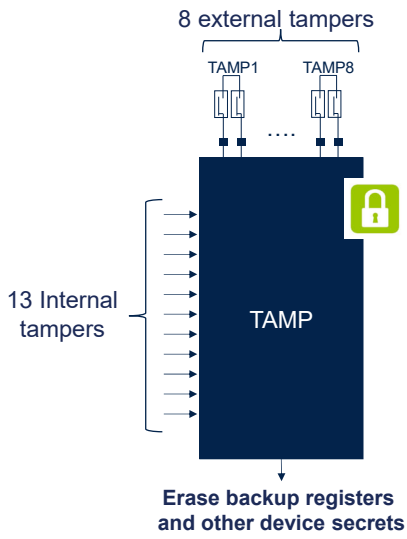
Hello, and welcome to this presentation of the STM32MP13 enhanced anti-tamper detection unit. It covers the main features of this peripheral, which is used to provide security against tamper events.

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
- 13 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 on some internal events.
The SRAM3, optionally the backup SRAM, and cryptographic peripherals are also erased when a tamper event is detected.
The STM32MP13 features 8 external tamper events, configurable in active or passive mode, and 13 internal monitoring tamper events. Passive tampers are detected on input edges or levels. Active tamper provides increased protection against open/short attacks.
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 and privilege access permissions.
Tamper detection is functional in all low-power modes and in VBAT mode. VBAT mode is when the main VDD supply is OFF, and the backup domain is supplied by a backup battery on VBAT pin.
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 sampling for level detection on tamper inputs.

Confirmed tamper detection effects

By default, all tampers are configured to erase sensitive data (confirmed tamper mode)

- Immediate erase of backup registers
- CRYP & SAES & HASH registers erase, PKA SRAM erase, RHUK (Root hardware unique key in BSEC) and SRAMs access blocked until complete SRAM erase
- SRAM3 erase
- Backup SRAM erase (depending on configuration bit)

A control bit allows blocking of R/W access to all these secrets

life.augmented

3

By default, each tamper source is configured to operate as a “confirmed tamper”. The effects of confirmed tamper detection are as follows:

- The backup registers are immediately erased.
- The sensitive information present in cryptographic units is erased : cryptographic IPs registers are reset, and PKA SRAM is erased.
- The SRAM3 is erased.
- Depending on software configuration, the backup SRAM is also erased or not.

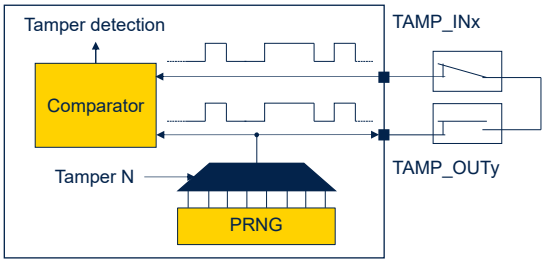
Device secrets access is blocked when erase is ongoing. The bus between the BSEC and the secure AES unit, used to transfer the root hardware unique key or RHUK, is blocked.

The software can disable access to backup registers and device secrets by setting the BKBLOCK control bit.

Active Tampers

Protection against physical attacks

- 12 tamper I/Os, available in all low power modes and in VBAT modes
  - 8 TAMP_IN, 5 TAMP_OUT
  - 5 independent meshes, up to 8 meshes if one output used for several inputs
  - Programmable detection time
  - Digital filtering:
    - 2 comparisons false, in 4 consecutive comparison samples
    - Minimum filtered pulse width: from 30µs to 62.5 ms



life.augmented

4

Active tamper detection detects the physical open short attack and is functional in VBAT mode.
The 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.
TAMP_OUT pin must be externally shortened to TAMP_IN pin.
Tamper active mode is based on a comparison between a TAMP_OUT pin and a TAMP_IN pin, which occurs continuously at a configurable sampling frequency.
The STM32MP13 implements flexible active tamper I/O management: from 5 meshes (each input associated to its own exclusive output) to 8 meshes (single output shared for up to 8 tamper inputs).

Detection time is programmable, and digital filtering is available: tamper triggered after two false comparisons in four consecutive comparison samples. The minimum filtered pulse width is programmable from 30µs to 62.5 ms. In order to ensure TAMP_OUT signal randomness, 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
  - Glitch filter
- HSE monitoring (CSS or over frequency detection)
- Temperature monitoring, functional in VBAT mode
- Backup domain voltage continuous monitoring, functional in VBAT mode

life.augmented

5

The 13 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. The clock security system that monitors the HSE, with an additional over frequency detector, can also cause a tamper.
Out of range temperature and backup domain voltage conditions are also detected.
All these monitors, except HSE monitoring, are functional in VBAT mode.

Internal tampers

Three voltage monitoring through ADC analog watchdogs

RTC calendar overflow

JTAG/SWD access

Two monotonic counters overflow

Counter incremented at any write, limits the number of routine execution

Crypto IPs fault generation

life.augmented

6

ADC2 integrates three watchdogs that can assert a tamper event. They can be used to monitor supply voltages.
The other sources of internal tampers are:

- An overflow of the RTC calendar
- A debug access, either through JTAG or SWD port
- Two monotonic counter overflow. These counters are incremented at any write, which can be used to limit the number of routine execution.
- Cryptographic peripherals faults (SAES, CRYP, PKA or TRNG).

Software filtering mechanism

Capability to configure each tamper source not to launch secrets erase

- When a tamper flag is raised in this mode, all secrets access is blocked until the tamper flag is cleared:
  - RHUK : tied to 0
  - Backup registers, SRAM3, PKA SRAM and optionally backup SRAM: read-as-zero, write-ignored
  - AES, SAES, HASH: IP reset
- After software filtering:
  - Either launch secrets erase with software command (confirmed tamper)
  - Or just clears the flags to release secrets blocking (false tamper)
- Timeout mechanism to force erase
  - Launched by IWDG reset while a tamper flag is already set

life.augmented

7

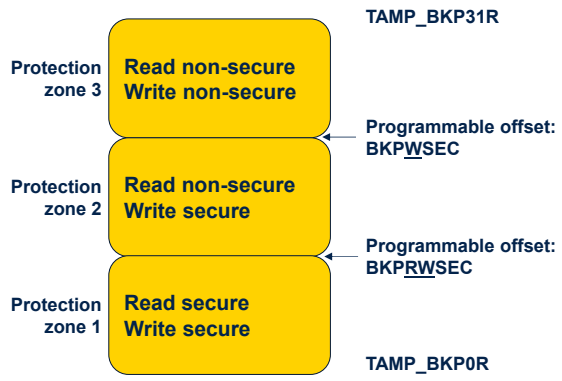
Each tamper source can be individually configured to operate as a “potential tamper”, so as not to launch secrets erasure.
In such situation, when the tamper flag is raised, access to secrets is blocked until the tamper flag is cleared by software.
Once the application, notified by the tamper event, analyzes the situation, there are two possible cases:

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

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

secrets.

Backup registers 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. This protection zone can be protected or not against unprivileged access.
- Protection zone 2 starts at backup register x and ends at backup register y-1. Access permissions are non-secure reads and secure writes. This protection zone can be protected or not against unprivileged write access.
- 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_SECCFGR 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
  - 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.
For this purpose, these registers must belong to 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 can no longer be accessed by software.
BHKLOCK cannot be cleared by software and is cleared by hardware following a tamper event. In this case, the backup registers are also erased.
A dedicated hardware bus is used to load the boot

hardware key in the secure AES co-processor.

Thank you

© STMicroelectronics - All rights reserved.
The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.

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.