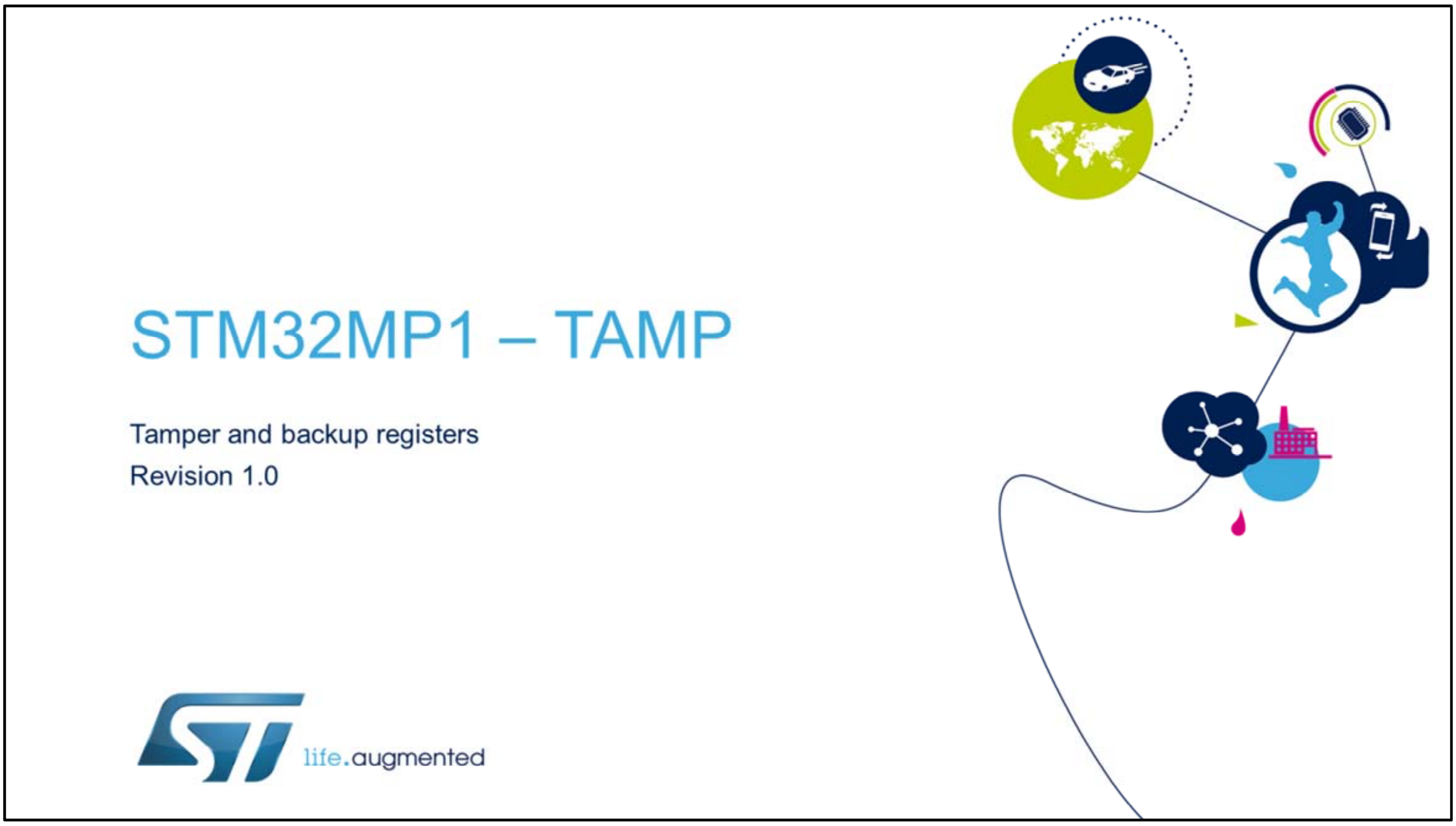
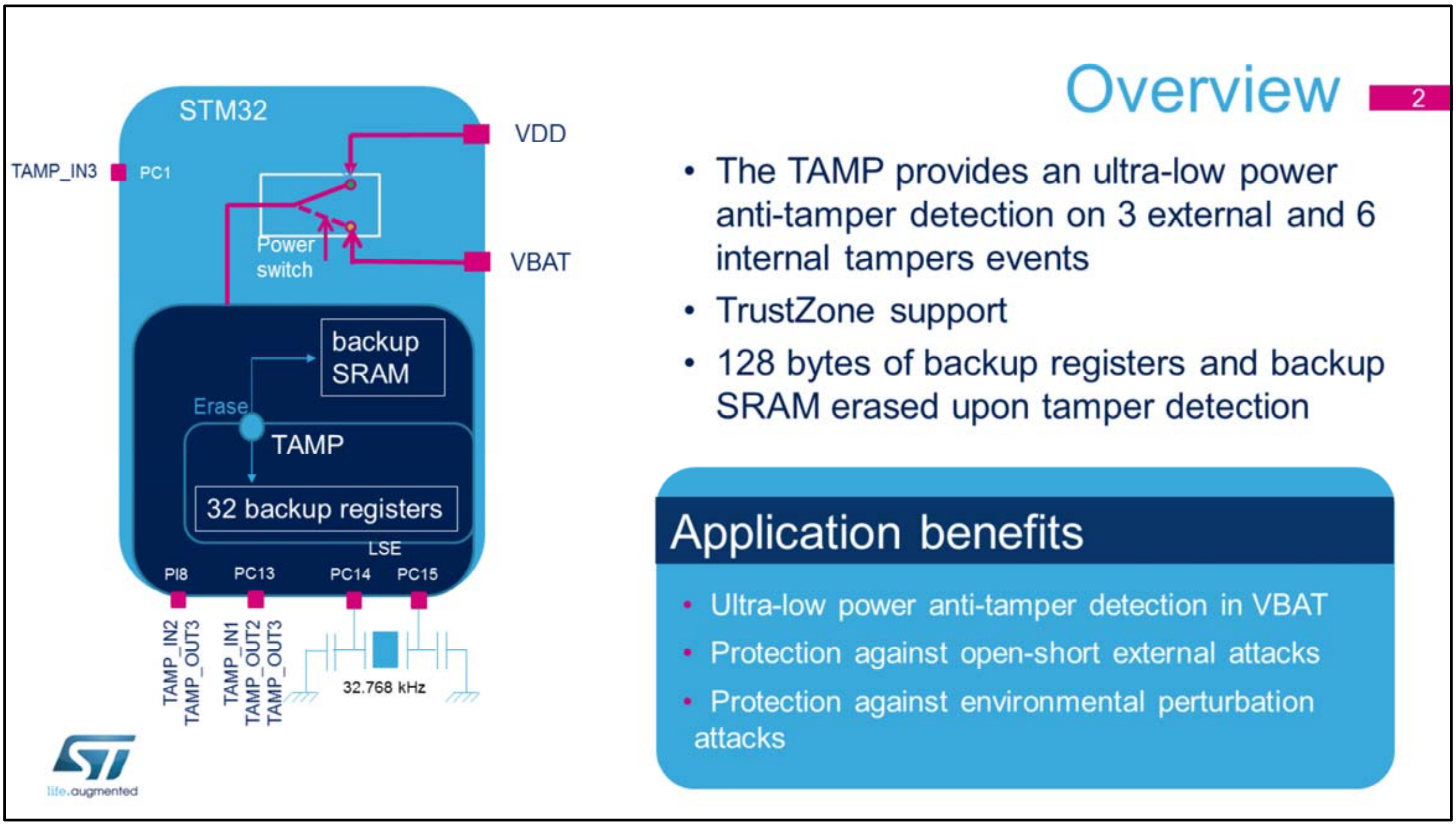


STM32MP1 – TAMP

Tamper and backup registers

Revision 1.0

Hello, and welcome to this presentation of the STM32 Tamper and backup registers. It covers the main features of this peripheral, which is used to ensure security protection against physical and environmental external attacks.



Overview

- The TAMP provides an ultra-low power anti-tamper detection on 3 external and 6 internal tampers events
- TrustZone support
- 128 bytes of backup registers and backup SRAM erased upon tamper detection

Application benefits

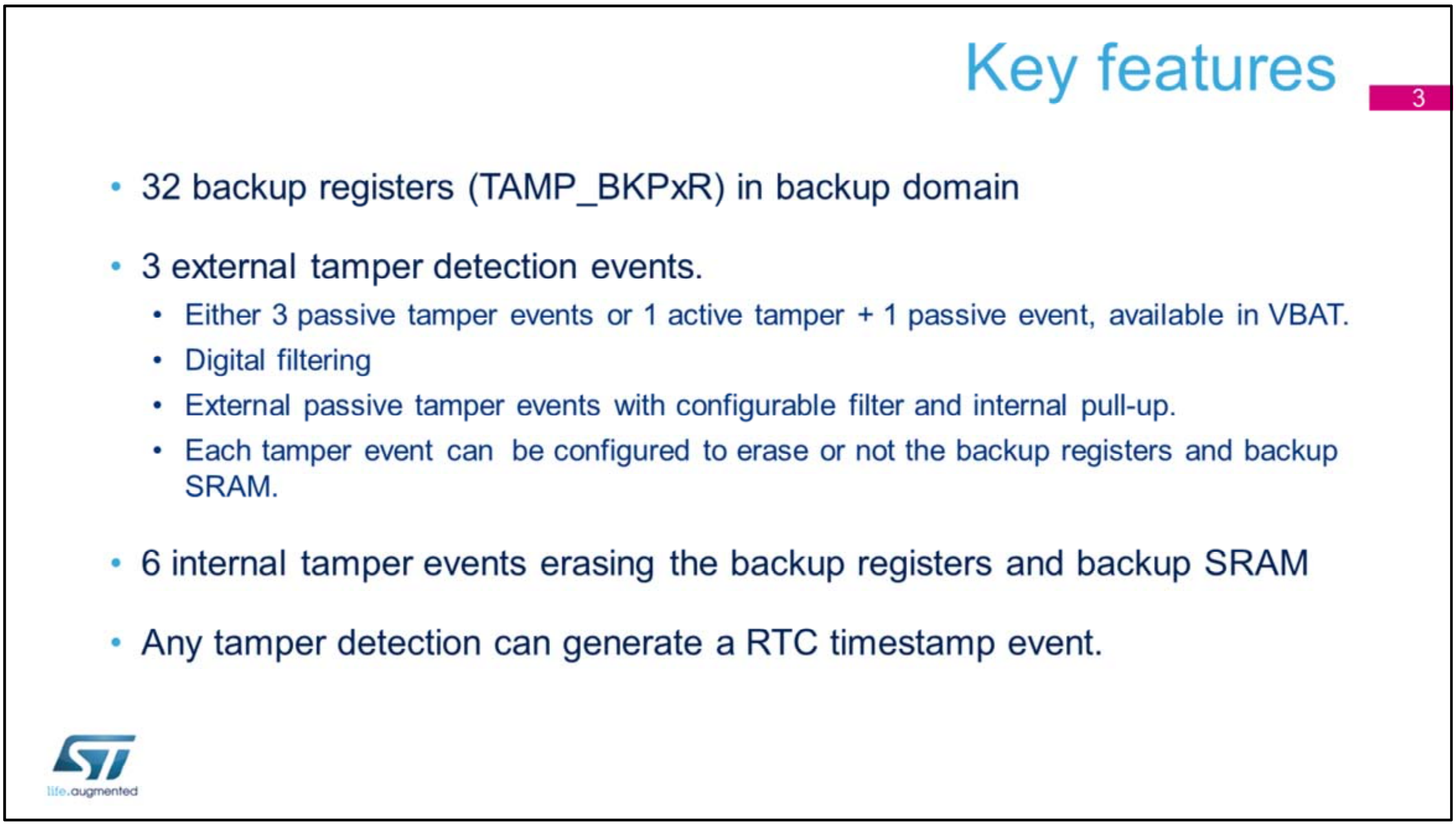
- Ultra-low power anti-tamper detection in VBAT
- Protection against open-short external attacks
- Protection against environmental perturbation attacks

The TAMP peripheral features an ultra-low power anti-tamper detection which runs in all low-power modes. Additionally, the TAMP is functional even when the main supply is off and the VBAT domain supplied by a backup battery.

The TAMP block embeds 128 bytes of backup registers, used to preserve data when the main supply is off. These backup registers can be used to store secure data, as they are erased when a tamper event is detected on the tamper pins. In addition, the backup SRAM is also erased when a tamper event occurs.

Three external events can be detected with 3 different configuration modes depending on the security application requirements, and six internal events can be generated based on embedded monitors, ensuring protection against environmental attacks.

The TAMP registers can be configured to be protected against non-secure access.



Key features

3

- 32 backup registers (TAMP_BKPxR) in backup domain
- 3 external tamper detection events.
  - Either 3 passive tamper events or 1 active tamper + 1 passive event, available in VBAT.
  - Digital filtering
  - External passive tamper events with configurable filter and internal pull-up.
  - Each tamper event can be configured to erase or not the backup registers and backup SRAM.
- 6 internal tamper events erasing the backup registers and backup SRAM
- Any tamper detection can generate a RTC timestamp event.

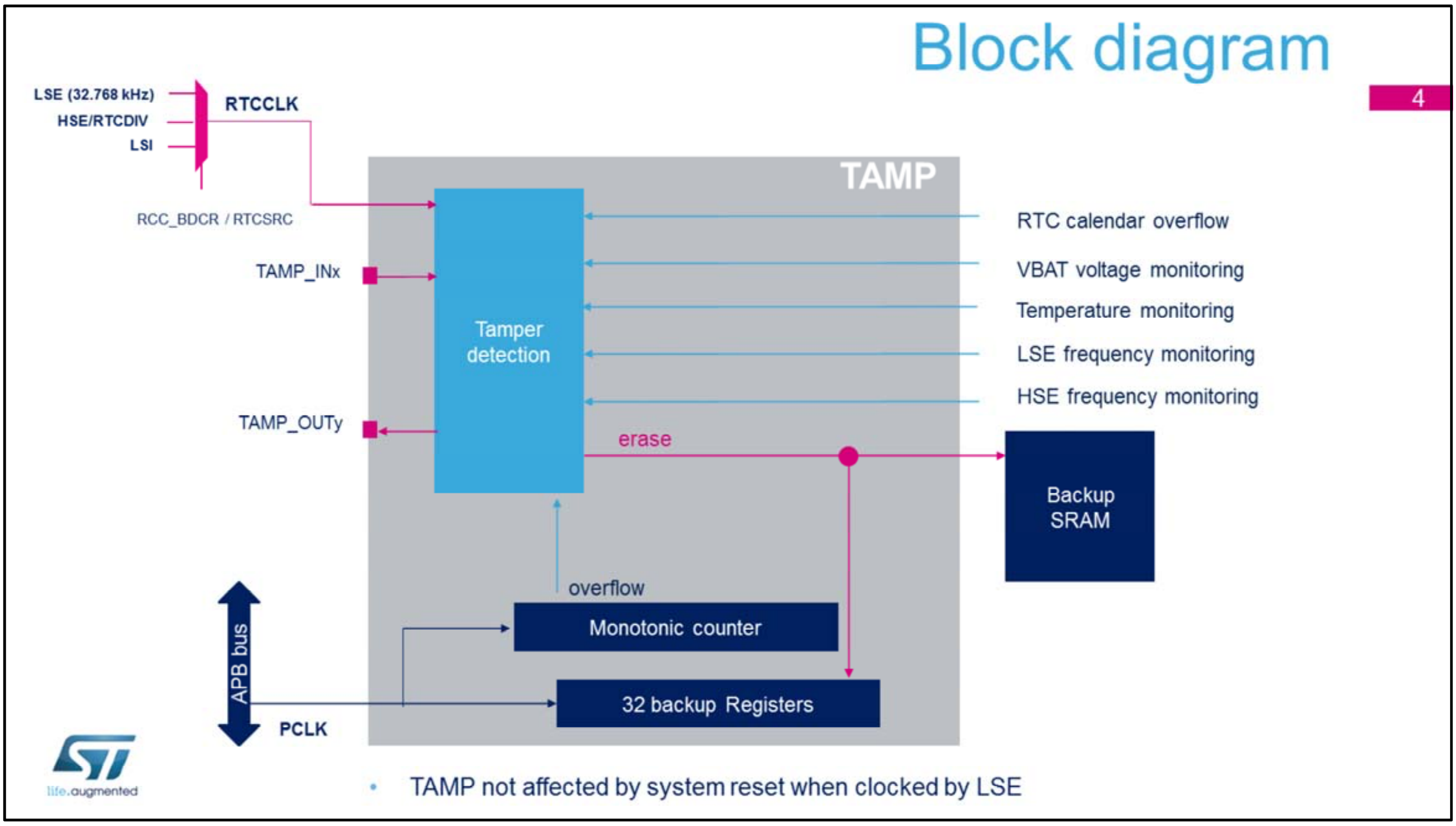
life.augmented

The key features of the TAMP are:

- 128 bytes of backup registers, split into thirty-two 32-bit backup registers. These registers are preserved in all low-power modes and in VBAT mode, and are erased when a tamper detection event occurs on any one of the three tamper pins or on the internal tamper monitors.
- Up to three external tamper events are supported. The modes of these tamper events can be configured either in passive mode or in active mode, allowing either 3 passive tampers pins and events, or 1 active tamper + 1 passive tamper event, available in all low-power modes and VBAT.
- The passive mode can either be I/O edge detection, or level detection with configurable filtering and internal pull-up which is the lowest power tamper detection mode.
- The anti-tamper circuitry includes ultra-low-power digital filtering, avoiding false tamper detections on I/Os. Each external tamper event can be individually configured to

erase or not the backup registers and backup SRAM.

- 6 internal events from various monitors erase also the backup registers and backup SRAM.
- The tamper events can generate a RTC timestamp event.



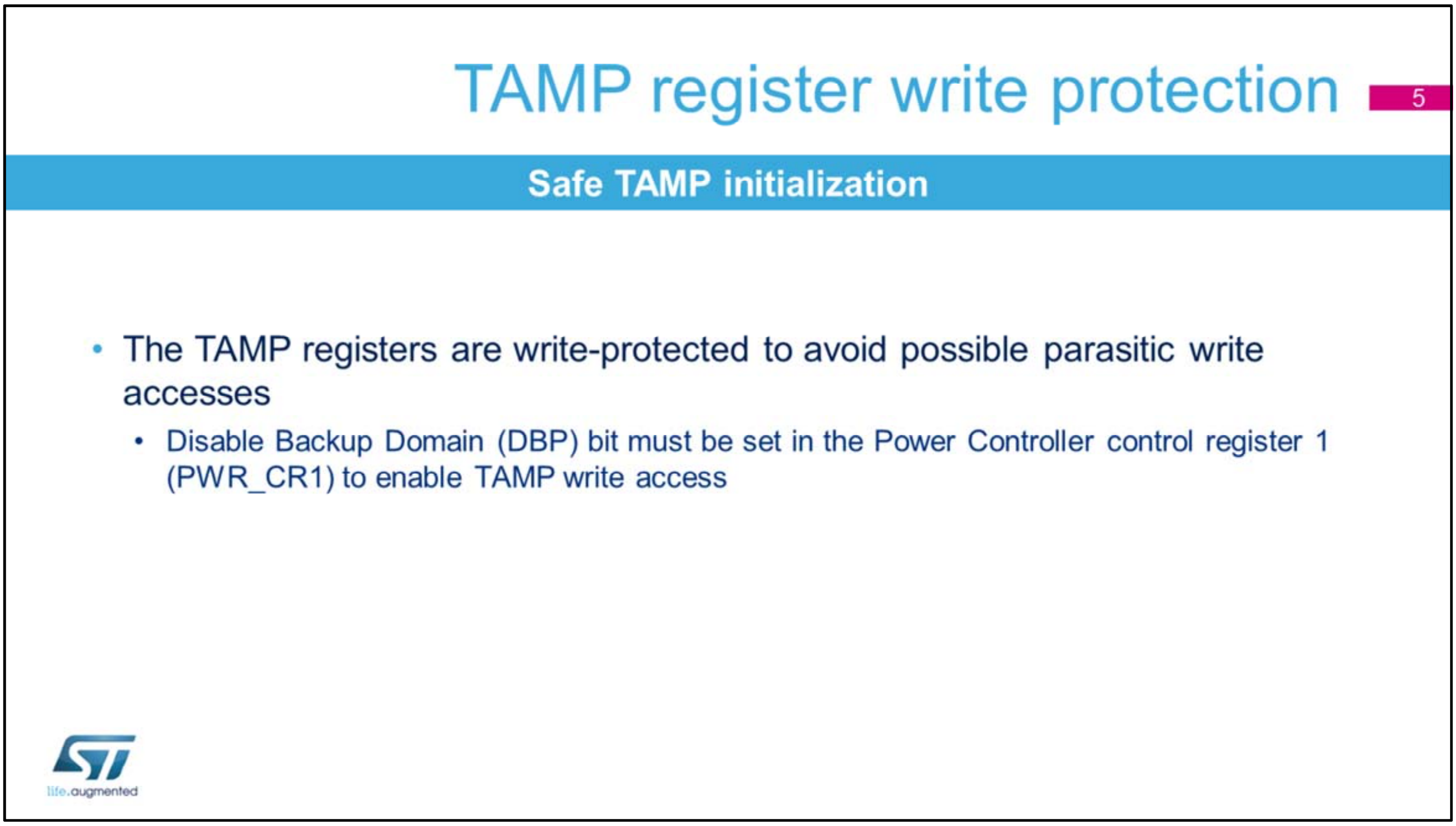
Block diagram

- TAMP not affected by system reset when clocked by LSE

Here is the TAMP block diagram. The TAMP has two clock sources: the first one is the TAMP clock (RTCCLK) which is only used for the tamper detection in level mode with filtering, and for active tamper detection.
The second clock is the APB clock used for TAMP and backup registers read and write accesses. Tampers edge detection or internal tampers detection do not need any clock. The TAMP clock can use either the high-speed external oscillator (HSE), divided by the RTCDIV divider in the Reset and Clock Control, from 1 to 64. The other clock sources are the low-speed external oscillator (LSE), or the low-speed internal oscillator (LSI). Only LSE or LSI are functional in Stop and Standby modes. Only LSE is functional in VBAT mode.

Several internal features can generate a tamper event: the temperature monitoring, the VBAT voltage monitoring, the LSE monitoring, the HSE monitoring, a RTC calendar overflow, and the monotonic counter overflow.

By default all tampers detection will erase the backup registers and the backup SRAM.



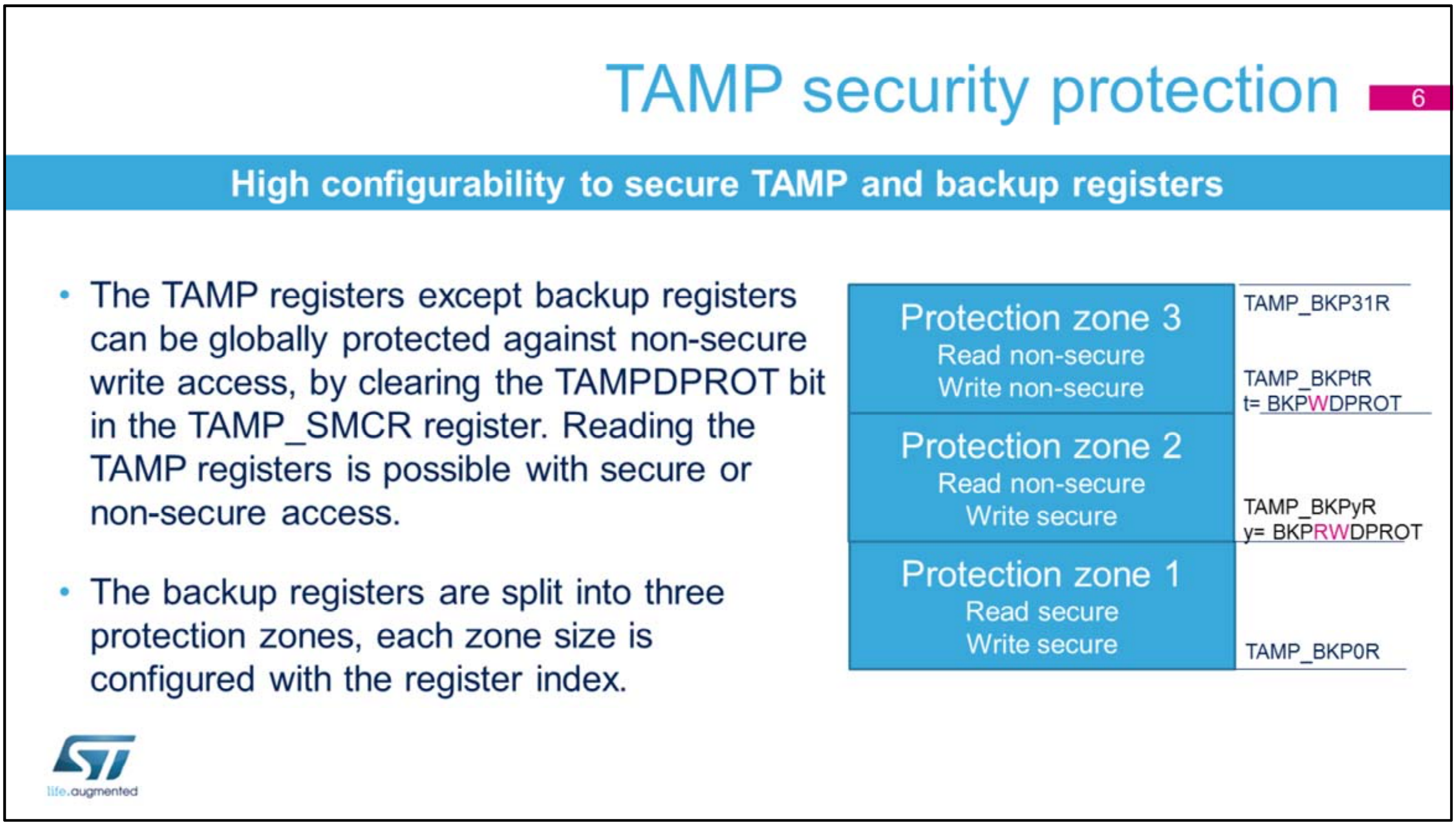
TAMP register write protection

Safe TAMP initialization

- The TAMP registers are write-protected to avoid possible parasitic write accesses
  - Disable Backup Domain (DBP) bit must be set in the Power Controller control register 1 (PWR_CR1) to enable TAMP write access

life.augmented

The TAMP registers are write-protected to avoid any possible parasitic write accesses. First, the Disable Backup Domain Protection bit must be set in the Power Controller control register in order to enable TAMP write accesses.



TAMP security protection

6

High configurability to secure TAMP and backup registers

- The TAMP registers except backup registers can be globally protected against non-secure write access, by clearing the TAMPDPROT bit in the TAMP_SMCR register. Reading the TAMP registers is possible with secure or non-secure access.
- The backup registers are split into three protection zones, each zone size is configured with the register index.

Protection zone 3
Read non-secure
Write non-secure

Protection zone 2
Read non-secure
Write secure

Protection zone 1
Read secure
Write secure

TAMP_BKP31R

TAMP_BKPtR
t= BKPWDPROT

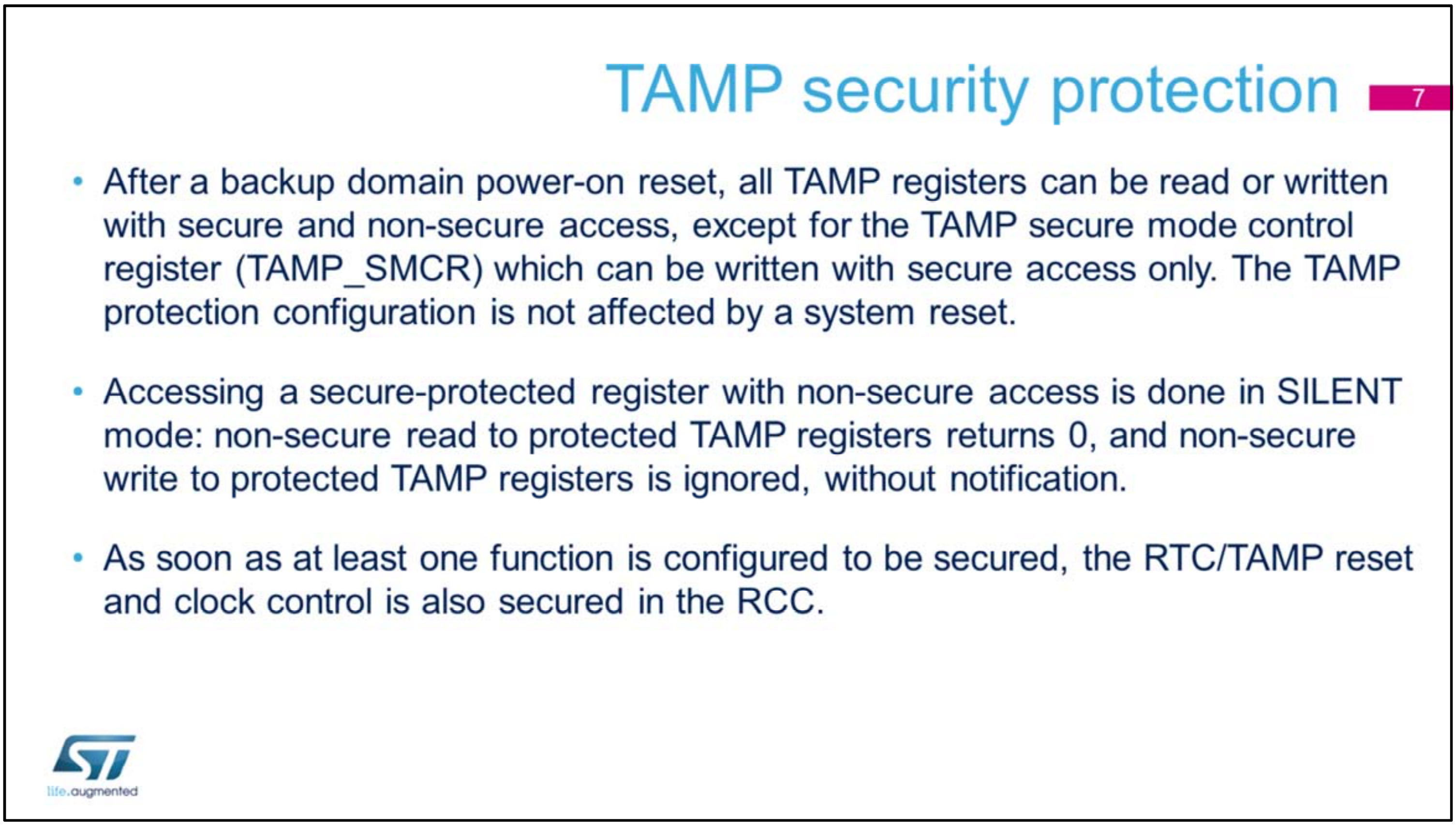
TAMP_BKPyR
y= BKPRWDPROT

TAMP_BKP0R

life.augmented

The TAMP supports TrustZone protection against non-secure write access. The protection can be set for the complete TAMP registers except backup registers by clearing the DECPROT bit in the TAMP secure mode control register. The TAMP registers protected with DECPROT can be read with secure and non-secure access.
The backup registers have their own protection setting. The backup registers can be split into three protection zones, the size of each zone is configured by software.
The protection zone 1 is protected against non-secure read access and against non-secure write access. This zone starts from Backup register 0 and ends with the register defined by the BKPRWDPROT field in the TAMP_SMCR register.
The protection zone 2 is protected against non-secure write access but can be read with secure and non-secure access. This zone starts from the register defined by the BKPRWDPROT field and ends with the register defined by

the BKPWDPROT field in the TAMP_SMCR register.
The protection zone 3 is not protected against non-secure access. This zone starts from the register defined by the BKPWDPROT field in the TAMP_SMCR register and ends with the last Backup register 31.

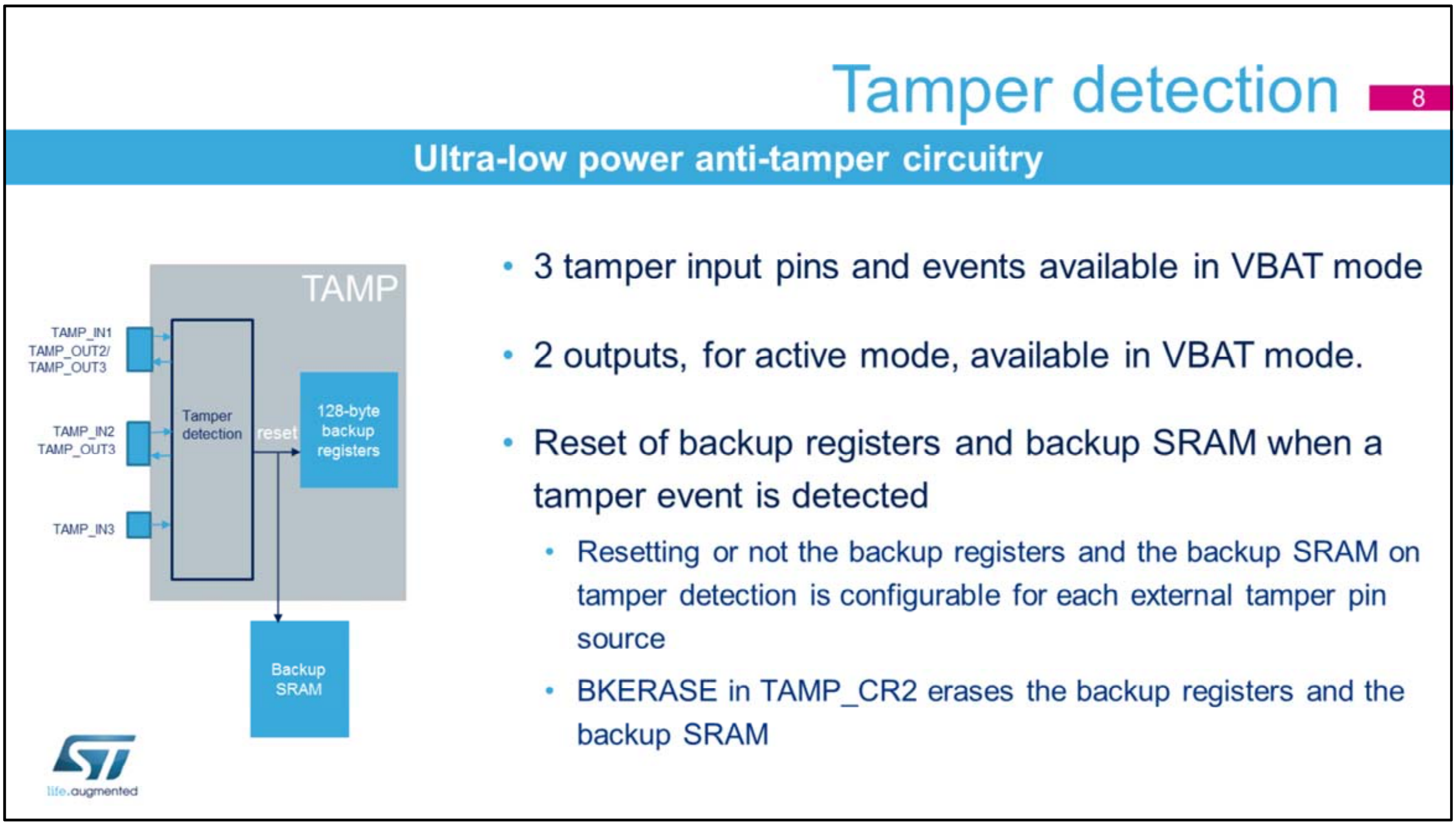


TAMP security protection

7

- After a backup domain power-on reset, all TAMP registers can be read or written with secure and non-secure access, except for the TAMP secure mode control register (TAMP_SMCR) which can be written with secure access only. The TAMP protection configuration is not affected by a system reset.
- Accessing a secure-protected register with non-secure access is done in SILENT mode: non-secure read to protected TAMP registers returns 0, and non-secure write to protected TAMP registers is ignored, without notification.
- As soon as at least one function is configured to be secured, the RTC/TAMP reset and clock control is also secured in the RCC.

After a backup domain power-on reset, all TAMP registers can be read or written with secure and non-secure access, except for the TAMP secure mode control register which can be written with secure access only. The TAMP protection configuration is not affected by a system reset.
Accessing a secure-protected register with non-secure access is done in SILENT mode: the read-protected registers are read as 0, the write-protected bits are not written without notification.
As soon as at least one function is configured to be secured, the RTC and TAMP reset and clock control is also secured in the RCC.



Tamper detection

8

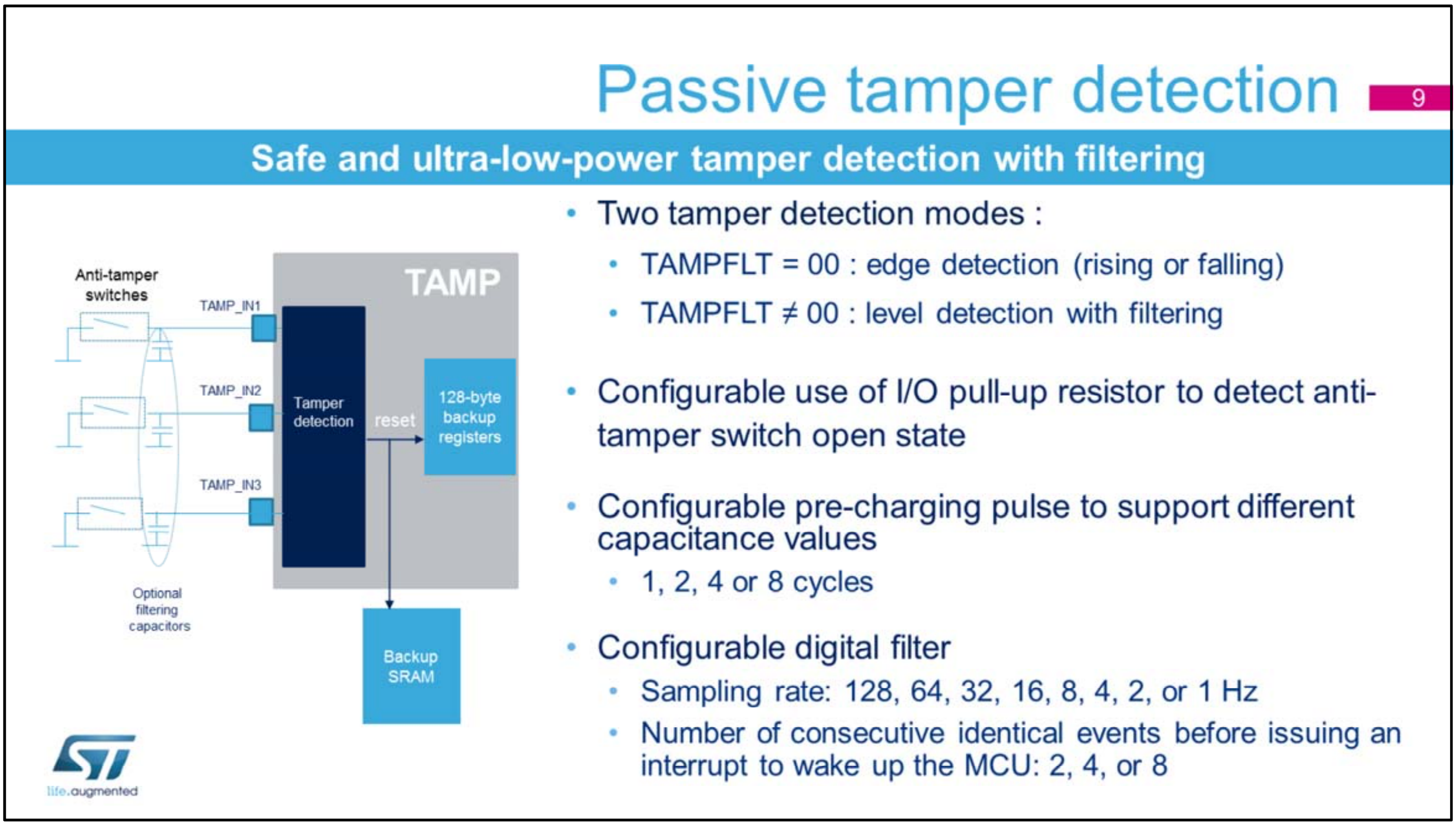
Ultra-low power anti-tamper circuitry

- 3 tamper input pins and events available in VBAT mode
- 2 outputs, for active mode, available in VBAT mode.
- Reset of backup registers and backup SRAM when a tamper event is detected
  - Resetting or not the backup registers and the backup SRAM on tamper detection is configurable for each external tamper pin source
  - BKERASE in TAMP_CR2 erases the backup registers and the backup SRAM

The TAMP features an ultra-low-power tamper detection circuitry. The purpose is to protect the device content and functionality against external attacks, This is required for secure applications. In case of intrusion, sensitive data are automatically erased.

3 tamper input pins and events are supported, and are functional in all low-power modes and in VBAT mode. 2 output pins used in active tamper mode are functional in all low-power modes and in VBAT mode.

In the default configuration, the Backup registers and the backup SRAM content are erased when a tamper event is detected. Each tamper event can be individually configured to not erase the Backup registers and the backup SRAM . In this case, the software can perform some checks to discriminate if it is a true or a false tamper event and then decide to launch the backup registers and the backup SRAM erasure by setting the BKERASE bit in the TAMP_CR2 register, in case the tamper event is confirmed to be real.



Passive tamper detection

9

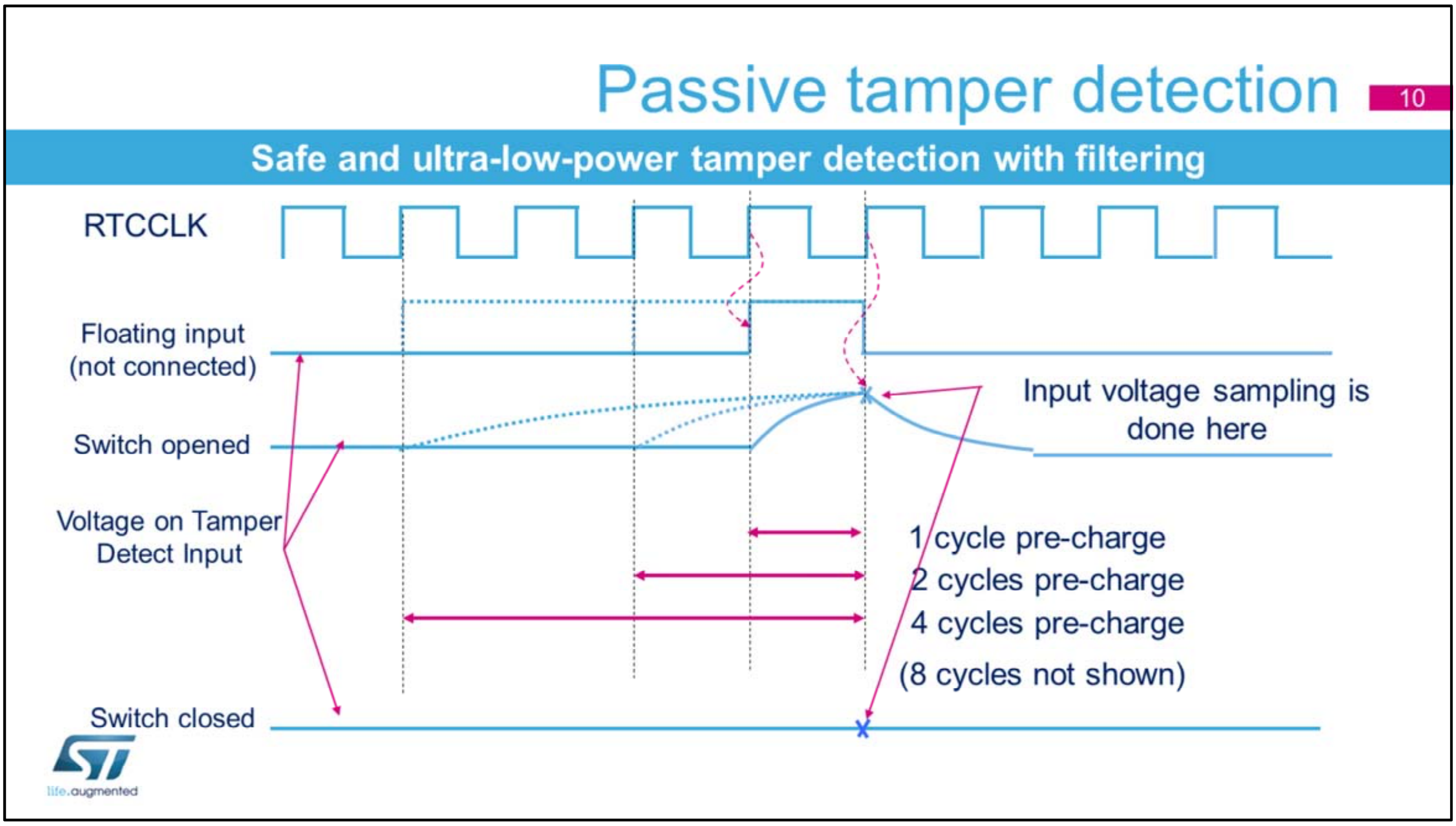
Safe and ultra-low-power tamper detection with filtering

- Two tamper detection modes :
  - TAMPFLT = 00 : edge detection (rising or falling)
  - TAMPFLT ≠ 00 : level detection with filtering
- Configurable use of I/O pull-up resistor to detect anti-tamper switch open state
- Configurable pre-charging pulse to support different capacitance values
  - 1, 2, 4 or 8 cycles
- Configurable digital filter
  - Sampling rate: 128, 64, 32, 16, 8, 4, 2, or 1 Hz
  - Number of consecutive identical events before issuing an interrupt to wake up the MCU: 2, 4, or 8

life.augmented

Passive tamper can be configured either in edge detection mode, or in level detection with filtering mode. In edge detection mode, it is possible to configure the detection on the rising or falling edge.
In level detection with filtering mode, the internal I/O pull-up is used to detect the anti-tamper switch open state. The I/O pull-up is applied only during the pre-charging pulse in order to avoid any consumption if the tamper pin is at a low level. The pre-charging pulse duration is configurable to support different capacitance values, and can be 1, 2, 4 or 8 RTC clock cycles. The pin level is sampled at the end of the pre-charging pulse.

The tamper detection circuit includes an ultra-low power digital filter to reduce the risk of false tamper events detection. It consists of detecting a given number of consecutive identical events before issuing an interrupt to wake up the device. This number is configurable and can be 2, 4 or 8 events, at a programmable sampling rate ranging from 1 to 128 Hz.



Passive tamper detection

10

Safe and ultra-low-power tamper detection with filtering

RTCCLK

Floating input (not connected)

Switch opened

Voltage on Tamper Detect Input

Switch closed

Input voltage sampling is done here

1 cycle pre-charge

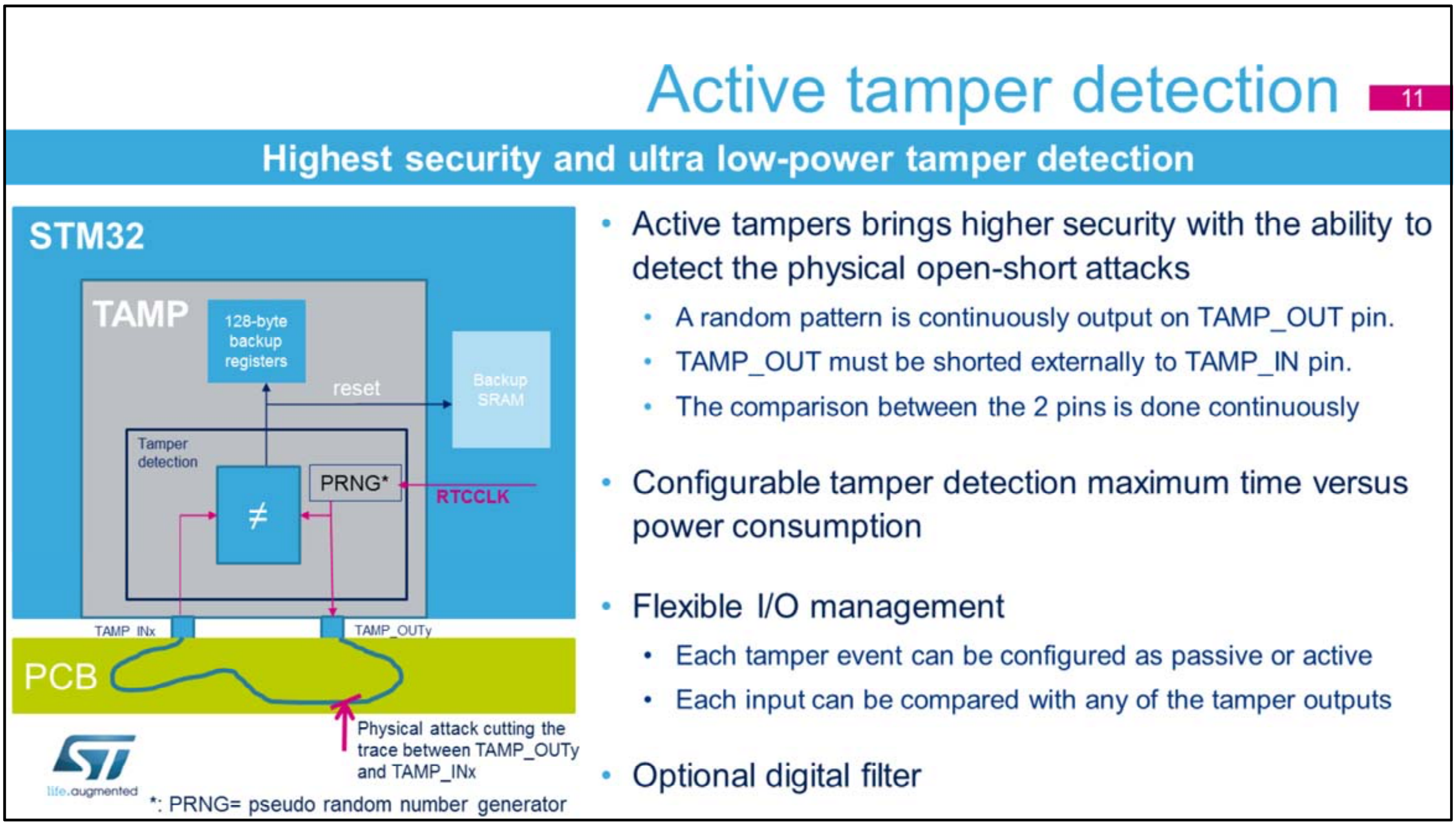
2 cycles pre-charge

4 cycles pre-charge

(8 cycles not shown)

life.augmented

This figure illustrates tamper detection using the internal pull-up. The internal pull-up can be applied for 1, 2, 4 or 8 cycles.
If the switch is opened, the level is pulled-up by the resistor.
If the switch is closed, the level remains low.
The input voltage is sampled at the end of the pre-charge pulse.



Active tamper detection

11

Highest security and ultra low-power tamper detection

- Active tampers brings higher security with the ability to detect the physical open-short attacks
  - A random pattern is continuously output on TAMP_OUT pin.
  - TAMP_OUT must be shorted externally to TAMP_IN pin.
  - The comparison between the 2 pins is done continuously
- Configurable tamper detection maximum time versus power consumption
- Flexible I/O management
  - Each tamper event can be configured as passive or active
  - Each input can be compared with any of the tamper outputs
- Optional digital filter

Physical attack cutting the trace between TAMP_OUTy and TAMP_INx

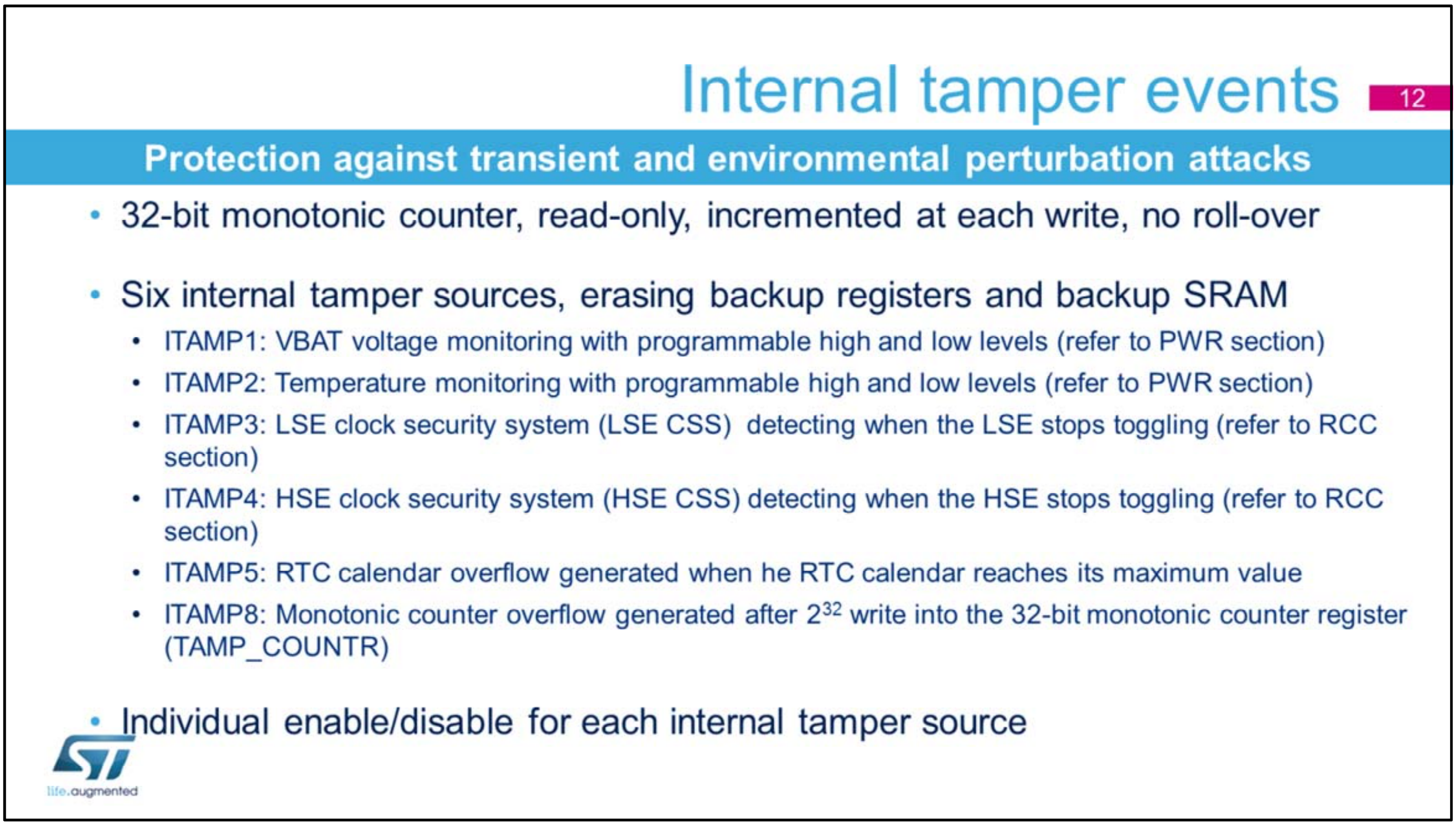
*: PRNG= pseudo random number generator

The tamper detection can be configured in active mode for a higher security level. The passive tamper detection just checks a static level, so if the attack manages to short the tamper input pin to the inactive state, the tamper event will not be detected. The active tamper is able to detect the physical open-short attacks.

With the active tamper, the MCU outputs a random pattern continuously on the TAMP_OUT pin. This output pin must be shorted externally to a TAMP_IN pin. The comparison between the 2 pins is done continuously, so if there is a short on the tamper pin or if the external wire is broken by a physical intrusion, it will be detected thanks to the fact that after each TAMP_OUT value (coming from a random number generator), the opposite value is also sent after. So it is not possible to have a long sequence of same 0 or 1 value. The change frequency of the TAMP_OUT value is software programmable, and impacts the intrusion detection maximum time. The power consumption can be reduced by decreasing the TAMP_OUT frequency, and consequently increasing the detection time.
A PCB mesh is used for active tamper detection.

The tamper events can be individually configured to be passive (only the input is needed) or active (an output must be associated to an input for comparison). In active tamper mode, the tamper output pin to be compared with each tamper input pin is selected by software, and the same output can be used for several inputs.

A digital filter can be enabled to reduce the risk of false tamper events detection. In this case, the tamper is detected only when 2 comparisons are false, in 4 consecutive comparison samples.



Internal tamper events

12

Protection against transient and environmental perturbation attacks

- 32-bit monotonic counter, read-only, incremented at each write, no roll-over
- Six internal tamper sources, erasing backup registers and backup SRAM
  - ITAMP1: VBAT voltage monitoring with programmable high and low levels (refer to PWR section)
  - ITAMP2: Temperature monitoring with programmable high and low levels (refer to PWR section)
  - ITAMP3: LSE clock security system (LSE CSS) detecting when the LSE stops toggling (refer to RCC section)
  - ITAMP4: HSE clock security system (HSE CSS) detecting when the HSE stops toggling (refer to RCC section)
  - ITAMP5: RTC calendar overflow generated when he RTC calendar reaches its maximum value
  - ITAMP8: Monotonic counter overflow generated after 2^{32} write into the 32-bit monotonic counter register (TAMP_COUNTR)
- Individual enable/disable for each internal tamper source

life.augmented

Several monitors are integrated in the device to detect perturbation and environmental attacks. These monitors are connected to the internal tamper detection blocks, which can be individually enabled or disabled, and which erase the backup registers and backup SRAM content in case of internal tamper event.

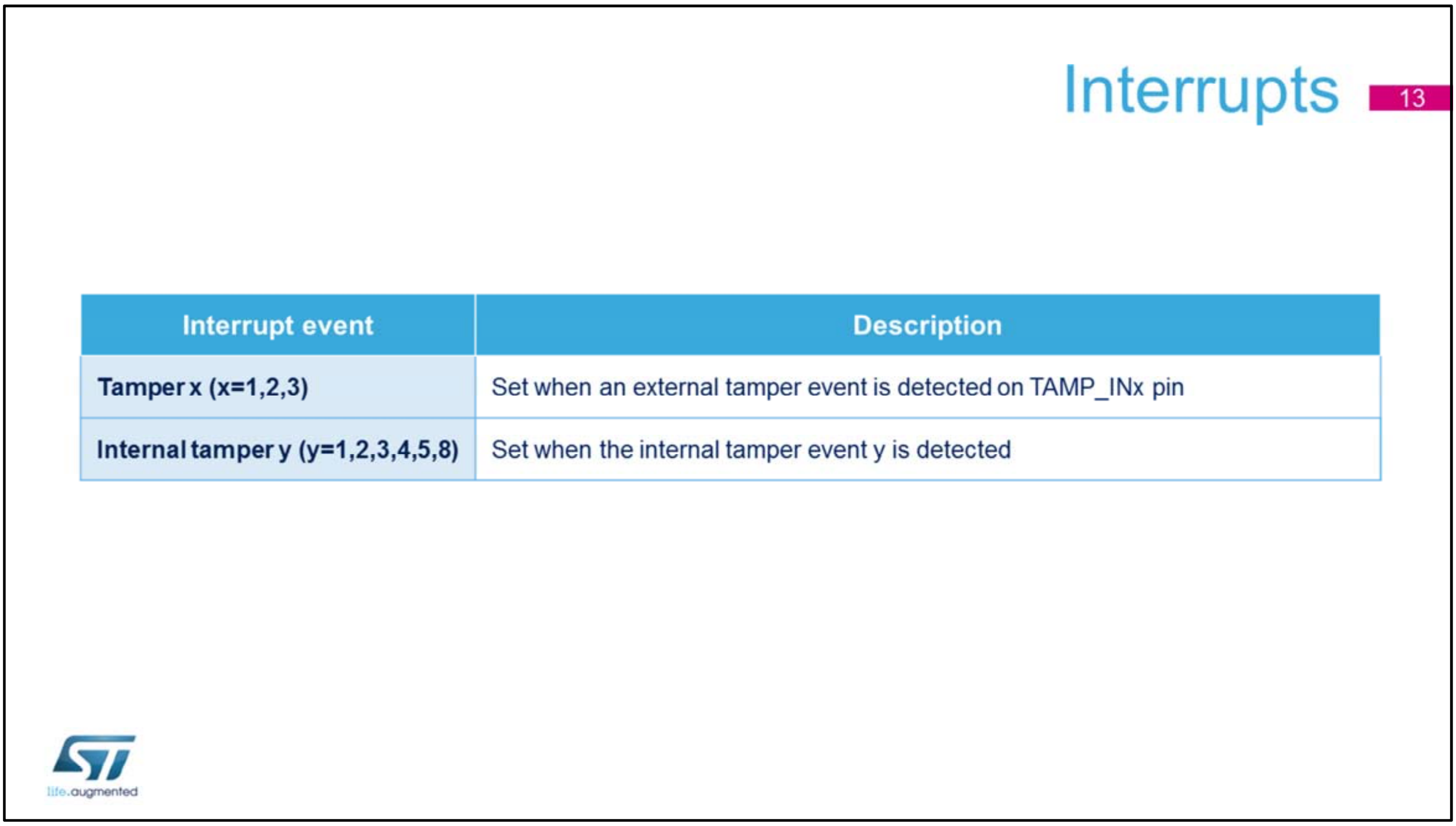
A 32-bit monotonic counter is implemented in the TAMP peripheral. This register is read-only and is incremented by one when a write access is done to this register. This register cannot roll-over and is frozen when reaching the maximum value. The 2 power 32 last write into this counter can generate a tamper event. The monotonic counter overflow is connected to the internal tamper detection block 8.

Environmental perturbation attacks can be detected thanks to VBAT voltage monitoring and temperature monitoring, both available in all low-power modes and in VBAT mode. For each monitor, the low level and the high level thresholds are programmable. VBAT voltage monitor is connected to the internal tamper detection block 1 and temperature monitor is connected to the internal tamper detection block 2.

A RTC clock attack can be detected thanks to the LSE clock security system in the Reset and Clock Control, which detects when the LSE stops toggling. The CSS on LSE is available in all low-power modes, but not in VBAT mode. CSS on LSE is connected to the internal tamper detection block 3.

If the HSE is used as system clock, a tamper can be generated in case the HSE stops toggling thanks to the HSE clock security system in the Reset and Clock Control. CSS on HSE is connected to the internal tamper detection block 4.

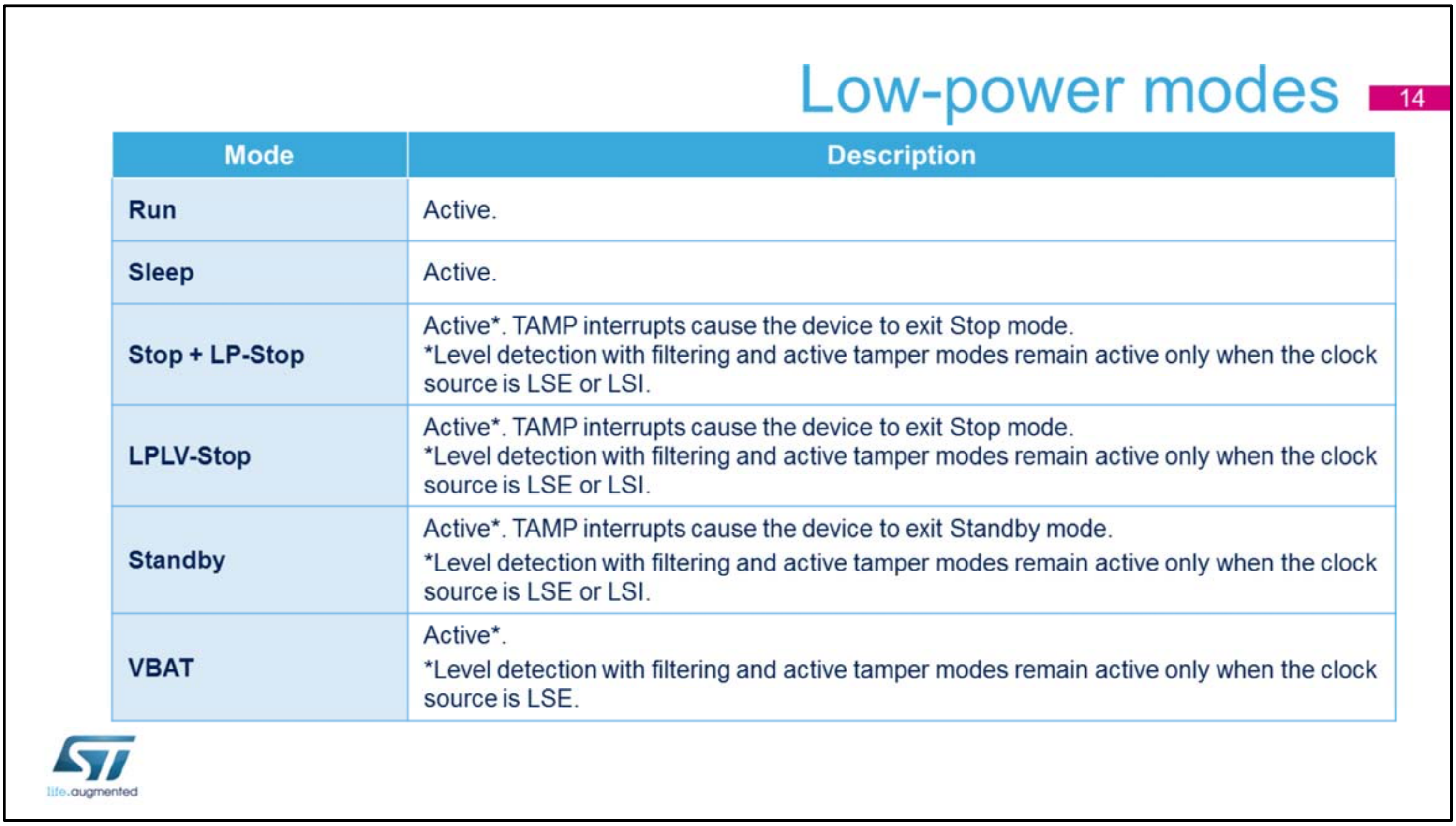
Software attacks to corrupt the RTC counters can be detected thanks to the RTC calendar overflow generated when he RTC calendar reaches its maximum value, on the 31st of December 99, at 23:59:59. The calendar is then frozen and cannot overflow. The RTC calendar overflow is connected to the internal tamper detection block 5.



Interrupts

Interrupt event	Description
Tamper x (x=1,2,3)	Set when an external tamper event is detected on TAMP_INx pin
Internal tamper y (y=1,2,3,4,5,8)	Set when the internal tamper event y is detected

Each tamper detection event, external and internal, can generate an interrupt.

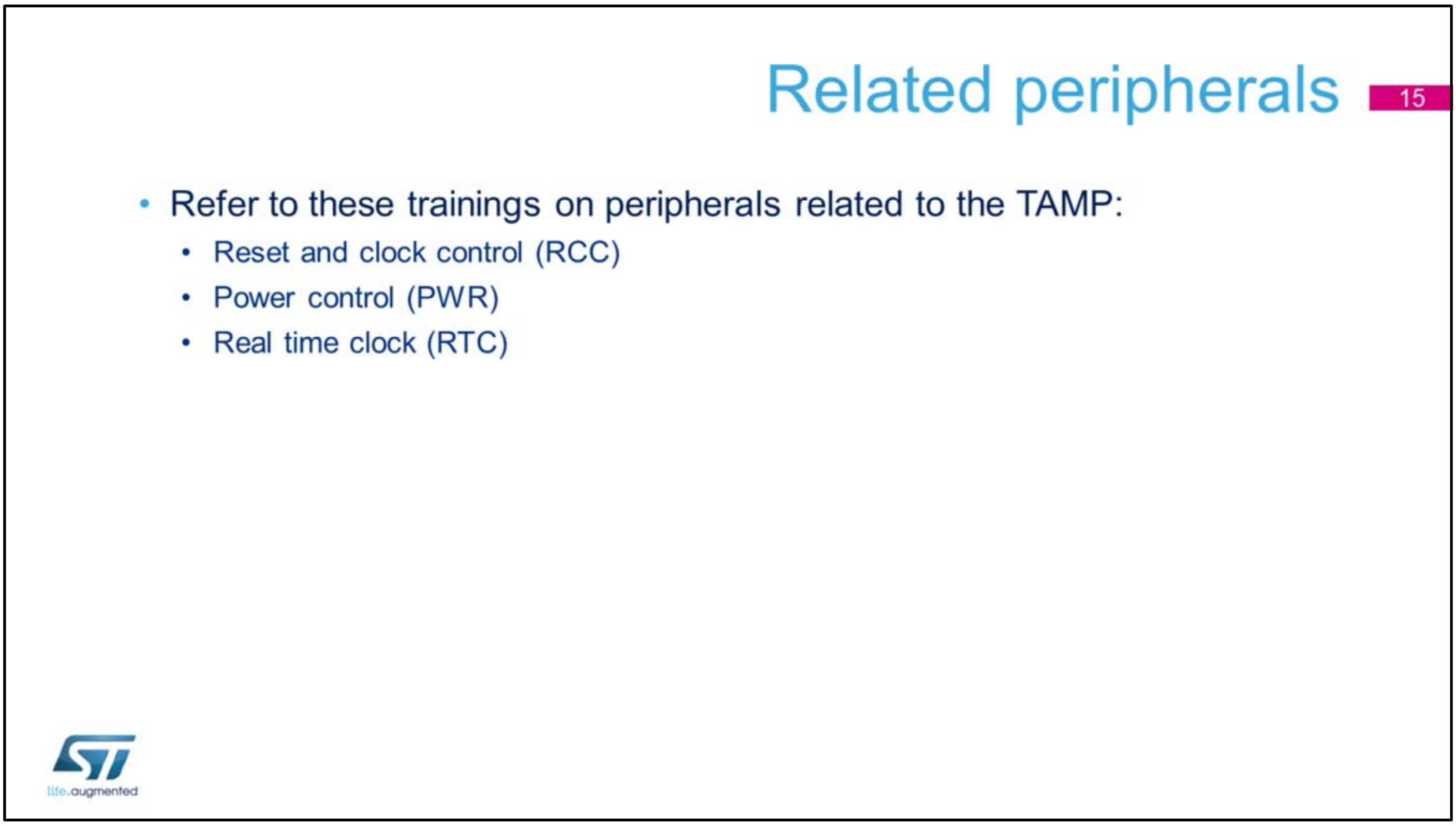


Low-power modes

Mode	Description
Run	Active.
Sleep	Active.
Stop + LP-Stop	Active*. TAMP interrupts cause the device to exit Stop mode. *Level detection with filtering and active tamper modes remain active only when the clock source is LSE or LSI.
LPLV-Stop	Active*. TAMP interrupts cause the device to exit Stop mode. *Level detection with filtering and active tamper modes remain active only when the clock source is LSE or LSI.
Standby	Active*. TAMP interrupts cause the device to exit Standby mode. *Level detection with filtering and active tamper modes remain active only when the clock source is LSE or LSI.
VBAT	Active*. *Level detection with filtering and active tamper modes remain active only when the clock source is LSE.

life.augmented

The TAMP peripheral is active in all low-power modes and in VBAT mode. In Stop and Standby modes, the level detection with filtering and active tamper modes remain active only when the clock source is LSE or LSI. Note that only the LSE clock is functional in VBAT mode. If the tamper source is available in low-power mode, the TAMP interrupts cause the device to exit a low-power mode.



Related peripherals

15

- Refer to these trainings on peripherals related to the TAMP:
  - Reset and clock control (RCC)
  - Power control (PWR)
  - Real time clock (RTC)

This is a list of peripherals related to the tamper and backup registers peripheral. Please refer to these peripheral trainings for more information if needed.

- Reset and clock control
- Power control
- Real time clock