7.6.5 GRTC

GRTC is implemented with split security, meaning it handles access from both secure and non-secure code. Individual GRTC SYSCOUNTER compare/capture channels and interrupts can have independent security settings that define them as secure or non-secure.

SYSCOUNTER compare/capture channels

The SYSCOUNTER compare/capture channels have the following security:

- Secure — The channel and its associated registers, trigger/subscribe tasks, and receive/publish events can only be accessed by secure code.
- Non-secure — The channel and its associated registers, trigger/subscribe tasks, and receive/publish events can be accessed by secure and non-secure code.

GRTC interrupts

GRTC interrupts can be defined as secure or non-secure.

A security fault is triggered when an invalid access targets registers INTEN/INTENSET/INTENCLR/INTPEND associated with an GRTC interrupt.

GRTC interrupt can only be generated by a COMPARE[j] event if the interrupt and channel have the correct security attribute.

A secure GRTC interrupt can be triggered by a secure or non-secure GRTC channel.

A non-secure GRTC interrupt can be triggered by an event generated by non-secure GRTC channel. An event generated by secure GRTC channel cannot trigger the interrupt.

7.7 Physical security

The device has countermeasures for physical attacks. It can detect and report fault injection attacks such as voltage glitching or electromagnetic fault injection.

The external active shield I/O interface is provided to facilitate PCB and product level security. It can detect if a product's encapsulation has been opened, or if the product has been tampered with. For more information, see TAMPC — Tamper controller on page 192.

The crypto accelerator (CRACEN) peripheral is protected against differential power analysis (DPA) attacks. The AES, SM4, and public key acceleration engines all have countermeasures against DPA attacks and will report attack attempts. For more information, see CRACEN — Cryptographic accelerator engine on page 133.

7.8 Security components

7.8.1 CRACEN — Cryptographic accelerator engine

The main features of the CRACEN peripheral are the following:

- Cryptomaster – Symmetric cryptographic engines and digest engines
  - AES
    - Supports 128-, 192-, and 256-bit keys
    - Masking countermeasures
    - Context switching
  - HASH – including MD5, SHA1, SHA224, SHA256, SHA384, SHA512, and HMAC