Arm Cortex-M TrustZone security attribute	Destination address security attribute	Secure fault	Access allowed
S	S	No	Yes
S	NS	No	Yes
NS	NS	No	Yes
NS	S	Yes	No

Table 29: TrustZone security access

The first two columns show the TrustZone security attribute from the TrustZone security attributes table.

The Arm Cortex-M TrustZone security attribute is the TrustZone security attribute seen by the Arm Cortex-M CPU while executing a program. This shows if the Arm Cortex-M CPU program is executed from S, NS, or NSC memory. The NSC for the Arm Cortex-M TrustZone security attribute behaves same as S in the table.

The destination address security attribute is the TrustZone security attribute of the destination address lookup from the SAU and IDAU. It is used by the Arm Cortex-M CPU on the bus transaction.

7.3 Immutable boot region

The device RRAM has a boot region that can be made immutable before the CPU starts up.

Boot initiated from an immutable source allows later boot steps to be performed by authenticated code.

The boot region starts at address `0x00000000`. This address contains the initial secure program counter (PC), the stack pointer (SP), and the interrupt vectors. The size and permissions of the region are configured using UICR register BOOTCONF on page 64.

After configuration, when there is a device reset, the hardware state-machine reads UICR fields and configures RRAMC. This enforces boot region protection before the Arm Cortex-M33 is released from reset.

For more information about the immutable boot region, see RRAMC — Resistive random access memory controller on page 47.

7.4 Security attributes

Bus access can have secure or non-secure attribution which follows the transaction through the system.

Non-secure peripherals use non-secure DMA bus transactions. Secure peripherals have configurable DMA security and can generate either secure or non-secure DMA bus transactions. The peripheral security is configured using SPU — System protection unit on page 180.

For Arm Cortex CPUs, see the Arm TrustZone architecture document for more details on security.

7.5 Security fault

Memory accesses that violate security permissions will generate a security fault.

If the Arm Cortex-M processor accesses RAM or NVM memory that violate security permissions, and the SAU regions match the device secure/non-secure memory map, the processor generates a SecureFault exception before the transaction enters the system busses.