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.

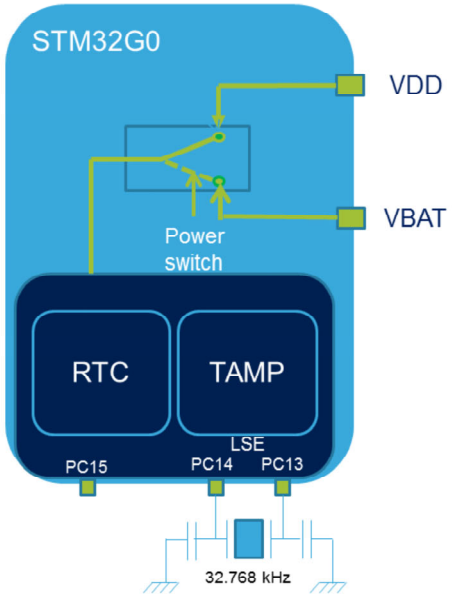
Main differences with STM32F0

- The main differences with STM32F0 microcontrollers is the introduction of the internal Tamper channel
- Separation of TAMP and RTC blocks, Backup registers are still part of the TAMP block

life.augmented

In the STM32G0, two separate units are present, tamper detection peripheral (TAMP) and real-time clock (RTC). Backup registers are contained in the TAMP block.
In the STM32F0, a unique block is in charge of both tamper and RTC units.

Overview



- The TAMP features 5 backup registers, erased on tamper detection
- Two types of tamper input: external (2 GPIOs) and internal (4 sources)
- 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

life.augmented

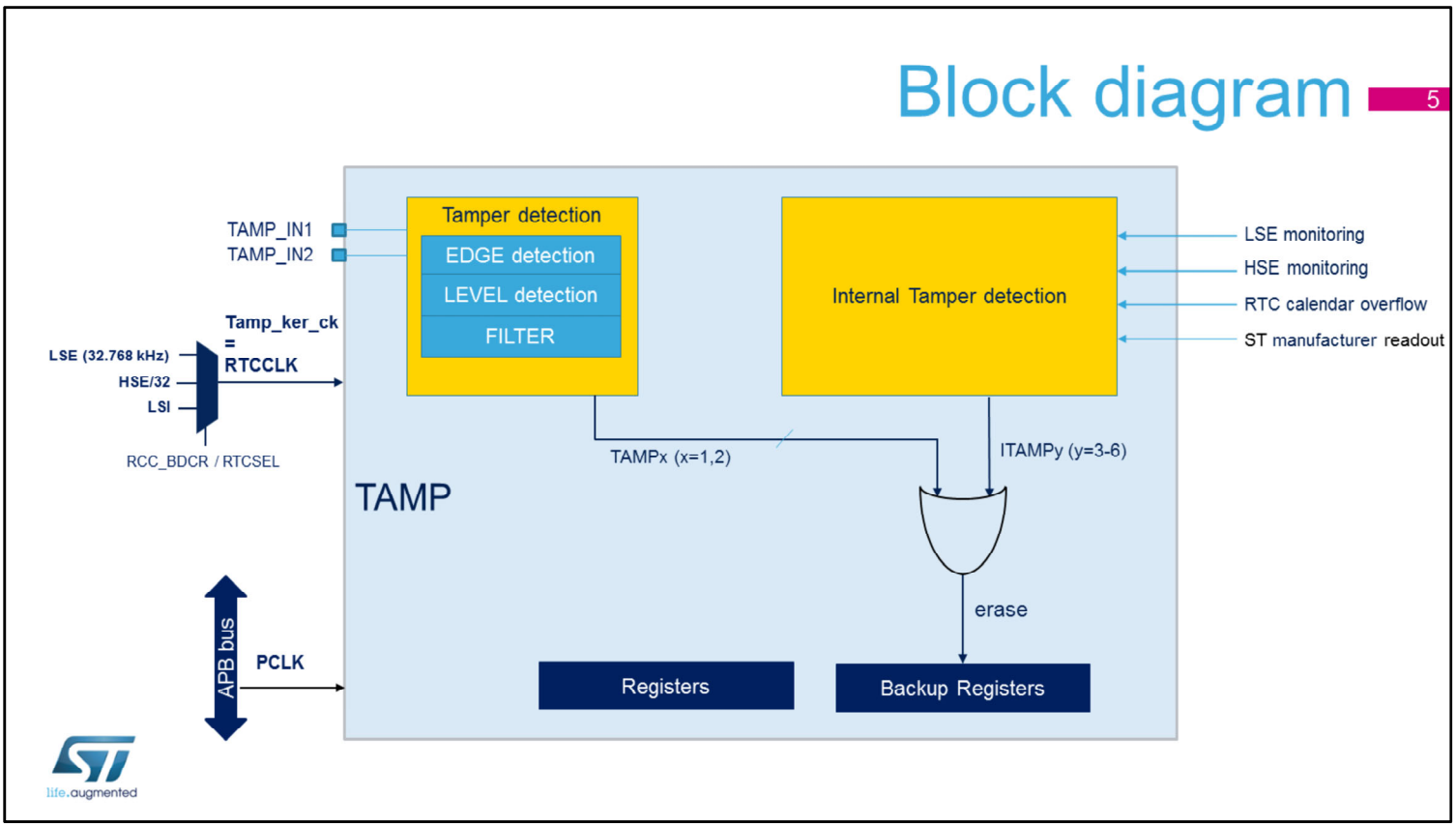
The TAMP peripheral features five 32-bit backup registers used to preserve data when the main supply is off. These backup registers can be used to store secure data, as they are erased when a tamper event is detected on the tamper pins or on some internal events. The tamper detection is functional in 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.

Key features

- 5 backup registers:
  - The backup registers (TAMP_BKP0-4R) are implemented in the battery backup domain that remains powered-on by VBAT when the VDD power is switched off
- 2 external tamper detection events
  - External passive tampers with configurable filter and internal pull-up
- 4 internal tamper events
- Any tamper detection can generate an RTC timestamp event.
- Any internal tamper detection erases the backup registers
  - Regarding external tamper, erasure can be disabled

life.augmented

The key features of the TAMP are:
20 bytes of backup registers, split into five 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 two tamper pins, or the 4 internal tamper events. Regarding external tamper events, software can select whether backup registers are erased when the tamper event is detected.
The 2 tamper pins are available in VBAT mode.
The 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.



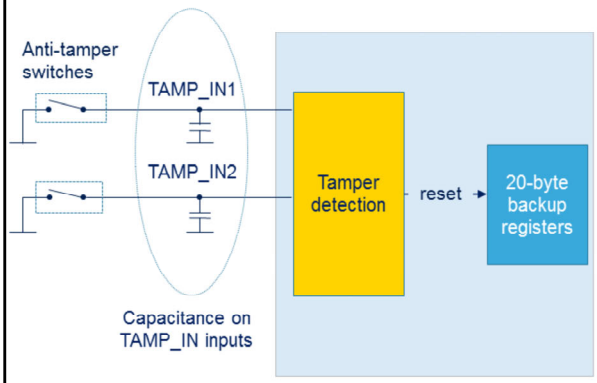
Here is the TAMP block diagram. The TAMP has two clock sources: the TAMP clock (RTCCLK) is only used for the tamper detection in Level Detection mode with filtering, and the APB clock is used for TAMP and backup registers read and write accesses. Tamper edge detection or internal tamper detection do not need any 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.

Several internal features can generate a tamper event: LSE monitoring, HSE monitoring, RTC calendar overflow, and ST manufacturer readout.

By default, all tamper detection events will erase the backup registers.

Tamper detection

Ultra-low power anti-tamper circuitry



- 2 tamper pins and events, available in VBAT mode
- Configurable active edge or level for each event
- Reset of backup registers when an external tamper event is detected
  - May be disabled
- Tamper can generate a timestamp event

life.augmented

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.
2 tamper pins and events are supported, and 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 configurable for each event.
A precharge time is determined by the TAMPRECH 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.
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

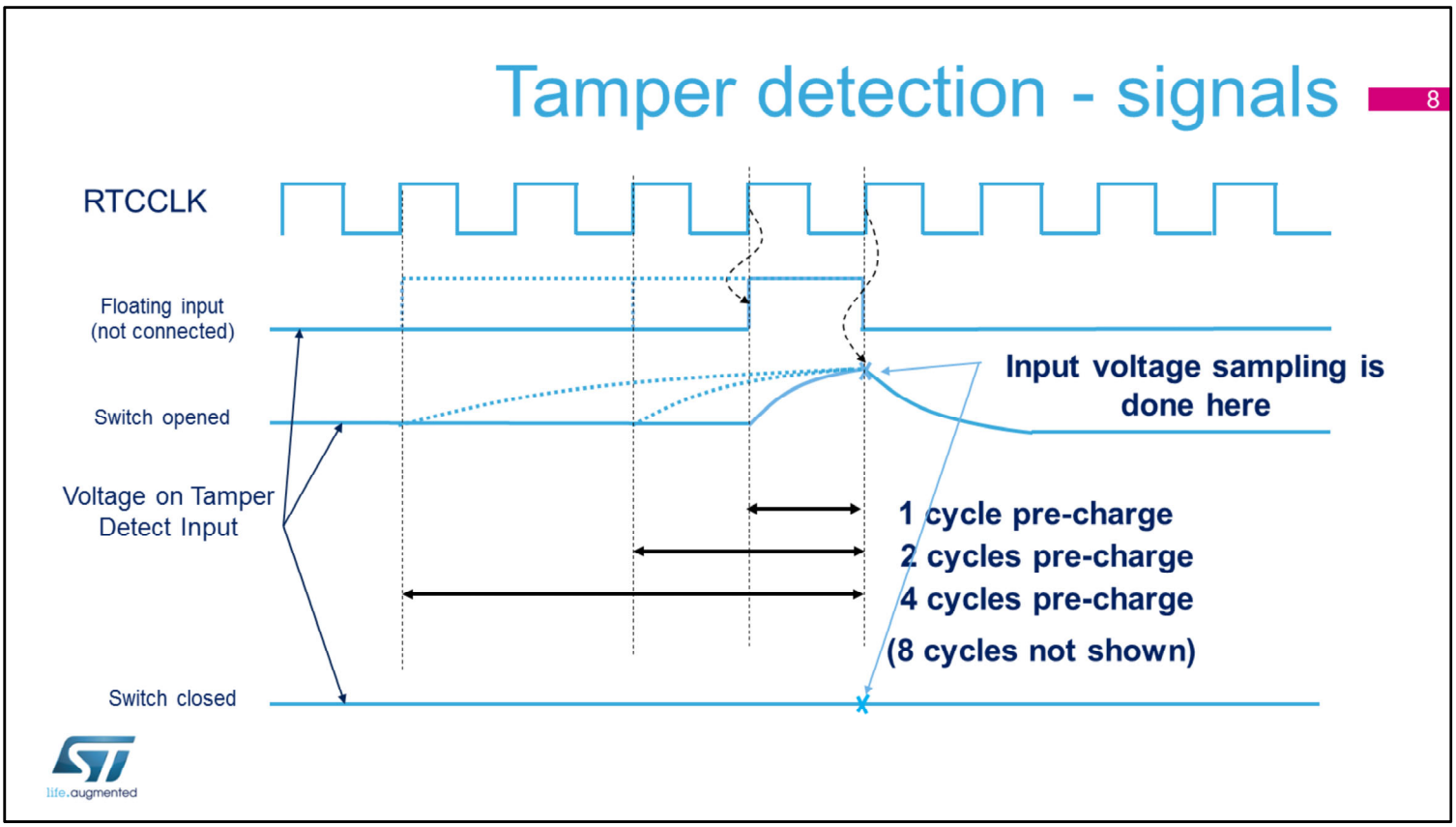
7

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 MCU: 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

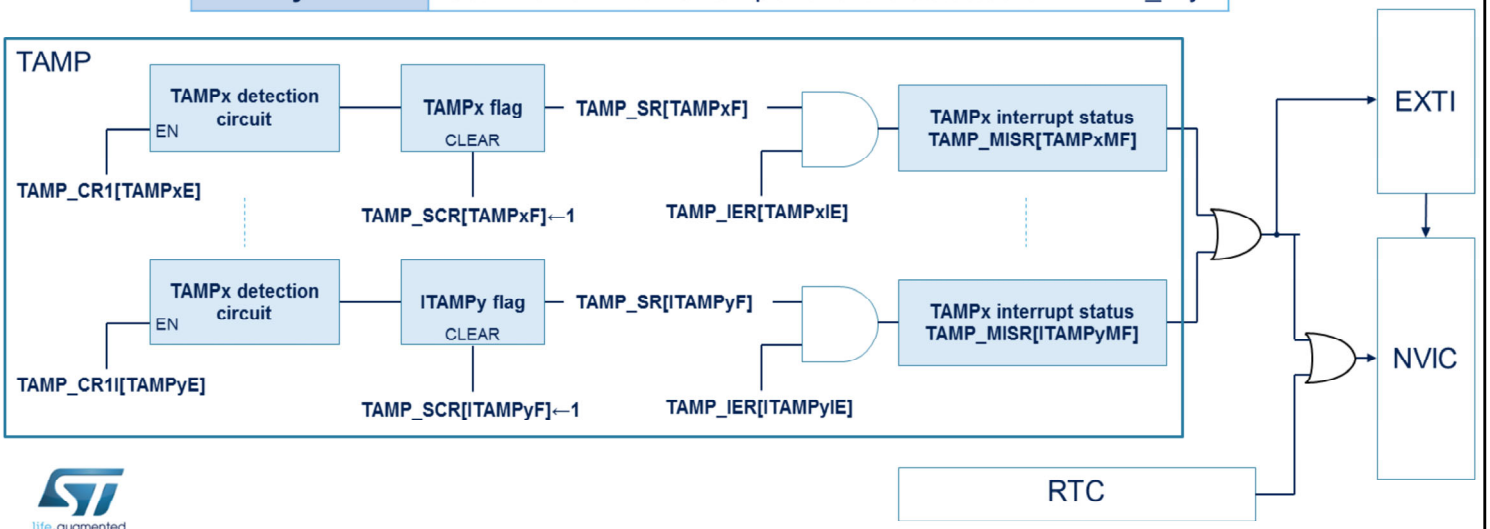
- Tamper detection can generate interrupts or trigger events, and can benefit from digital filtering
  - Interrupts can be enabled/disabled for each event
  - Backup registers erase is configurable for each external event
  - Hardware trigger to the low-power timers is configurable for each external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

life.augmented

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 backup registers or not. Each external tamper event can be individually configured to generate a hardware trigger to low-power timers. This takes advantage of the digital filtering present on these I/Os for interrupt or trigger generation.

Interrupts

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 register which contains flags identifying the source of the tamper event interrupt.
The nested vectored interrupt controller (NVIC) has a unique input related to RTC and TAMP modules.
The output of the OR gate combining all tamper interrupt requests is also connected to the extended interrupt

controller (EXTI) as a direct line type, which is required to generate a CPU event wakeup signal or request a system and core wakeup.

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	Level detection with filtering is active only when clocked by LSE or LSI. TAMP interrupts cause the device to exit Stop 0/Stop 1 mode.
Standby	Level detection with filtering is active only when clocked by LSE or LSI. TAMP interrupts cause the device to exit Standby mode.
Shutdown	Level detection with filtering is active only when clocked by 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, 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

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

life.augmented

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

- Real-time clock
- Reset and clock control
- Power control
- Extended interrupt controller
- Nested vectored interrupt controller