The security attribution of a bus transaction from the Arm Cortex-M33 is determined by the CPU, SAU, and IDAU settings. See TrustZone security on page 125 for more information.

For RISC-V and peripherals, the attribution of the bus transaction is determined by the SPU settings.

The destination's security attribute is a combination of MPC and SPU configurations.

Abbreviation	Description
NS	Non-secure – TrustZone security attribute is non-secure
S	Secure – TrustZone security attribute is secure
NSC	Non-secure callable – TrustZone security attribute is non-secure callable
IDAU	Arm implementation defined attribution unit
SAU	Arm security attribution unit
SPU	Nordic system protection unit
MPC	Nordic memory privilege controller

Table 24: Abbreviations

Memory access overview

The following table lists the security attributes of the bus manager and their access to memory configured as secure and non-secure.

Bus manager security attribute	Destination memory security attribute	Access successful	MPC bus fault and error event
S	S	Yes	No
NS	S	No	Yes
S	NS	Yes	No
NS	NS	Yes	No

Table 25: Memory access overview

Peripheral access overview

Peripherals are moved in the memory map based on their security association. Non-secure peripherals can be accessed through addresses starting with 0x4 while secure peripherals are accessible in the memory region starting with 0x5.

The security association of each peripheral is controlled via the SPU. Only peripherals with programmable security association can be moved in the memory map.