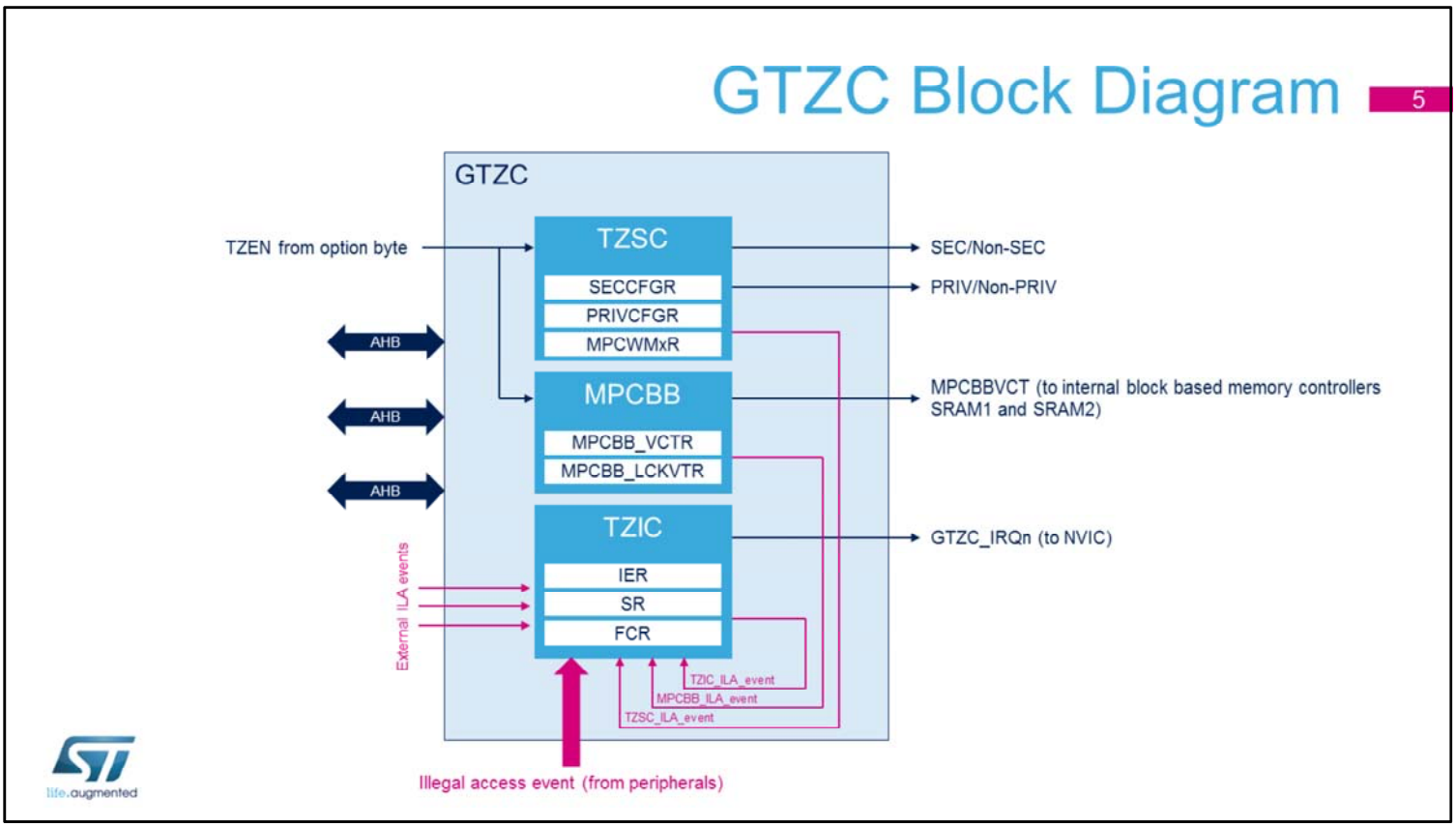
GTZC provides the capability to manage:

- the security for all securable external memories
- the security of blocks of securable embedded memories



This figure highlights the various security mechanisms present in the STM32L5, that are controlled by the GTZC:

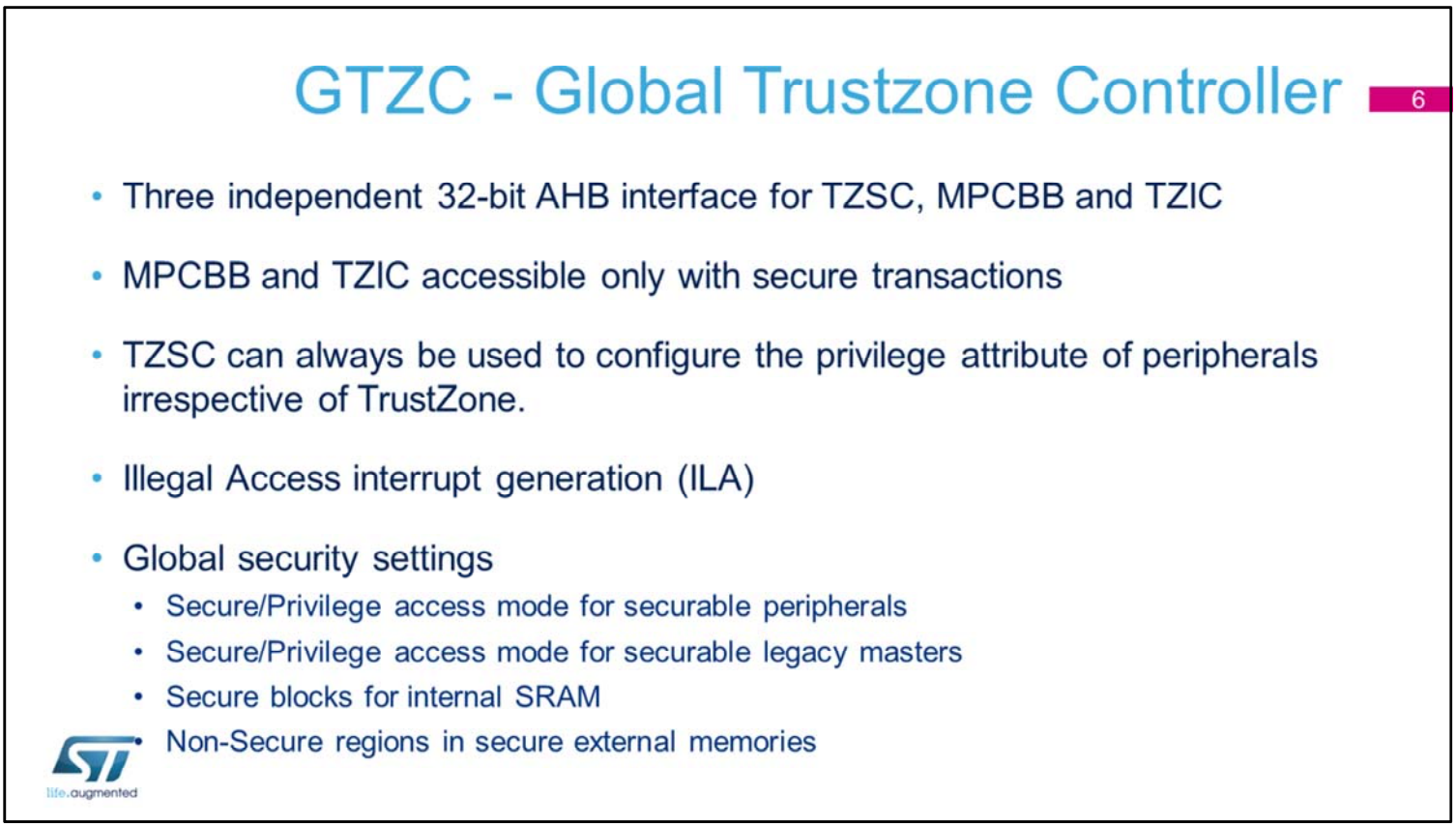
- MPCBB1 and 2 set the secure attribute of SRAM1 and SRAM2 blocks
- MPCWM1, 2 and 3 define the secure address ranges in the external memories, accessible from OctoSPI1 and FSMC
- PPC assigns secure and privilege attributes to AHB/APB securable peripherals and also checks the access permissions
- Sec/Priv gate assigns secure and privilege attributes to APB securable peripherals and also checks the permissions
- The Security Master Wrapper assigns the security attribute to the SDMMC1 master. As DMA is a TrustZone aware IP it does not require any external wrapper.
- The TZIC reports illegal accesses to the Cortex-M33 core through a secure interrupt request.



This figure details the operation of the three GTZC sub-units:

- The TZSC is in charge of assigning the secure and privilege attributes of securable peripherals and masters.
- The MPCBB is in charge of assigning the secure attribute of internal SRAM blocks
- The TZIC signals illegal accesses to the Cortex-M33 core.

Illegal accesses can occur internally or externally to the GTZC, when a non-secure access to a secure memory-mapped registers is attempted.



The GTZC supports 3 independent AHB interfaces for configuring the TZSC, the MPCBB and the TZIC.
The GTZC is a TrustZone-aware peripheral: the MPCBB and TZIC are accessible only with secure transactions, but the TZSC can be used by non-secure firmware to set the privilege attribute of non-secure peripherals.
Any attempt to access a secure resource while running in non-secure state can cause an illegal access interrupt generation.
The TZSC is in charge of setting the secure and privilege attributes to:

- Securable peripherals
- Securable masters that are not TrustZone aware

The TZSC is in charge of setting the secure attribute to external memories.
The MPCBB is in charge of setting the secure attribute to internal SRAM blocks.

TZSC features

- Provides configuration of Secure and Privilege attributes for all securable peripherals.
  - If a peripheral is a master and it is set secure it will issue always secure transactions
- Provides configuration (size) of up to two non-secure area per secure external memory (watermark). Configuration is secure-only.
  - WMxSTRT1 / WMxLGTH1: define start / length of first area
  - WMxSTRT2 / WMxLGTH2: define start / length of second area

- Security (resp. privilege) mode of peripherals is programmed in SECCFGR (resp. PRIVCFGR) registers, only accessible in secure (resp. privileged) state
  - Bit in SECCFGR becomes privileged if the corresponding peripheral is set as privileged in PRIVCFGR register
  - Bit in PRIVCFGR becomes secure if the corresponding peripheral is set as secure in PRIVCFGR register

life.augmented

The TZSC provides the configuration of secure and privilege attributes for all securable peripherals.
It is itself a TrustZone-aware peripheral, because it contains a mix of secure and non-secure registers.
The Watermark start and length register pairs define non-secure regions per protected external memory, defined secure by default. These registers are only accessible in secure state.

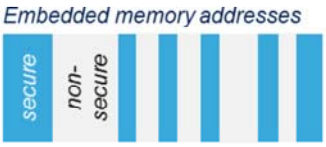
- In STM32L5 five non-secure areas can be defined this way: two in OctoSPI address range, two in FSMC NOR address range, one in FSMC NAND address range.

The SECCFGR registers set the secure attribute of peripherals. These registers are only accessible in secure state. They can be restricted to privilege state according to the PRIVCFGR register setting.
The PRIVCFGR registers set the privilege attribute of peripherals. These registers are only accessible in privilege

state. They can be restricted to secure state according to the SECCFGR register setting.
The power-on and reset state of the TZSC clears all the bits of the SECCFGRx and the PRIVCFGRx registers to 0, which respectively means non-secure and privileged or non-privileged.

MPC-BB features

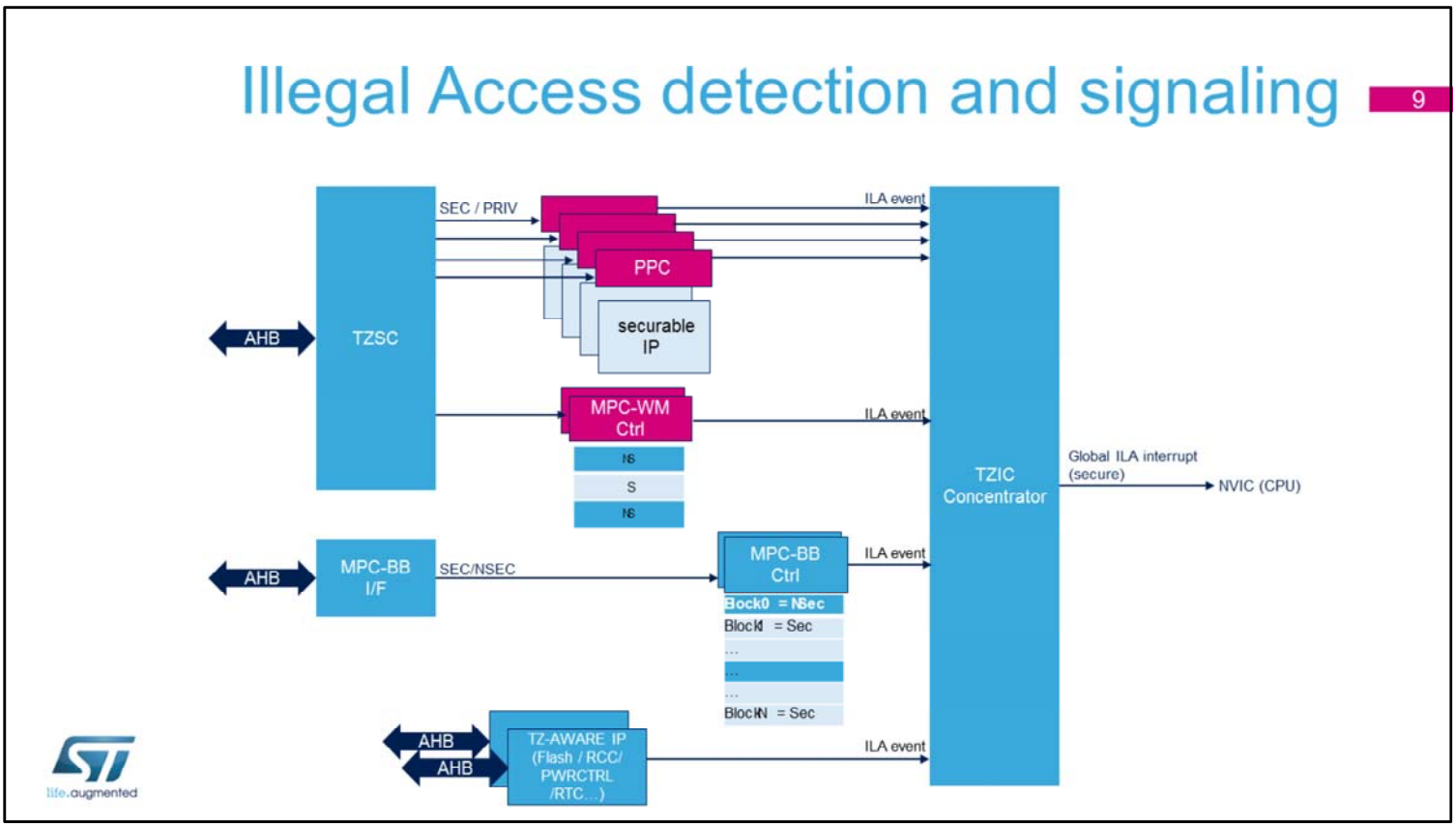
- Provides configuration, at boot or run time, of the security of all 256-bytes blocks of internal SRAMs
  - Access is secure-only



- MPCBBz_VCTRx define the security of page x located in embedded SRAMz
  - Each page has 32 blocks of 256 Bytes (size: 8 kBytes)
- Setting the SRWILADIS bit in MPCBB_CR allows secure data access to non-secure blocks (instruction access is always denied)
- All configuration in MPCBB can be locked until the next reset
  - Each MPC_VCTRx register is locked by the corresponding bit in MPCBB_LCKVTR
  - LCK bit in MPCBB_CR locks the register

life.augmented

The MPC block based configures the secure attribute of internal SRAM 256-byte blocks. Each of them has a corresponding control bit.
The MPC-BB is only accessible in secure state.
MPCBBCR is a control register. The Secure read/write illegal access disable bit determines whether secure data accesses are permitted to non-secure SRAM blocks.
The MPC-BB vector registers are bitmaps, each bit corresponding to an internal SRAM chunk of 256 bytes.
Each bit in MPC-BB Lock vector registers locks the secure mode of corresponding 8-KBytes super-block until the next reset.
A super-block contains 32 blocks of 256-bytes.



This figure details the various sources of illegal accesses and their signaling to the Cortex-M33 core through a secure interrupt request.
The TZSC assigns secure and privilege attributes to securable peripherals. Whenever a non-secure access to a secure peripheral is attempted, an illegal access is reported to the TZIC concentrator.
The MPC-Watermark controller determines which areas of external memories are non-secure. Whenever a non-secure access to a secure area is attempted, an illegal access is reported to the TZIC concentrator.
The MPC-Block based controller assigns the secure attribute to internal SRAM blocks. Whenever a non-secure access to a secure block is attempted, an illegal access is reported to the TZIC concentrator.
Finally, TrustZone-aware peripherals report an illegal access when a non-secure access attempts to access a secure resource.

The TZIC concentrator receives all these illegal access reports and signals the error to the Cortex-M33 core through a secure interrupt request.

The TZIC gathers all illegal access events and generates a maskable global secure interrupt towards the NVIC.
Only secure accesses are allowed to TZIC registers.
It supports three types of registers:

- Illegal access event mask
- Illegal access event status
- Illegal access event clear.

By default, all illegal access events are masked.
Any non-privilege transaction trying to access a privilege resource is considered as illegal. There is no illegal access event generated for this type of illegal access. The addressed resource follows a silent-fail behavior, returning all zero data for read and ignoring any write. No bus error is generated.

Related peripherals

11

- Refer to these trainings linked to this peripheral for more information
  - Interrupts (NVIC)
  - TrustZone (TRZ)

life.augmented

The GTZC has relationships with the following modules:

- Interrupts (NVIC)
- TrustZone (TRZ)