7 Security

The device is designed with state-of-the-art security features that include the following.

- Arm TrustZone for memory, peripherals, GPIO pins, PPI channels, and interrupts
- Tamper controller to monitor and prevent physical attacks
  - Active driven tamper switches (active shield)
  - Signal protectors for critical configuration signals
  - Glitch detectors to guard against fault injection attacks
- Crypto accelerator with built-in self-check and countermeasures
  - Masking against simple and differential power analysis
  - Protection against timing attacks
- NIST SP 800-90B random number generator
- Non-volatile memory controller with built-in secure key storage (key management unit)
- Immutable boot region for establishing root of trust
- Authenticated debug to prevent unauthorized access to the debug port

7.1 Memory and peripheral access permissions

Access permissions are controlled by TrustZone, MPC, and SPU security peripherals.

The following figure shows the system security control modules for memory, peripherals, GPIO, and PPI.

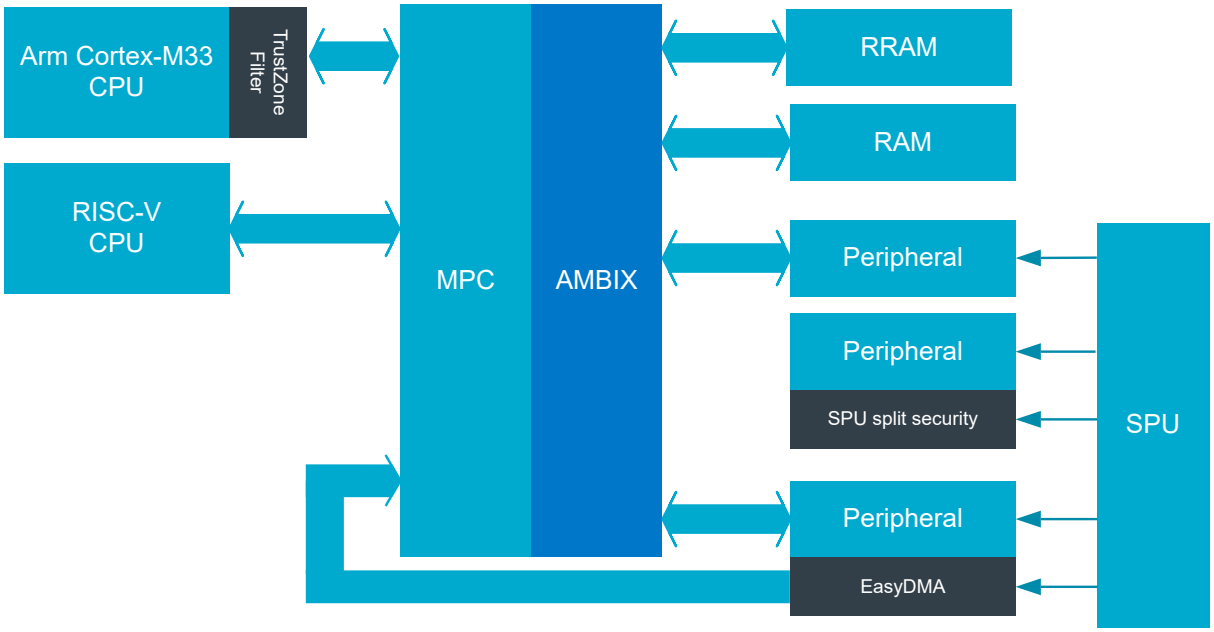

Figure 28: Modules filtering access permissions

The Arm Cortex-M33 CPU enforces TrustZone security internally, before issuing bus transactions. For security checks internal to the Arm Cortex-M33, see TrustZone security on page 125. After the internal CPU security check, the transaction is available on the bus.

Secure and non-secure memory has to be configured in the SAU and MPC.