

Bus manager security attribute	Destination memory security attribute	Address region	Access successful	SPU bus fault and error event
S	S	0x5	Yes	No
S	S	0x4	No	Yes
NS	S	0x5	No	Yes
NS	S	0x4	No	Yes
S	NS	0x5	No	Yes
S	NS	0x4	Yes	No
NS	NS	0x5	No	Yes
NS	NS	0x4	Yes	No

Table 26: Peripheral access overview

In addition, the following also applies:

- For split security peripherals, bus faults are not generated for blocked split security bit accesses. Reads as 0, write is ignored.
- In a split peripheral, access is blocked to secure registers using the non-secure 0x4 memory region because it is through non-secure transactions. Make sure to use the secure memory region to access secure registers.

7.2 TrustZone security

The security architecture is based on Arm TrustZone.

The Arm Cortex-M based CPU supports Arm TrustZone for secure, non-secure, and non-secure callable memory regions.

The security attribution unit (SAU) and implementation defined attribution unit (IDAU) define the access permissions based on the security state.

The IDAU configuration divides system memory space into secure (S) and non-secure (NS) regions. The SAU provides configurable regions for the Arm Cortex-M CPU, and is used to define non-secure callable (NSC) regions.

IDAU preset configuration

IDAU configuration is preset in hardware and is not available for user configuration. The security attribution follows the address map, and the peripheral memory space is aliased for the secure and non-secure memory state, as defined in the following table.