7.8.6 TAMPC — Tamper controller

The tamper controller peripheral handles input from internal and external physical attack detectors and controls the device response.

The following figure shows an overview of the TAMPC detectors, input, and output.

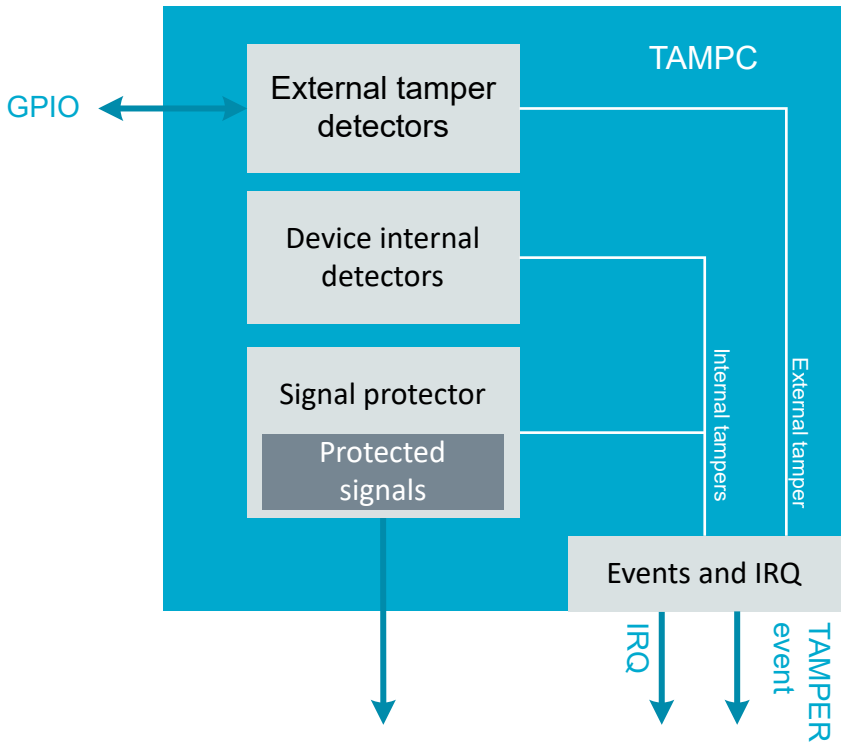

Figure 35: TAMPC overview

TAMPC implements the following physical security features:

- Detection of external tampering attacks
  - Detector supporting an active driven shield mounted on a PCB that is on top of a device
- Detection of fault injection attacks (voltage glitching, electromagnetic fault injection, etc.)
  - Signal protector to guard critical configuration signals
  - Glitch detectors to detect timing violations of internal logic
  - Built-in self-check for correctness inside the CRACEN

The tamper detectors are divided into two categories: external and internal. The external detectors rely on external stimuli through dedicated GPIO pins, and the internal detectors rely on internal signals not exposed outside the device package.

External tamper detectors

A tamper attack detected by any of the external tamper detectors indicates that a break-in attack is ongoing. This could include breaking the product encapsulation. This is detected through the external active shield detectors.

Internal tamper detectors

A tamper attack detected by any of the internal tamper detectors indicates that the device's internal logic could be affected by the attack, and the system state could be compromised. The default system reaction from reset is to trigger a system wide reset if any of the internal tamper detectors senses a tamper attack.