SP 800-90B Non-Proprietary Public Use Document

Entropy Source Name: STM32U5x TRNG

Document Version: 1.1

Hardware Version: revision B and later

STMicroelectronics

39 Chemin du Champ des Filles

Plan-Les-Ouates, Geneva, CH-1228

Switzerland

December 16, 2022

**Revision History**

|  |  |
| --- | --- |
| Version | Change |
| 1.0 | Initial version |
| 1.1 | Reference update under Security Boundary |

Table of Contents

[Description 4](#_Toc117774276)

[Security Boundary 4](#_Toc117774277)

[Operating Conditions 5](#_Toc117774278)

[Configuration Settings 5](#_Toc117774279)

[Physical Security Mechanisms 6](#_Toc117774280)

[Conceptual Interfaces 6](#_Toc117774281)

[Min-Entropy Rate 7](#_Toc117774282)

[Health Tests 7](#_Toc117774283)

[Maintenance 7](#_Toc117774284)

[Required Testing 7](#_Toc117774285)

# Description

The STM32U5x TRNG entropy source is the physical hardwired peripheral generating random numbers, implemented in the STM32U575x/STM32U585x family of microcontrollers of revision B and Later.

Version of the STM32U5x TRNG entropy source can be read as 0x41 from the version register in the RNG peripheral (RNG\_VERR).

# Security Boundary

The STM32U5x TRNG entropy source depicted in Figure 1 below, is composed of a few major sections, which map to the conceptual components contained within an SP 800-90B entropy source.

The STM32U5x TRNG entropy source contains:

* Physical noise source, consisting of multiple copies of an analog noise source following SP 800-90B and FIPS 140-3 IG D.K Resolution 10.
* Digitization
* Health tests including:
  + Startup
  + On-Demand
  + Continuous
* Conditioning

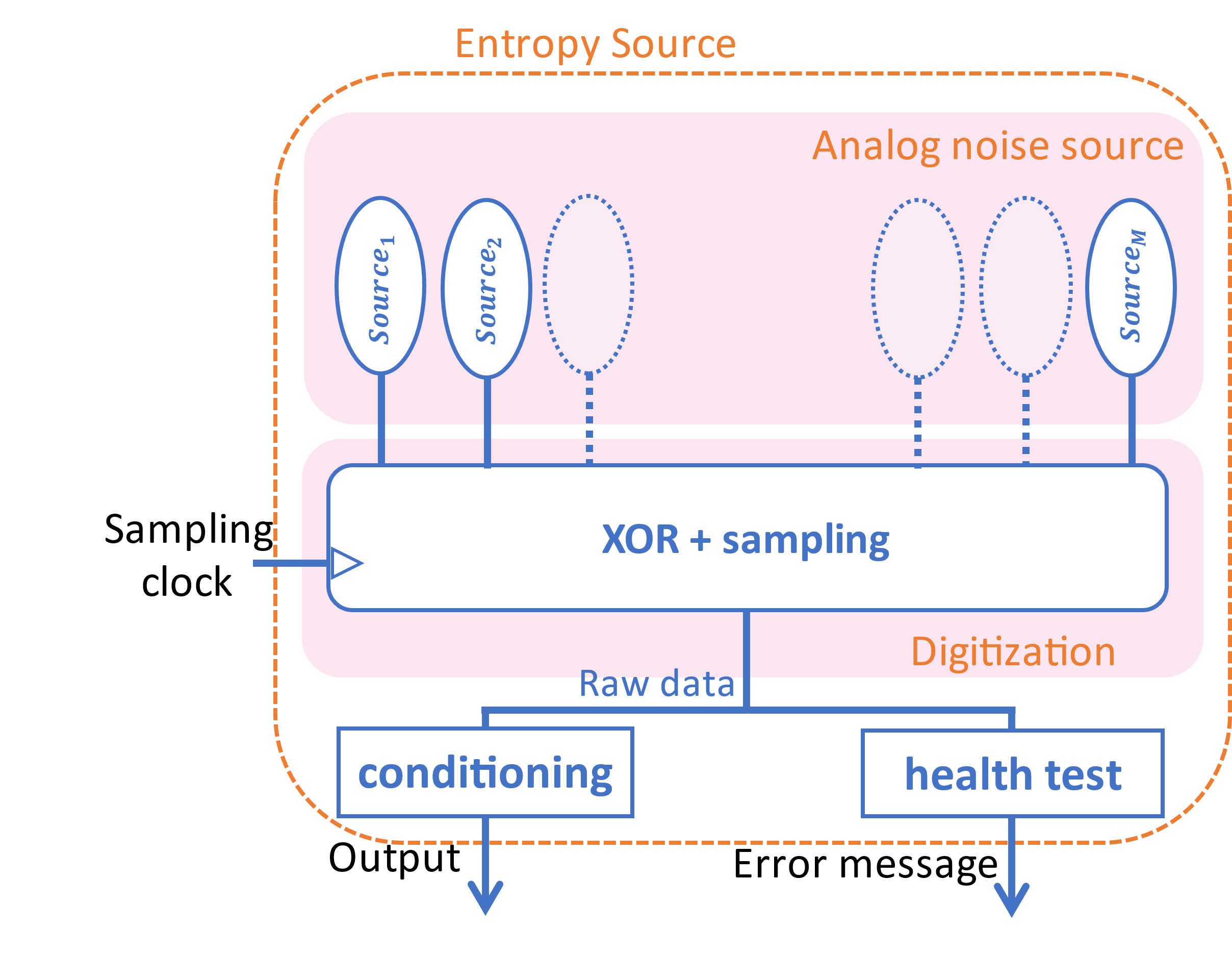


Figure 1: The STM32U5x TRNG entropy source

The analog noise sources are dedicated to the entropy source peripheral, and their behaviors cannot be altered by any code or by any debugger.

# Operating Conditions

Table 1 summarizes the operating conditions under which the STM32U5x TRNG source entropy assessments has been performed.

|  |  |  |
| --- | --- | --- |
| Parameter | Value | Description |
| System clock | 160 MHz | Microprocessor CPU clock |
| Temperature | 25 °C | Microprocessor operating temperature range |
| RNG AHB clock | 160 MHz | RNG peripheral bus clock |
| RNG kernel clock | 48 MHz | RNG peripheral dedicated kernel clock  (integrated oscillator HSI) |
| RNG voltage | 3.3V | RNG peripheral digital power supply |

Table 1: operating conditions

# Configuration Settings

When using the register configurations summarized in Table 2, the STM32U5x TRNG entropy source configuration is set correctly (sample interval, startup delay, conditioning function and compression ratio, health-tests cutoffs).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Register | Description | Bits | Values | Comment |
| RNG\_CR | Control register | [31:0] | 0x80F0 0DXX | This configuration is valid for RNG Kernel clock= 48MHz.  Bit 31 locks the RNG configuration until next IP reset.  The XX value depends on the application: Bit 2 is set when RNG peripheral is needed, bit 5 is set to detect too low RNG kernel clock, and bit 3 is set to enable RNG interrupts. Other bits in the byte stays at 0. |
| RNG\_NSCR | Noise source control register | [31:0] | 0x17CBB | This register is used to activate mutually independent sources. |
| RNG\_HTCR | Health test register | [31:0] | 0x06E9C | For α=2-20 corresponds to 27 for repetition tests and 668 for adaptive tests |
| 0x0A2B0 | For α=2-30 corresponds to 40 for repetition tests and 688 for adaptive tests |

Table 2: Entropy source registers configuration

The RNG\_HTCR controls the health test cutoffs for the SP 800-90B approved health tests. The options in the table, α=2-20 or α=2-30, represent the selection of a false positive rate for the entropy source health tests to operate with. This is achieved by the register selecting different cutoff limits for each health test, which has been mathematically calculated to have the respective false positive rate.

# Physical Security Mechanisms

The STM32U5x TRNG entropy source is a fully hardwired module implemented in the microcontroller's integrated circuit as an RNG peripheral.

The entropy source module does not give access to raw data from the noise source.

The STM32U5x microcontroller hardware and software resources can be partitioned so

that they exist either in the secure world or in the non-secure world, using Arm® TrustZone® technology. The secure world can be used to protect critical code against intentional or unintentional tampering from the more exposed code running in the non-secure world. The initial partitioning of the platform is under the responsibility of the secure firmware executed after reset of the device. This protection is activated when TZEN option bit is set in the FLASH\_OPTR register.

The STM32U5x TrustZone® hardware protection can be used to protect the configuration of the RNG peripheral, to ensure the correct behavior of the entropy source. Specifically, application can set RNGSEC bit in GTZC1\_TZSC\_SECCFGR3 register to restrict access to the RNG peripheral to secure world only. Setting this bit also restrict to secure world only the RNG peripheral control bits for clock, reset, clock source selection and clock enable during low-power modes.

RNG peripheral 48MHz clock source (HSI48) configuration can also be made secure-only in the RCC peripheral.

# Conceptual Interfaces

The GetNoise interface is available for certification purpose only. Indeed, when using microcontrollers dedicated to entropy certification, the entropy source can provide the raw data generated by the noise source, by reading the RNG peripheral data register (RNG\_DR).

The raw data of the noise source is never available when using standard STM32U575x/STM32U585x microcontrollers.

The GetEntropy interface is accessible in the field. The entropy source provides random data outputted by the conditioner directly in the RNG peripheral data register (RNG\_DR).

The HealthTest interface is always accessible. The entropy source clears to 0 the bits 1 & 2 of RNG status register (RNG\_SR) if the entropy source passed the NIST SP800-90B approved health tests. The bits 1 & 2 are set to 1 otherwise.

# Min-Entropy Rate

The STM32U5x TRNG entropy source provides 128 bits of min-entropy per 128 bits output sample, or full entropy.

# Health Tests

The STM32U5x TRNG entropy source continuously performs the repetition count test (RCT) and the adaptative proportion test (APT) Health Tests specified in SP800-90B section 4.4. The health tests operate at either a false positive rate of α=2-20 or α=2-30 dependent on the configuration of the RNG\_HTCR register.

# Maintenance

No maintenance is required for the STM32U5x TRNG entropy source.

# Required Testing

The STM32U5x TRNG entropy source was tested by collecting data from the designated operational range and processed with the SP 800-90B tool. Raw and restart noise data was collected through an interface not available during normal operation. Test data was collected following the requirements of Section 3 of SP 800-90B. All tested data was evaluated at a higher entropy than the defined entropy of the assessment, and all restart sanity checks were passed.

No further testing is required.