Memory map name	Address map	IDAU TrustZone security attribute
Private peripheral bus	0xE0000000 – 0xFFFFFFFF	Not applicable
Device memory	0xA0000000 – 0xDFFFFFFF	NS
External memory	0x60000000 – 0xAFFFFFFF	NS
Peripheral (secure)	0x50000000 – 0x5FFFFFFF	S
Peripheral (non-secure)	0x40000000 – 0x4FFFFFFF	NS
Data memory	0x20000000 – 0x3FFFFFFF	NS
Program memory	0x00000000 – 0x1FFFFFFF	NS

Table 27: IDAU configuration

SAU configuration

The Arm Cortex-M33 CPU must configure its SAU regions when the CPU starts. The CPU assumes the memory map is secure before configuring the SAU regions.

SAU configuration registers are documented in the *Arm Cortex-M33 Technical Reference Manual*.

TrustZone security attributes

Based on IDAU and SAU configuration, the following table shows the TrustZone security attribute results.

IDAU security attribute	SAU security attribute	Security attribute result
S	NS, NSC, or S	S
NS, NSC, or S	S	S
NS	NS	NS
NS	NSC	NSC

Table 28: TrustZone security attributes

For the memory region that contains the secure gateway instruction branch veneers (entry points), the TrustZone security attribute seen by the Arm Cortex-M must be NSC for the secure functions that are callable from a non-secure program.

Example memory map

The following figure shows an example memory map using SAU regions to provide NS, S, and NSC regions. The figure also includes the required MPC override configuration to ensure correct secure/non-secure system partitioning.