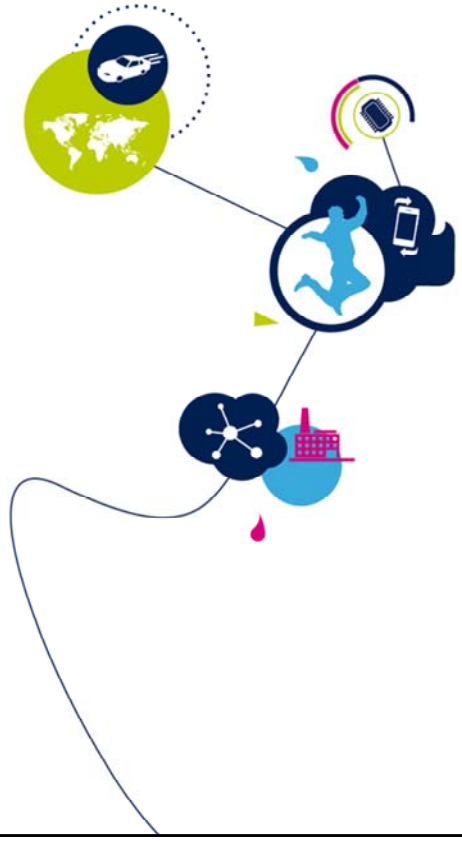
STM32L5 – TAMP

Tamper and backup registers

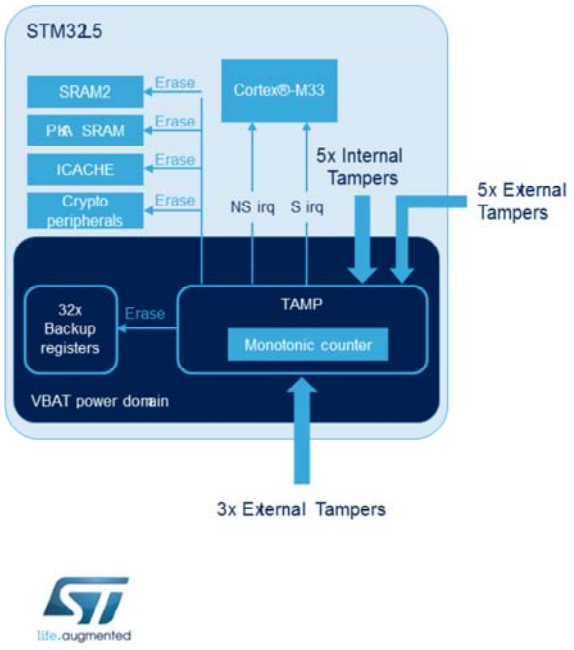
Revision 1.0



life.augmented

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 provide security against tamper events.

Overview

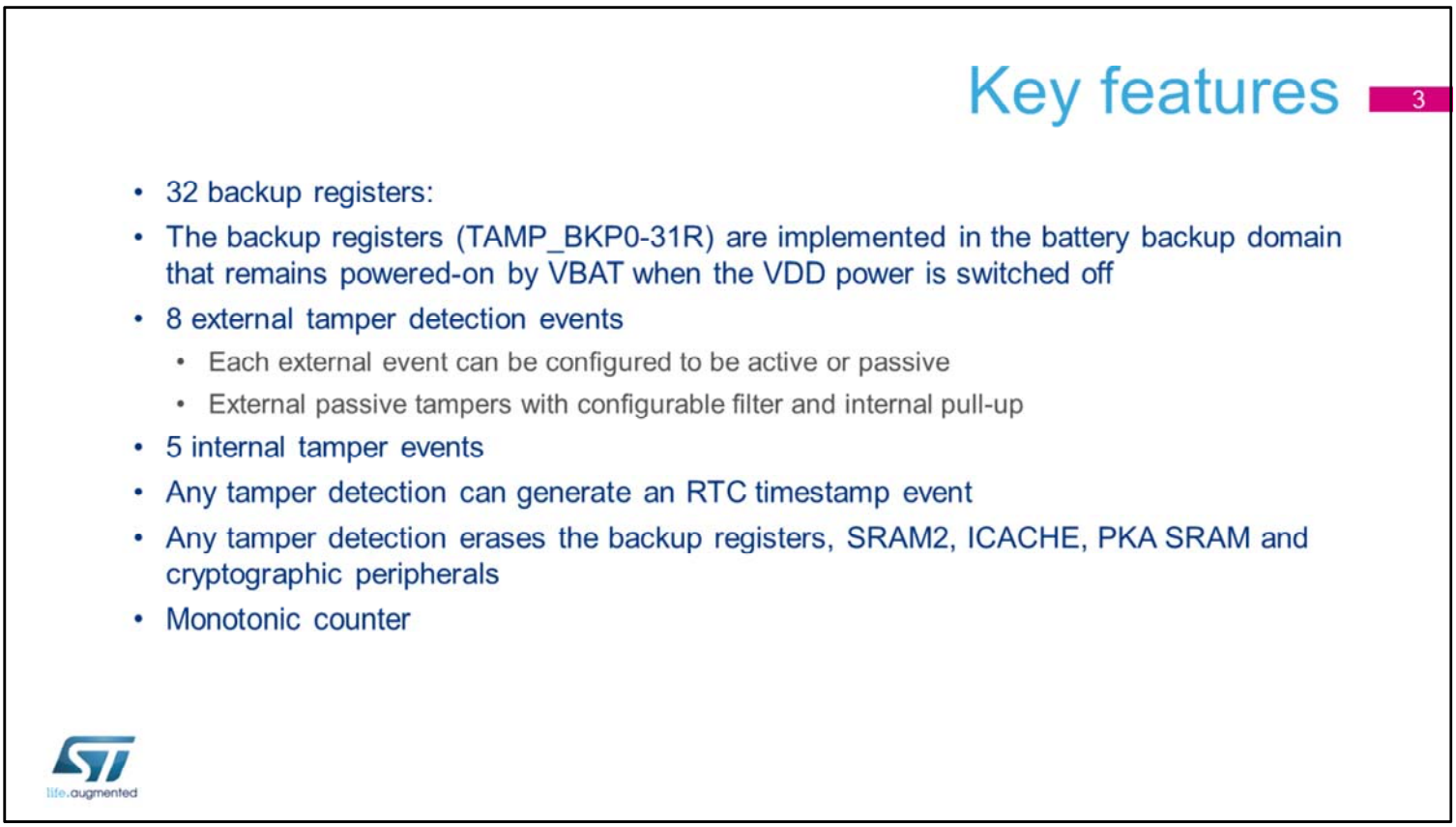


- The TAMP features 32 backup registers, erased on tamper detection
- Two types of tamper input:
  - External (8 GPIOs)
  - Internal (5 sources)
- TAMP unit belongs to the Battery Backup Domain, so it remains functional when the main supply is off

Application benefits

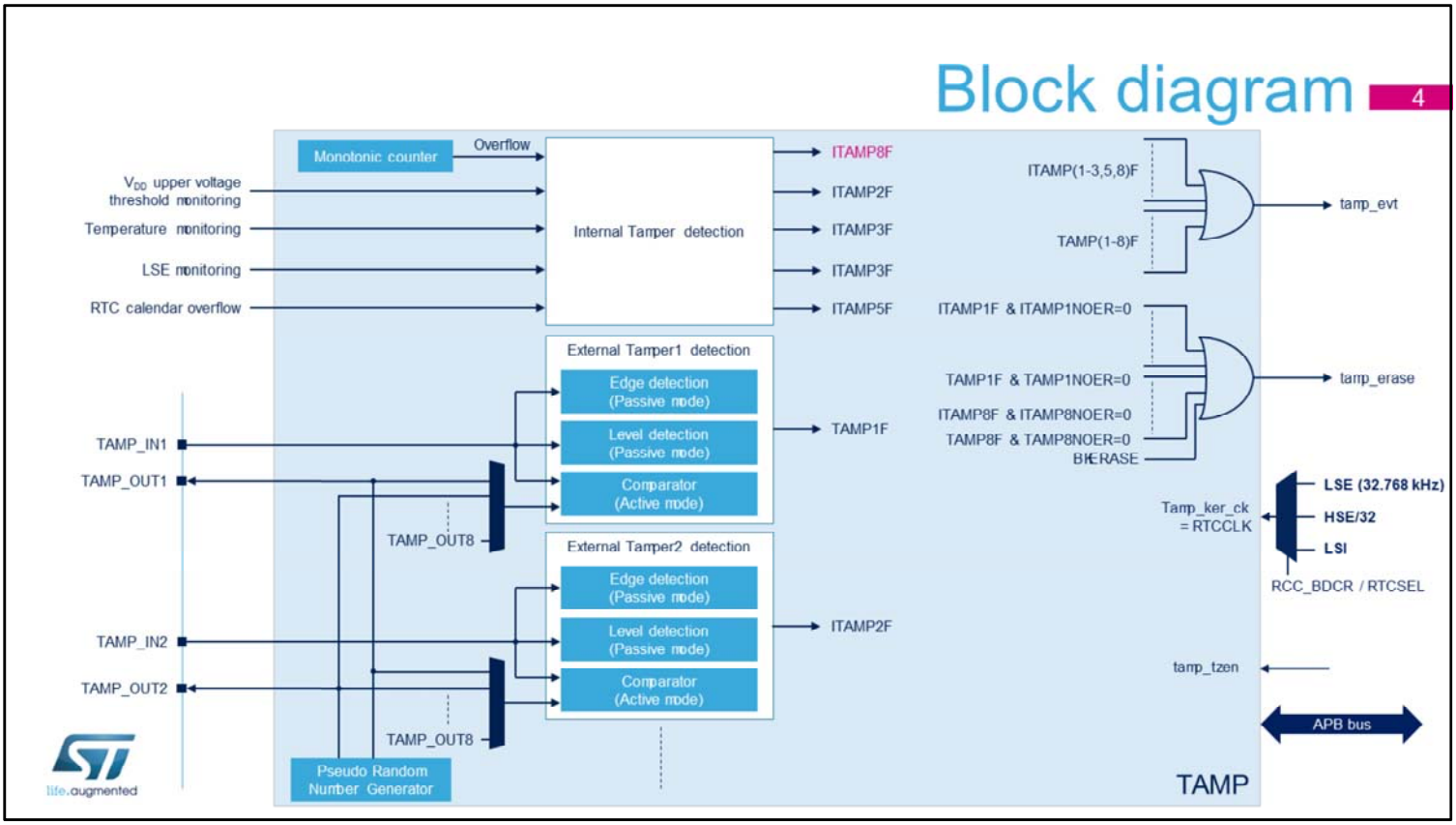
- Tamper-protected backup registers
- Ultra-low-power tamper detection with filtering

The TAMP peripheral features 32 32-bit backup registers used to preserve data when the main supply is off.
These backup registers can be used to store sensitive data, as they are erased when a tamper event is detected on the tamper pins or due to some internal events.
The SRAM2, the PKA SRAM and the instruction cache are also erased when a tamper event is detected.
The tamper detection is functional in low-power modes when the VBAT domain is supplied by a backup battery.
The anti-tamper circuitry includes ultra-low-power digital filtering, avoiding false tamper detections.



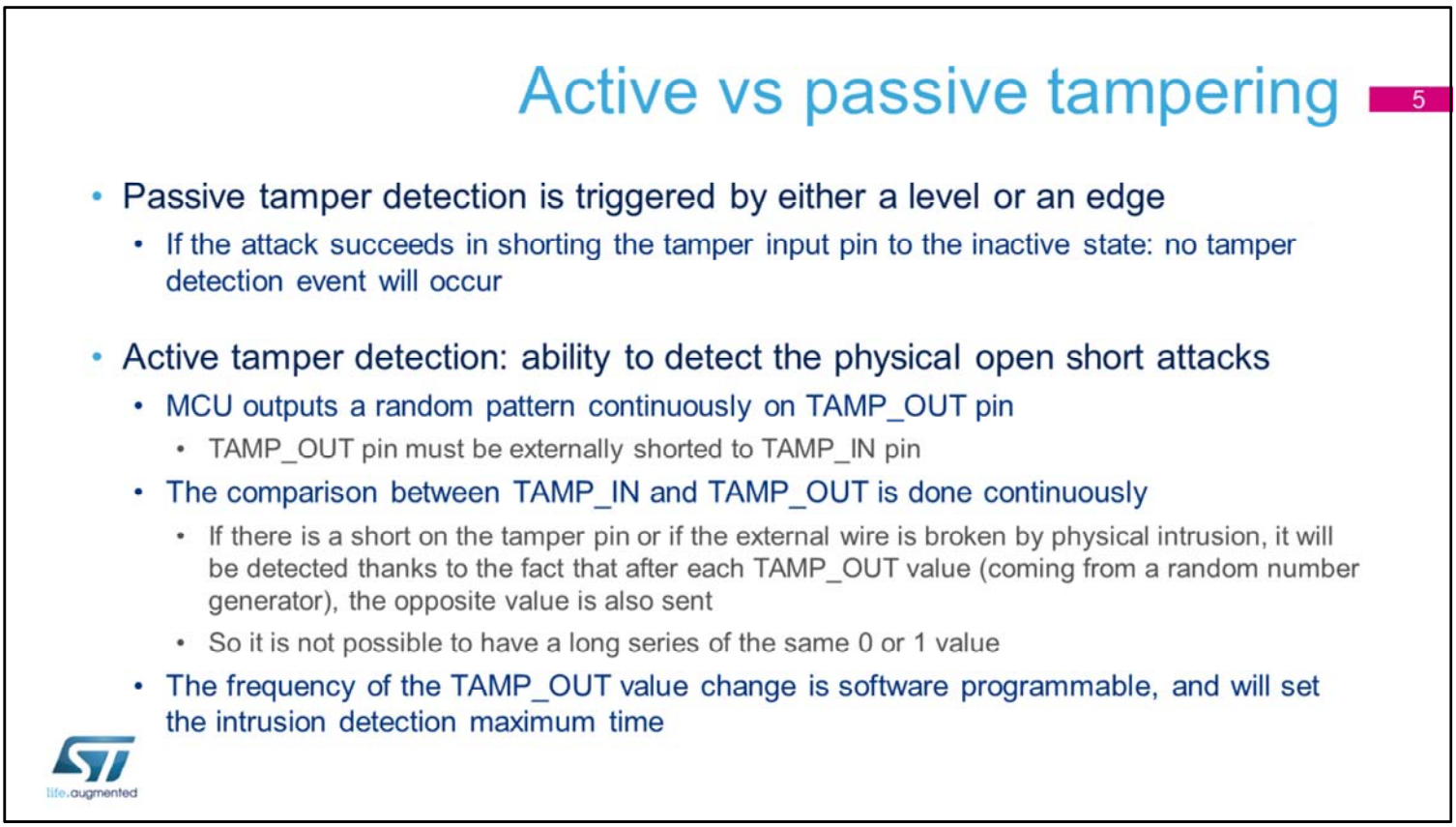
The key features of the TAMP are:
128 bytes of backup registers, split into 32 32-bit backup registers.
These registers are preserved in all low-power modes and in VBAT mode, and are erased when a tamper detection event occurs.
Three of the eight external tamper pins are available in VBAT mode.
External tampers can be configured in either passive or active mode.
The passive external tamper events can be detected on a programmable edge, or on level with a configurable filter and using an internal pull-up in an ultra-low power mode.
A timestamp function is used to save calendar contents in timestamp registers, depending on any tamper event.
Any tamper detection erases the backup registers,

SRAM2, Instruction cache, PKA SRAM and cryptographic peripherals.
The TAMP unit also includes a monotonic counter, generally used in protection against replay attacks.



Here is the TAMP block diagram.
Several internal features can generate a tamper event: VDD upper voltage threshold monitoring, temperature monitoring, LSE monitoring, RTC calendar overflow, and monotonic counter overflow.
Each internal and external tamper has an enable control bit. By default internal and external tampers are enabled.
By default, all tamper detection events will erase the backup registers, the SRAM2, the ICACHE, the PKA SRAM and the cryptographic peripherals.
Note that the backup registers are not reset by a system reset or when the device wakes up from Standby mode.
Backup registers can be reset when a tamper detection event occurs or when the readout protection of the flash is changed from level 1 to level 0.
The tamp_evt is used to generate a RTC timestamp event.

Temp_erase output is asserted following either tamper event detection (internal or external) or the software erase request done by writing BKERASE to 1.
The tamp_tzen input is used to activate TrustZone in the device.
The TAMP module has two clock sources: the TAMP clock (or RTCCLK), and the APB clock.
The TAMP clock can use either the high-speed external oscillator (HSE), divided by 32, 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 Shutdown and VBAT modes.



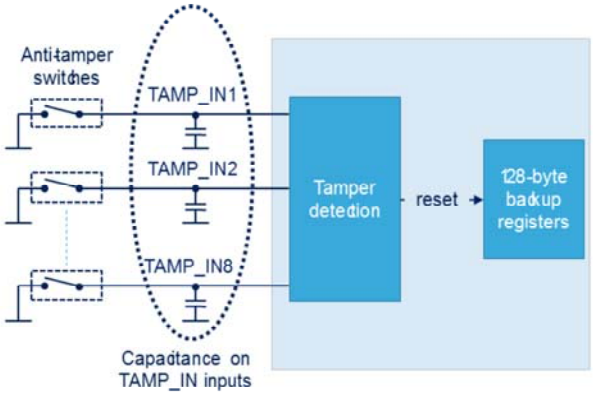
Passive tamper detection just checks a static level. It is typically used to connect a sensor and to detect a change of the sensor output: either a level- or edge-triggered detection. So if the attack succeeds in shorting the tamper input to the inactive state, no tamper detection event will occur.
Active tamper detection detects the physical open short attack.
A TAMP_OUT output pin provides a pseudo-random value. After outputting this value, the TAMP_OUT pin outputs its opposite value. A TAMP_OUT pin must be externally shorted to a TAMP_IN pin.
Tamper active mode is based on the continuous comparison between a TAMP_OUT pin and a TAMP_IN pin.
The same output can be used for several tamper inputs.
The pseudo-random generator must be initially and

periodically fed with a new seed

Tamper detection in passive mode

Ultra-low power anti-tamper circuitry

- 8 external tamper pins and events
  - 3 in the VBAT domain
- Selectable active edge or level for each event when configured in passive mode
- Reset of backup registers, SRAM2, PKA SRAM, ICACHE and cryptographic peripherals when an external tamper event is detected
  - May be disabled
- Tamper can generate a timestamp event and a hardware trigger for LP timers



The TAMP embeds ultra-low-power tamper detection circuitry.
The purpose is to detect physical tampering in a secure application, and to automatically erase sensitive data in case of intrusion.
8 tamper pins and events are supported, three of them are functional in all low-power modes and in VBAT mode.
The detection can be edge- or level-triggered, and the active edge or level is selectable for each event, when configured in passive mode.
A pre-charge time is determined by the TAMPPRECH bits, in order to support large capacitances on the TAMP_Inx inputs.
A tamper event can generate a timestamp event, which can be used to record the date of the intrusion attempt.
A tamper event can also be used as a trigger for LP timers.

The capacitors shown in the figure perform filtering.
If no external capacitors are explicitly connected to a Tamper input, they provide a model of the trace capacity.
Note that an external pull-up is required in Edge Detection mode.
In Level Detection mode, the internal pull-up is used, as explained in the next slides.

Tamper detection in passive mode

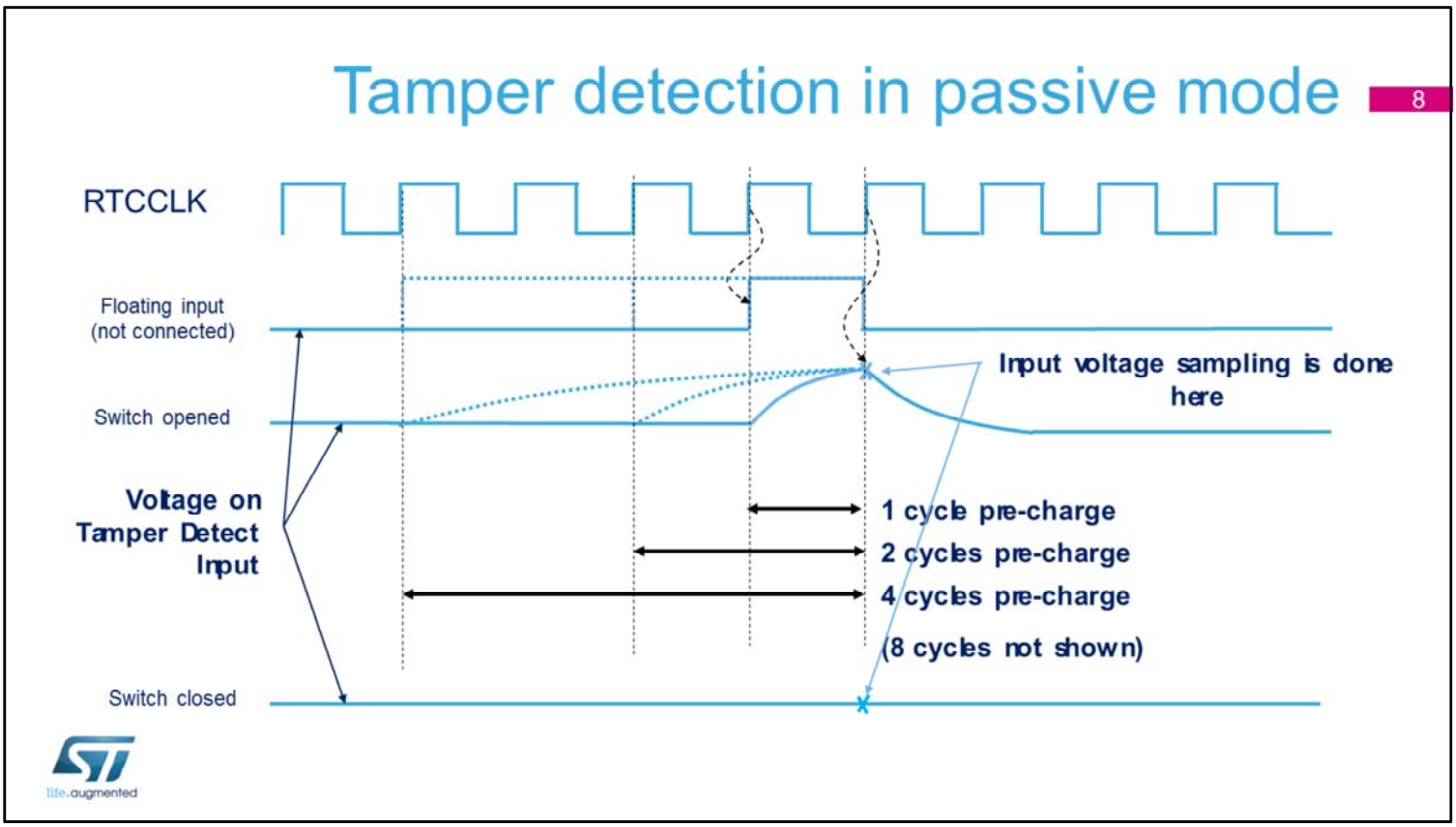
Safe and ultra-low-power tamper detection with filtering

- 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 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 microcontroller: 1, 2, 4, or 8

life.augmented

The tamper detection circuit includes an ultra-low power digital filter.
The internal I/O pull-up can be used to detect the anti-tamper switch 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 TAMP clock cycles.
The pin level is sampled at the end of the pre-charging pulse.
A filter can be applied to the tamper pins.
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 1, 2, 4 or 8

events, at a programmable sampling rate from 1 to 128 Hz.



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.

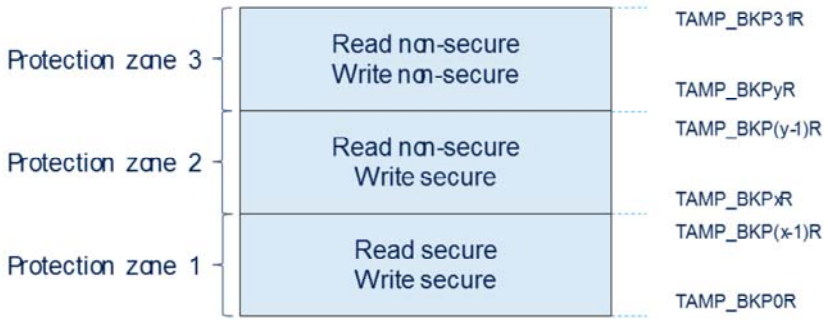
Tamper detection

- Tamper detection can generate interrupts or trigger events, and can benefit from digital filtering
  - Interrupts can be enabled/disabled for each event
  - Sensitive data erase is configurable for each external event
  - Hardware trigger to the low-power timer is configurable for each external event

The tamper detection circuitry can also be used to generate interrupts or trigger events.
Each tamper interrupt can be individually enabled or disabled.
Each external tamper event can be individually configured to erase the sensitive data or not.
Each external tamper event can be individually configured to generate a hardware trigger to low-power timer.
This takes advantage of the digital filtering present on these I/Os for interrupt or trigger generation.

TAMP secure protection modes

- When TrustZone® is enabled and the TAMPDPROT bit is cleared in the TAMP_SMCR register:
  - Writing the TAMP registers is possible only in secure mode, except for the backup registers which have their own protection setting
    - The 32 backup registers can be split into three protection zones



By default after a backup domain power-on reset, all TAMP registers can be read or written in both secure and non-secure modes, except for the TAMP secure mode control register (TAMP_SMCR) which can be written in secure mode only when TrustZone is enabled.
The TAMP protection configuration is not affected by a system reset.
When the TAMPDPROT bit is cleared in the TAMP_SMCR register, writing the TAMP registers is possible only in secure mode, except for the backup registers which have their own protection setting.
The 32 backup registers, representing 128 bytes, can be split into three protection zones:

- Protection zone 1 starts at backup register 0 and ends at backup register x-1. Access permissions are secure reads and writes.
- Protection zone 2 starts at backup register x and ends at backup register y-1. Access permissions are non-secure

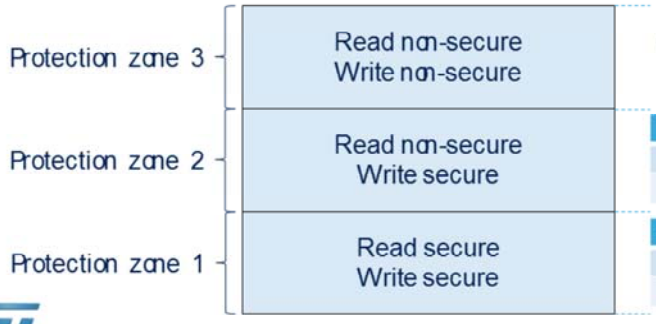
reads and secure writes.

- Protection zone 3 starts at backup register y and ends at backup register 31. Access permissions are non-secure reads and writes.

x and y are set in the BKPRWDPROT and BKPWDPROT fields of the TAMP_SMCR register.

TAMP privilege protection modes

- When the TAMPPRIV bit is set in the TAMP_PRIVCR register:
  - Writing the TAMP registers is possible only in privilege mode, except for the backup registers which have their own protection setting
    - The privileged attribute is programmable for Protection zones 1 and 2:



Non-privileged area

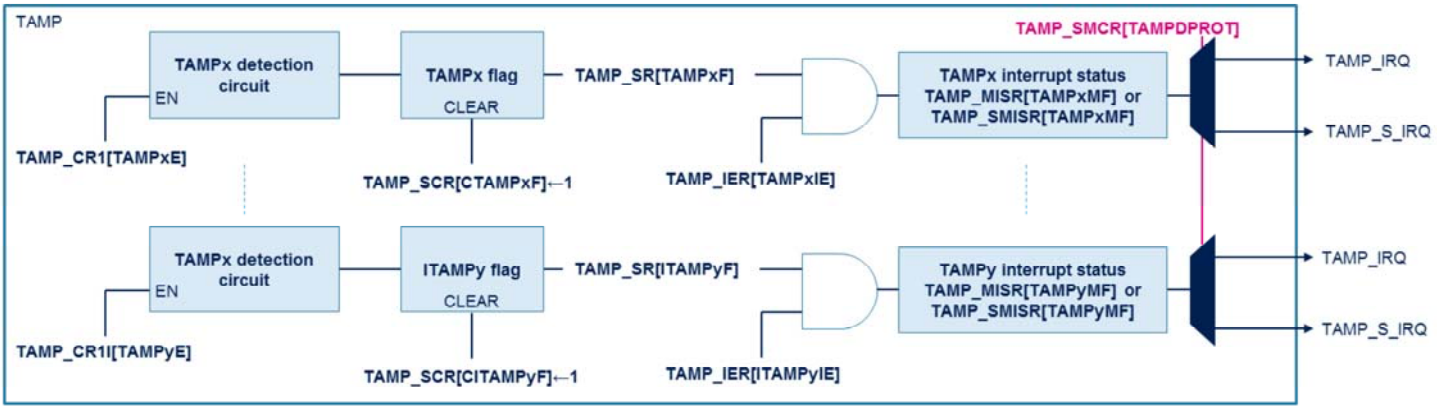
TAMP_PRIVCR[BKPWPRIV]	Backup registers zone 2 privilege protection
0	Privileged or nonprivileged mode
1	Privileged mode

TAMP_PRIVCR[BKPRWPRIV]	Backup registers zone 1 privilege protection
0	Privileged or nonprivileged mode
1	Privileged mode

life.augmented

By default after a backup domain power-on reset, all TAMP registers can be read or written in both privileged and non-privileged modes, except for the TAMP privilege mode control register (TAMP_PRIVCR) which can be written in privilege mode only.
The TAMP protection configuration is not affected by a system reset.
When the TAMPPRIV bit is set in the TAMP_PRIVCR register, writing the TAMP registers is possible only in privilege mode, except for the backup registers which have their own protection setting.
The BKPWPRIV bit in TAMP_PRIVCR register sets the privilege attribute of protection zone 2.
The BKPRWPRIV bit in TAMP_PRIVCR register sets the privilege attribute of protection zone 1.

Interrupt event	Description
TAMPx	Set when a tamper event is detected on TAMP_INx
ITAMPy	Set when an internal tamper event is detected on ITAMP_INy



All interrupts can wake the processor up from all low-power modes. The detection on all tamper pins and internal tamper sources can generate an interrupt.
Any tamper detection circuit can be enabled or disabled by programming the TAMP_CR1 register.
If it is enabled and a tamper event is detected, the corresponding flag is set in the TAMP_SR register.
Then TAMP_IER register masks or enables the tamper event interrupt.
The interrupt service routine can easily determine which tamper event has occurred by reading the TAMP_MISR or TAMP_SMISR register which contains flags identifying the source of the tamper event interrupt. MISR is relevant when the interrupt is non-secure, SMISR when it is secure.
The TAMPDPROT bit in the TAMP_SMCR register determines whether the TAMP module asserts the non-

secure or the secure interrupt request to the NVIC.

Low-power modes

Mode	Description
Run	Active
Sleep	Active ➢ TAMP interrupts cause the device to exit Sleep mode.
Low-power run	Active
Low-power sleep	Active ➢ TAMP interrupts cause the device to exit Low-power sleep mode
Stop 0/Stop 1/Stop 2	No effect on all features, except for level detection with filtering and active tamper modes which remain active only when the clock source is LSE or LSI ➢ TAMP interrupts cause the device to exit Stop 0/Stop 1/Stop 2 mode
Standby	No effect on all features, except for level detection with filtering and active tamper modes which remain active only when the clock source is LSE or LSI ➢ TAMP interrupts cause the device to exit Standby mode
Shutdown	No effect on all features, except for level detection with filtering and active tamper modes which remain active only when the clock source is LSE ➢ TAMP interrupts cause the device to exit Shutdown mode

life.augmented

The TAMP peripheral is active in all low-power modes and the TAMP interrupts cause the device to exit the low-power mode.
In Stop 0, Stop 1, Stop 2 and Standby modes, only the LSE or LSI clocks can be used to clock the TAMP.
Only the LSE is functional in Shutdown mode.

Related peripherals

14

- Refer to these peripheral trainings linked to the TAMP
  - Real-time clock (RTC)
  - Reset and clock control (RCC)
  - Nested vectored interrupt controller (NVIC)

life.augmented

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

- Real-time clock,
- Reset and clock control,
- Nested vectored interrupt controller.