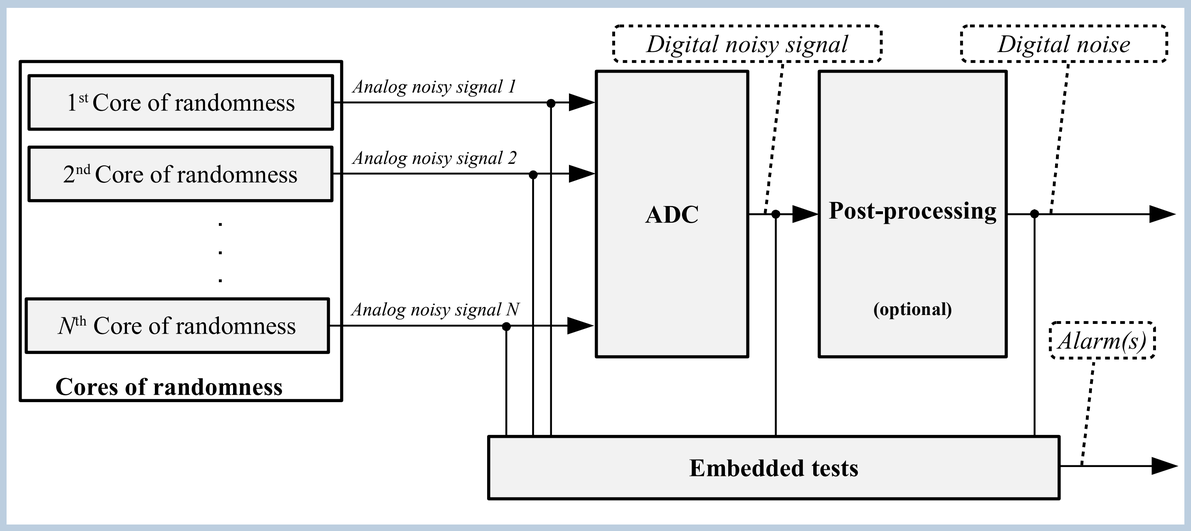
DGA Recommendations for Design and Validation of a Physical True Random Number Generator

David Lubicz
david.lubicz@univ-rennes.fr

TRNG Assumptions

In the vast majority of cases, the physical random phenomena used in PTRNGs are analog. The mechanism performing analog-to-digital conversion is thus an integral part of the generator. Accordingly, we distinguish four basic PTRNG blocks:

- Core(s) of randomness, which include source(s) of randomness,
- Analog-to-digital converter (ADC),
- Post-processor,
- Embedded tests.



Some important requirements

Requirement 1. (**[Model] Availability of the stochastic model of the core of randomness**) The statistical model $M(t, p_1, \ldots, p_n)$ of each core of randomness exploited by the generator for the production of the *proven entropy* shall be available.

Requirement 2. (**[Model] Mathematical description of the ADC**) The ADC transforms elements of $V \times S$ into a series of bits. The model of the ADC $f_0 : V \times S \to \{0,1\}^*$ describing this transformation shall be identified.

Requirement 3. (**[Model fitting] Evaluation of parameters of the physical noises**) One shall be able to evaluate experimentally the parameters $p_1, \ldots, p_n$ of the statistical model for physical noise $M(t, p_1, \ldots, p_n)$. One shall be able to evaluate the measurement errors of these parameters.

Requirement 4. (**[Model fitting] Evaluation of parameters of the physical noises**) One shall be able to evaluate experimentally the parameters $p_1, \ldots, p_n$ of the statistical model for physical noise $M(t, p_1, \ldots, p_n)$. One shall be able to evaluate the measurement errors of these parameters.

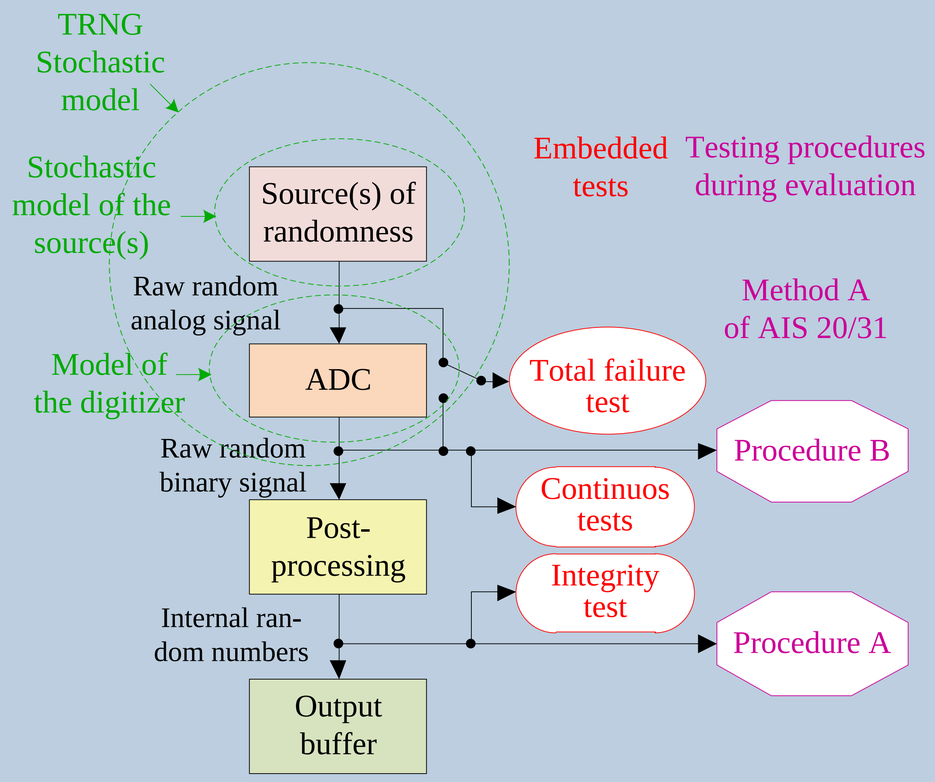
Requirement 5. (**[Model fitting] Stability of parameters of the statistical models of the physical noises**) The stability of parameters $p_1, \ldots, p_n$ of the stochastic model shall be evaluated for the physical noise.

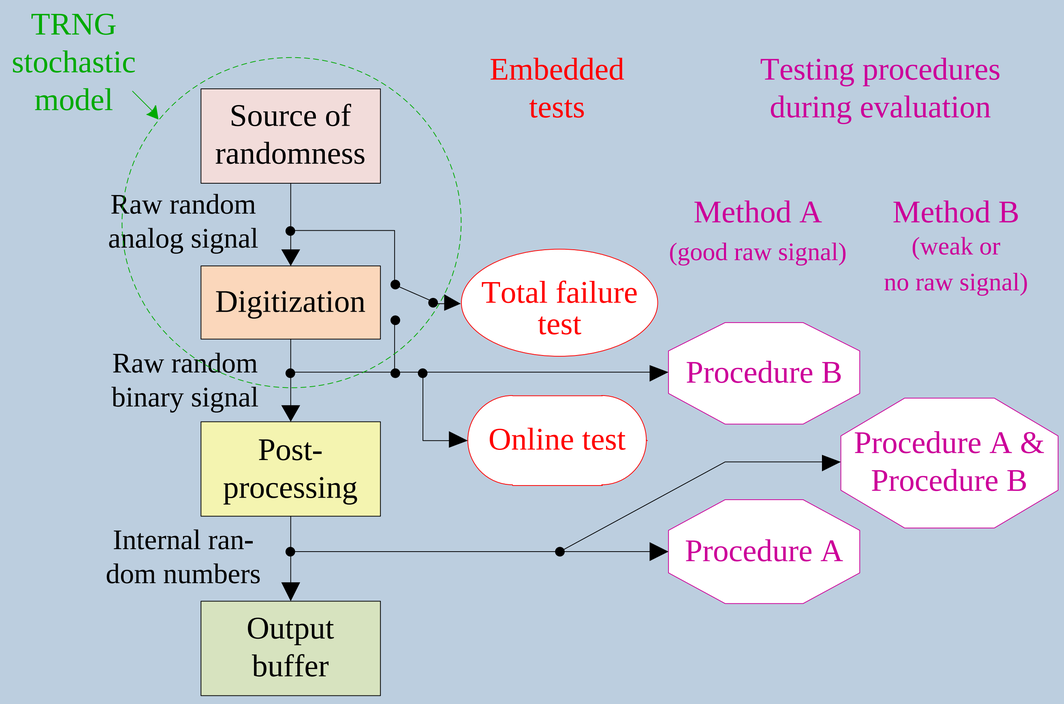
Requirement 6. (**[Tests] Verification of integrity of the PTRNG data path**) Correct operation of all the blocks between the core of randomness and the generator output shall be verified using the PTRNG integrity tests.

Comparison with AIS 31

We have checked that our guidelines are mostly compatible with AIS 31. However, the following list of requirements, which are not explicitly specified in AIS 20/31, shall be satisfied according to our document:

- Availability of the stochastic model of the core of randomness
- Mathematical description of the analog-to-digital conversion
- Characterization of the effect of the analog-to-digital conversion
- Consistency of the stochastic model of the PTRNG
- Evaluation of parameters of the physical noises
- Stability of parameters of the stochastic models of physical noises
- Verification of integrity of the whole datapath between outputs of sources of randomness and output of the digital noise.





References

[1] David Lubicz and Viktor FIscher. Recommendations for the design and validation of a physical true random number generator integrated in an electronic device. Cryptology ePrint Archive, Paper 2024/301, 2024.

[2] Wolfgang Killmann and Werner Schindler. A design for a physical RNG with robust entropy estimators. In *CHES*, pages 146–163, 2008.

[3] E. Barker and J. Kelsey. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90 (Revised). [online] Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-90r.pdf, 2007.