  - Secure registers in the 0x4XXX_XXXX range are not visible for secure or non-secure code, and an attempt to access such a register will generate a peripheral access error, and result in write-ignore, read as zero behavior.
  - Secure code can access both non-secure and secure registers in the 0x5XXX_XXXX range
- 0x5XXX_XXXX, if the peripheral security attribute is set to secure

Note: An access to an address that is within the address range of an APB interconnect, but is not within the address range of a peripheral, will generate a peripheral acccess error, and result in write-ignore, read as zero behavior.

7.8.5.2.3 Special considerations for peripherals with DMA master

Peripherals containing a DMA master can be configured so the security attribute of the DMA transfers is different from the security attribute of the peripheral itself. This allows a secure peripheral to do non-secure data transfers to or from the system memories.

If the following conditions are met:

- The DMA field of PERIPH[n].PERM.DMA is "SeparateAttribute"
- The peripheral itself is secure (PERIPH[n].PERM.SECATTR == 1)

Then it is possible to select the security attribute of the DMA transfers using the field DMASEC (PERIPH[n].PERM.DMASEC == Secure and PERIPH[n].PERM.DMASEC == NonSecure) in PERIPH[n].PERM.

7.8.5.2.4 Peripheral access error reporting

The SPU generates a peripheral access error event once access violation is detected.

The following will happen if the logic controlled by the SPU detects an access violation on one of the peripherals:

- The faulty transfer will be blocked
- In case of a read transfer, the data will read as zero
- If supported by the master, feedback is sent to the master through specific bus error signals. If the master is a processor supporting Arm TrustZone for Cortex-M, a SecureFault exception will be generated for security related errors.
- The PERIPHACCERR event will be triggered.

7.8.5.3 Feature access control

Access to the features can be restricted. A feature can be declared as secure so that only secure peripherals can access it.

The security attribute of a feature is configured by using corresponding SPU's feature register. When the secure attribute is set for a feature, only secure peripherals and code will be able to access that feature. For example, register FEATURE.GRTC.CC[n] is used to configure security for the capture-and-compare functionality of the GRTC peripheral. When the secure attribute is set, only secure code can access and use the corresponding capture-and-compare registers, tasks, and events.

See the SPU configuration to find the features supported by each SPU instance.