SP800-90B Non-Proprietary Public Use Document
SE051 Entropy Source V1.0.0

Document Version 0.3

November 16th, 2023

Prepared with support from

Table of Contents

References

Ref.	Full Specification Name	Date
[90A]	NIST, SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	24-Jun-2015
[90B]	NIST, SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation	10-Jan-2018
[140IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program	1-Aug-2023
[EAR]	Modified Bernoulli Shift Map (MBSM) Entropy Source Entropy Analysis and SP 800-90B Compliance Report	4-Feb-2022

1 Description

This document is a summary of the SE051 product family entropy source. The entropy source (depicted in Figure 1) is composed of a few major sections which map to the conceptual components contained within an SP 800-90B entropy source; the SE051 entropy source contains a noise source, health tests, and a conditioning algorithm.

This assessment was conducted using data and parameters measured in the evaluated version and configurations described In Table 1.

Table 1: Evaluated Entropy Source Specification

Identifier	Details
Entropy Source Name	SE051 Entropy Source
Part Numbers	FIPS SE051 and FIPS SE050
Hardware Revisions	N7121 B1 using ROM ID 2E5AD88409C9BADB
Entropy Category	Physical (P)
Test Platform(s)	FIPS SE051 and FIPS SE050
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

2 Security Boundary

The SE051 entropy source is depicted in the block diagram below.

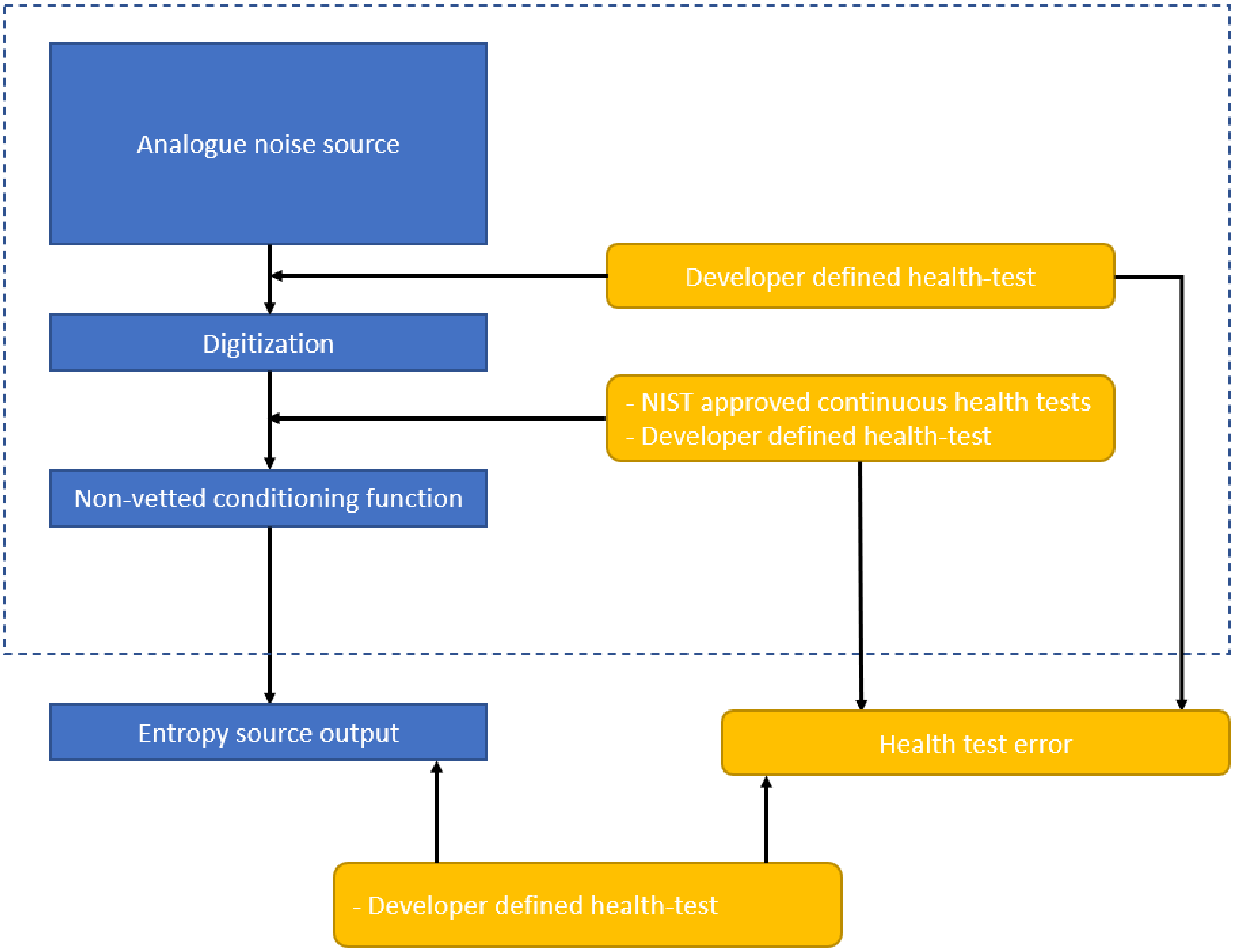
Analogue noise source
Developer defined health-test
Digitization
- NIST approved continuous health tests
- Developer defined health-test
Non-vetted conditioning function
Entropy source output
Health test error
- Developer defined health-test

Figure 1: SE051 entropy source

The analogue noise source is based on the repeated functional composition of a chaotic map. For the range of parameters that can arise in this implementation, this results in a 1-dimensional chaotic system.

Any bias and serial correlation present in the raw data is reduced by a conditioning algorithm which forms each bit of output using six time-shifted outputs from the noise sources for every bit produced. This conditioning algorithm takes in a total of 48 bits, and outputs 1 byte (8 bits).

Health testing occurs on both the raw data and on the conditioned data. If the results of the health tests are too far out of their expected range, then the health tests fail, and an error indicator is output.

3 Operating Conditions

The Entropy-relevant operating conditions for all entropy source variants listed in Table 1 are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	-60 to 125C
Voltage	N/A*

*The internal voltage within this part is regulated, so variations in the input voltage are not expected to produce any significant change in behavior so long as the input voltage is within the allowed bounds; if the input voltage is out of the bounds for which this behavior cannot be assured, then the entire part is disabled, including the entropy source.

4 Configuration Settings

There are no configuration settings required for the correct operation of the entropy source.

5 Physical Security Mechanisms

The NXP SE051 entropy source operates within the physical protections of the associated SoC package. The physical protection mechanisms of the SoC cover the whole entropy source.

6 Conceptual Interfaces

From a (end user) consuming application point of view, this section is N/A.
The output of the entropy source is available via SFR to specialized SW (crypto lib) that evaluates the health test information, computes a further developer-defined health test + implements CTR-DRBG (with derivation function). The consuming application only has access to this SW implemented DRBG output.

7 Min-Entropy Rate

The min-entropy rate for the NXP SE051 entropy source is > 7.30359 bits/byte.

8 Health Tests

The module continuously performs NIST approved health tests (RCT for SE051) as well as developer-defined health tests on both raw data as well as conditioned data. The combined set of tests guarantee that the data used for instantiating and reseeding the DRBG in SW is always healthy.

9 Maintenance

The SE051 design does not require maintenance.

10 Required Testing

The entropy source as incorporated in the SE051 families were tested in compliance with [90B] methods. In order to characterize the stability of the noise source and provide a bound for its min entropy production, samples
created by multiple hardware parts were analyzed under a variety of environmental conditions.

18 sample sets of raw data, with over 160 million samples in each sample set were analyzed. Each of these sample sets are the sequential raw data output from the SE051 noise source.
These sample sets are expected to allow the testing to characterize the full range of operations within the expected environmental and process envelope.

Built-in health tests described in the section above constantly check the validity of the produced output of the entropy source. Therefore, no further testing is required.

11 Vendor Permissions and Relationship

The reuse status of this entropy source is restricted to Christie Digital Systems Canada Inc. For any information please contact Amanda Fisher amanda.fisher@christiedigital.com.

NXP Semiconductors Netherlands B.V has provided explicit authorization to Christie Digital Systems Canada Inc. to be listed as the vendor on the ESV certificate.