3 Product overview

This document is applicable for the nRF54L15, nRF54L10, and nRF54L05 System-on-Chip devices. The main differences are memory, GPIO pin count, and package variants, which are detailed in their respective sections.

The device is an ultra-low power System on Chip (SoC) with advanced security features, a range of peripherals, and a multiprotocol 2.4 GHz transceiver. It supports Bluetooth Low Energy, IEEE 802.15.4 for Thread and Zigbee protocols, and allows for the implementation of proprietary 2.4 GHz protocols.

The main processing unit is an Arm Cortex-M33 processor running at up to 128 MHz, supported by non-volatile RRAM and RAM memory.

The Arm Cortex-M33 has a full set of digital signal processing (DSP) instructions and a memory protection unit (MPU) for application security. The full-featured, single-precision floating-point unit (FPU) supports all single-precision instructions.

The peripheral set offers a variety of analog and digital functionality, enabling single-chip implementation of a wide range of applications.

Hardware isolation between the secure and non-secure resources, as defined by Arm TrustZone, is implemented in the device. The hardware peripherals can be configured as secure or non-secure.

A key management unit (KMU) provides key storage, that when combined with a cryptographic accelerator (CRACEN), ensures discretion of encryption keys even within the secure world. The cryptographic accelerator has protection against differential power analysis (DPA) attacks.

The device protects against physical security attacks through several security measures. It can detect and report fault injection attacks such as voltage glitching or electromagnetic fault injection. An external active shield I/O interface provides PCB or product level security for the detection of a product's encapsulation being opened, or product tampering.

The non-volatile memory on the device has a boot region that can be made immutable before the CPU starts up. Boot initiated from an immutable source allows subsequent boot steps to be performed by authenticated code.

The debug access port can be enabled or disabled to allow both non-intrusive and intrusive debugging, from secure- or non-secure worlds. The non-volatile memory can be protected against erasing, providing protection from unauthenticated repurposing. Authenticated debug access control, such as facilitating the Arm ADAC architecture, is supported through a hardware mailbox. The mailbox allows on-chip firmware to authenticate the debug host before enabling the device debug interface.

The device has a dedicated RISC-V CPU (VPR), which is a fast, lightweight peripheral processor (FLPR) dedicated for software defined peripherals.

3.1 Block diagram

The block diagram illustrates the overall system.