7.8.6.1 Active shield

TAMPC supports an active shield to protect against physical access to the device and its connections on the PCB level.

The active shield detector is enabled using the register PROTECT.ACTIVESHIELD.CTRL on page 205. The active shield detector has a number of channels. Depending on its configuration, TAMPC will react when a channel in the active shield is broken, meaning there is a mismatch between the input and output signal of an enabled channel in the active shield. A broken channel detected in the active shield causes one of the following to occur:

- A TAMPC event is generated.
- A chip reset is triggered and the `SECTAMPER` value in the reset reason register indicates what happened, depending on the status of the register PROTECT.EXTRESETEN.CTRL on page 209.

A channel in the active shield detector consists of a signal propagating from an output pin to an input pin. The channels are enabled using the CH[i] fields in the register ACTIVESHIELD.CHEN on page 200. The GPIO pins reserved for the active shield detector channels must be configured before the channels are ready for use. Pin direction and CTRLSEL must be set according to the register interface in the GPIO peripheral. For more information about reserved active shield detector pins, see Pin assignments on page 859. Pins reserved for the active shield detector can be used as generic GPIO pins when the channel is unused.

The active shield detector contains a Pseudo-Random Bit Sequence (PRBS) generator. A PRBS signal is generated on an output pin at each rising edge of the 32 KHz clock. The signal is routed through an external shield to an input pin. The signal on the input pin is sampled on the falling edge of the 32KHz clock. If the sampled signal does not match the transmitted signal, a channel in the external shield is assumed broken and a tamper event is generated.

7.8.6.2 CRACEN tamper detector

The cryptographic accelerator engine (CRACEN) implements a separate tamper detector mechanism. This tamper detector is always enabled.

CRACEN has security countermeasures and notifies TAMPC if tampering is detected during its operations. TAMPC will react according to the register setting in PROTECT.CRACENTAMP.CTRL and one of the following will occur:

- A TAMPC event is generated.
- A chip reset is triggered and the `SECTAMPER` value in the reset reason register indicates what happened, depending on the status of the register PROTECT.INTRESETEN.CTRL on page 210.

The internal tamper reset enable signal INTRESETEN is enabled from reset.

For more information about CRACEN countermeasures, see CRACEN — Cryptographic accelerator engine on page 133.

7.8.6.3 Glitch detector

The device implements general detectors to prevent fault injection attacks.

Detectors are strategically placed among the digital logic to detect local timing glitches (timing violations). The glitch detectors monitor the effects of attempted fault injection attacks and not the attack attempt itself. For example, fault injection attempts could be utilizing voltage glitches on supply or decoupling pins, or electro magnetic fault injection (EMFI) techniques. The detectors are designed and tuned to be more sensitive to timing violations than normal logic, enabling the digital logic to react before an injected fault is propagated through the system.

The glitch detectors are enabled from reset and can be disabled for debugging using the registers PROTECT.GLITCHSLOWDOMAIN.CTRL on page 207 and PROTECT.GLITCHFASTDOMAIN.CTRL on page 208.