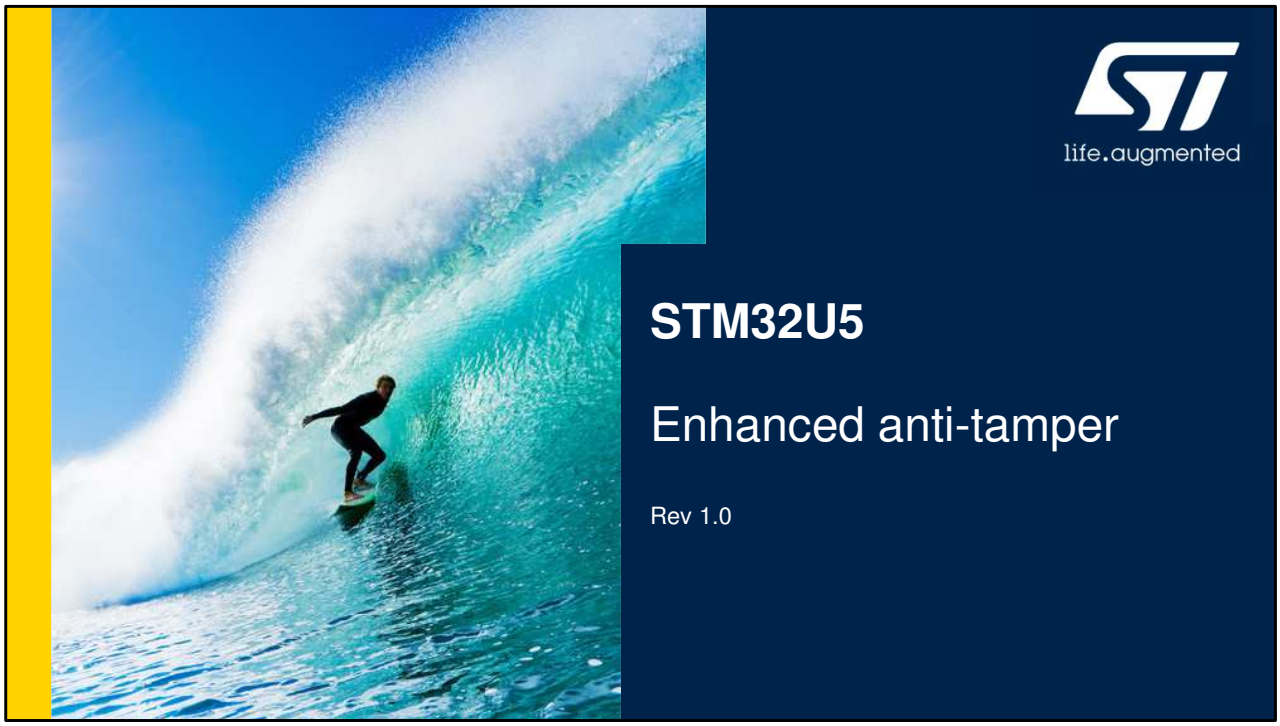
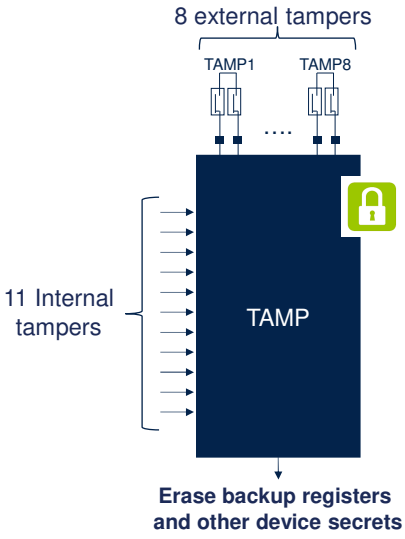


Hello, and welcome to this presentation of the STM32U5 enhanced anti-tamper detection unit. It covers the main features of this peripheral, which is used to provide security against tamper events.

Tamper overview



- 128 bytes of backup registers, retained in all low-power modes and VBAT, erased on tamper detection
- 8 external tamper events, active or passive
- 11 internal monitoring tamper events
- Monotonic counter
- Fully securable with TrustZone and privilege access filtering, 3 protection zones in backup registers

Application benefits

- Protection against physical attacks robustness with active tampers allowing short or open detection
- Protection against environmental perturbation attacks
- Anti-rollback protection with monotonic counter
- Configurable frequency for fast detection time/low-power compromise

life.augmented

2

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 by some internal events.
The SRAM2, the backup SRAM, the caches and cryptographic peripherals are also erased when a tamper event is detected.
The STM32U5 features 8 external tamper events, configurable in active or passive mode, and 11 internal monitoring tamper events.
The TAMP unit also includes a monotonic counter, generally used in protection against replay attacks.
Backup registers are split into 3 configurable-size areas in

order to implement different secure access permissions.
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 trade-off between tamper detection latency and power consumption can be optimized by selecting the frequency of the sampling for level detection on tamper inputs.

Tamper detection effects

- Immediate erasure of backup registers
- AES & SAES & HASH registers erasure, OTFDEC keys erasure, and encrypted regions read as zero, RHUK (Root hardware unique key in Flash) and SRAMs access blocked until complete SRAM erasure
- 2 KB backup SRAM erasure (depending on configuration bit) when VDD is present**
- 64 kB SRAM2 erasure when VDD is present**
- PKA SRAM erasure when VDD is present**

**If VDD is not present (VBAT mode), the erase occurs at next VDD power on.

NEW: a control bit allows to block the R/W access to all these secrets

life.augmented

3

The effects of a tamper detection are listed hereafter:
- Immediate erasure of backup registers
- Sensitive information present in cryptographic units erasure.

When VDD is present, the contents of the following RAMs are erased:
- Backup SRAM
- SRAM2
- PKA SRAM.

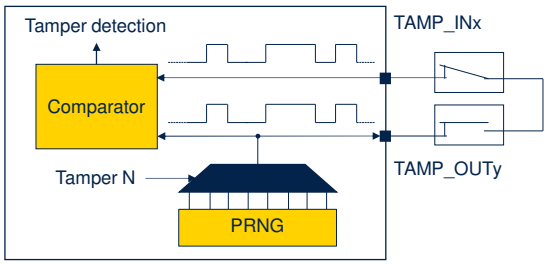
When the microcontroller is in VBAT mode, the erasure occurs at the next VDD power on.
The device secrets access is blocked when erasure is ongoing.
The bus between the flash memory and the secure AES

unit, used to transfer the root hardware unique key or RHUK, is blocked.
Software can disable the access to backup registers and device secrets by setting the BKBLOCK control bit. This is a new feature of the STM32U5 with respect to STM32L5.

Tampers list

Protection against physical attacks

- 8 tamper I/Os, available in all low power modes and in VBAT mode
  - 8 TAMP_IN, 8 TAMP_OUT
  - 4 independent meshes, up to 7 meshes if one output used for several inputs
  - Programmable detection time
  - Digital filtering:
    - 2 false comparisons, in 4 consecutive comparison samples



life.augmented

4

Active tamper detection detects physical open short attacks.
TAMP_OUT output pin provides a value received from the pseudo random number generator. After outputting this value, the TAMP_OUT pin outputs its opposite value. The TAMP_OUT pin must be externally shorted to the TAMP_IN pin.
Tamper active mode is based on a comparison between a TAMP_OUT pin and a TAMP_IN pin, which is done continuously.
The STM32U5 implements a flexible active tamper I/O management: from 4 meshes (each input associated to its own exclusive output) to 7 meshes (single output shared for up to 7 tamper inputs).

Detection time is programmable, and digital filtering is available: tamper triggered after two false comparison in four consecutive comparisons samples.
The pseudo-random generator must be initially and periodically fed with a new seed.

Internal tampers

Protection against transient or environmental perturbation attacks

LSE monitoring, functional in VBAT mode

- LSE missing or over frequency detection (> 2MHz)
- Glitch filter (> 2 MHz)

Temperature monitoring, functional in VBAT mode

Low temperature tamper detection	High temperature tamper detection
-39°C to -33°C	121°C to 128°C

Backup domain voltage continuous monitoring, functional in VBAT mode

VBAT Low voltage tamper detection	Backup domain High voltage tamper detection
1.58V*	3.5V to 3.6V

*Backup domain brown out reset generation

life.augmented

5

The 11 internal tamper events protect against transient or environmental perturbation attacks.
This slide and the following one detail these internal tampers.
First the clock security system that monitors the LSE oscillator can cause a tamper event.
Abnormal temperature and backup domain voltage conditions are also detected.

Internal tampers

Voltage monitoring through ADC analog watchdogs
Monitors VCORE, VREF+, down to Stop 2 mode

RTC calendar overflow

JTAG/SWD access when RDP > 0

Monotonic counter overflow
Counter incremented at any write, limits the number of routine executions

Crypto IPs fault generation

life.augmented

ADC4 integrated watchdogs can assert a tamper event. They can be used to monitor internal voltages, such as VCORE and VREF+, down to stop 2 mode, because the ADC4 belongs to the SmartRun domain.
The other sources of internal tampers are:

- An overflow of the RTC calendar
- A debug access, either through JTAG or the SWD port, when Readout Protection level is strictly larger than 0
- Monotonic counter overflow
- Cryptographic peripherals faults (SAES, AES, PKA or TRNG).

Software filtering mechanism

Capability to configure each tamper source not to launch immediate erase

- When a tamper flag is raised, all secret accesses are blocked until all tamper flags are cleared:
  - RHUK : tied to 0
  - Backup registers, backup SRAM, SRAM2 : read-as-zero, write-ignored
  - AES, SAES, HASH : IP reset
- After software filtering :
  - Either launch the erasure of secrets with a software command (confirmed tamper)
  - Or just clear the flags to release secrets blocking (false tamper)
- Timeout mechanism to force erasure
  - Launched by IWDG reset when a tamper flag is already set

life.augmented

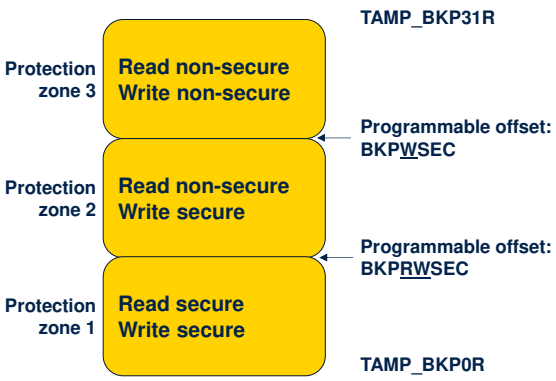
7

Each tamper source can be configured not to launch an immediate erasure.
In such situation, when the tamper flag is raised, access to secrets is blocked until all tamper flags are cleared.
Once the application, notified by the tamper event, analyzes the situation, there are two possible cases:

- Either the application launches the erasure of secrets erase with a software command, in the case of a confirmed tamper
- Or the application just clears the flags to release secrets blocking, in the case of a false tamper.

If the tamper software fails to react to such a tamper flag, an IWDG reset automatically triggers the erasure of secrets.

Backup register protection zones



- 3 security protection zones, combined with privilege protection:
  - The protection zone 1 can be protected against non-privilege read and write access if BKPRWPRIV=1
  - The protection zone 2 can be protected against non-privilege write access if BKPWPRIV=1
- Tamper configuration can be protected against non-secure read and write accesses (TAMPSEC=1) or against non-privileged read and write accesses (TAMPPRIV=1)

life.augmented

8

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.

Tamper configuration can be protected against non-secure

read and write accesses (TAMPSEC=1) or against non-privileged read and write accesses (TAMPPRIV=1).

Boot hardware key (BHK)

TAMP_BKP[7:0]R used to store a 256-bit boot hardware key for SAES

- BKPRWSEC must be greater or equal to 8 to include BHK in protection zone 1
- Once TAMP_SECCFGR.BHKLOCK = 1
  - BHK software access forbidden
  - BHKLOCK cleared only by hardware with tamper event or RDP regression
  - HW bus directly connected to SAES

life.augmented

9

The first eight backup registers from TAMP_BKP0R to TAMP_BKP7R can be used to store a boot hardware key for the secure AES.
These registers must belong to the Protection Zone 1: BKPRWSEC must be greater or equal to 8.
Once the backup registers are written with the boot hardware key, the BHKLOCK bit must be set in the TAMP_SECCFGR register.
Once BHKLOCK is set, the 8 backup registers cannot be accessed anymore by software.
BHKLOCK cannot be cleared by software, and is cleared by hardware following a tamper event or when the readout protection (RDP) is disabled
In both cases the backup registers are also erased.

A dedicated bus is used to load the boot hardware key in the secure AES co-processor.

Thank you

life.augmented

This is a list of peripherals related to the enhanced anti-tamper detection circuit. Please refer to these peripheral presentations for more information if needed.

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