On the way to secure random number generation

Patrick Haddad
STMicroelectronics - Advanced System Technology

Viktor Fischer & Florent Bernard
Université de Saint-Etienne- Laboratoire Hubert Curien

life.augmented

Random numbers in cryptography

Usage of random numbers in cryptography:

- Cryptographic keys
- Initialization vectors
- Nonces
- Padding values
- Counter-measures against side-channel attacks

Random number sequences are generated using random number generators:

- Pseudo-random number generators
- True random number generators

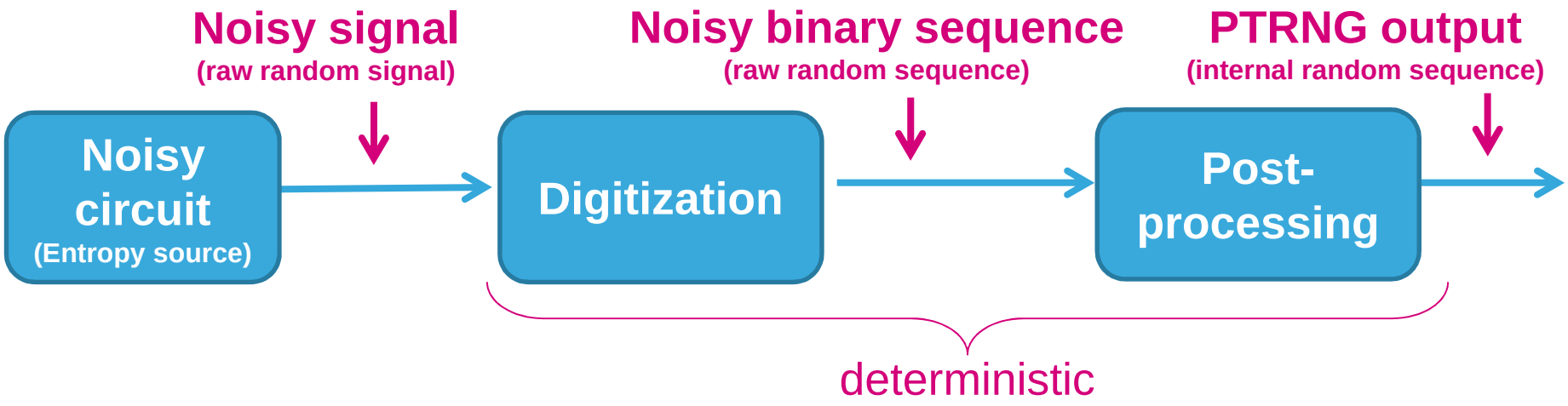
Basic requirements on random sequences:

- Good statistical quality
- Unpredictability and non-manipulability

Secure random number generators (RNG) in IC

1st security condition - unpredictability

RNG used in ICs exploits noisy physical phenomenon



The unpredictability of the generated sequence is guaranteed

Quantification of the influence of noisy signal on raw and internal random sequence

Their exact name is :

Physical True Random Number Generator (PTRNG)

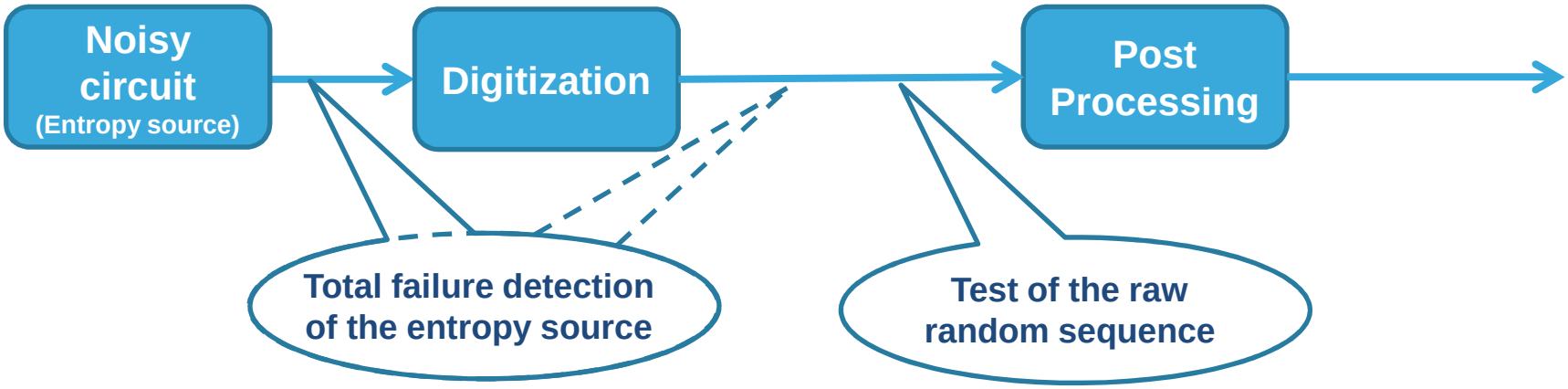
Secure PTRNG against non-invasive attacks

2nd security condition - non-manipulability

Recent works highlighted the random number unpredictability reduction with non-invasive attacks [1-4]

The unpredictability of the generated sequence is guaranteed → **Check the quality of the generated sequence while the PTRNG is in operation (online tests)**

AIS online tests recommendations (PTG2):



[1] : K. Wold & al, Robustness of TRNG against Attacks that Employ Superimposing Signal on FPGA Supply Voltage (2010).
[2] : A. Markettos, The frequency injection attack on ring-oscillator-based true random number generators (2009).
[3] : M. Soucarros & al , Influence of the temperature on true random number generators (2011).
[4] : P. Bayon & al, Contactless electromagnetic active attack on ring oscillator based true random number generator. (2012)

Overview of the presentation

PTRNG secure

- **Quantification of the influence of noisy signal on random sequences**
- **Quality check of the generated sequence while the PTRNG is in operation (online tests)**

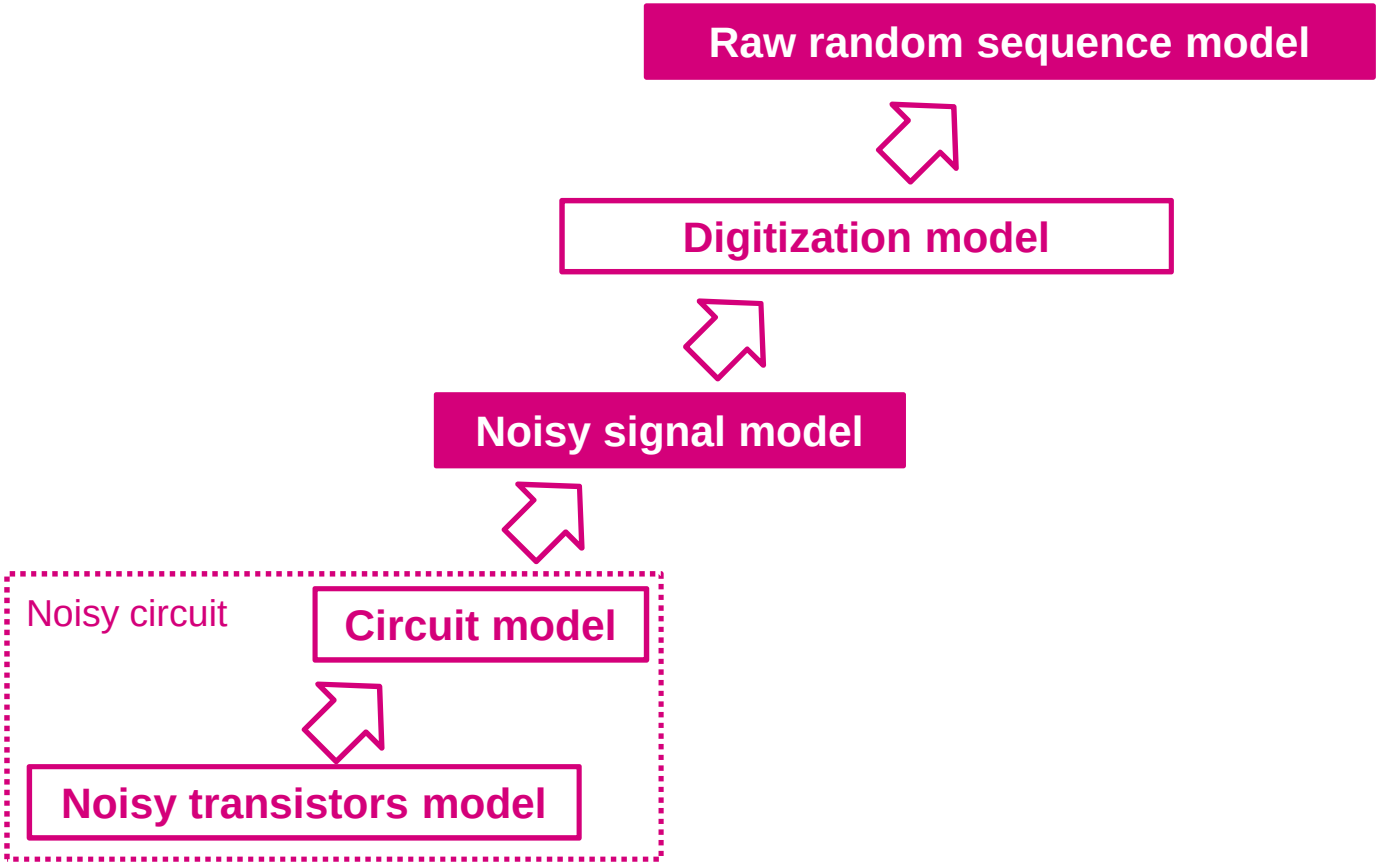
We will present:

- **A simple methodology to :**
  - **Quantify the influence of noisy transistors on raw random sequence**
  - **Help in the design of online tests**

- **Apply the proposed methodology to a PLL based PTRNG**

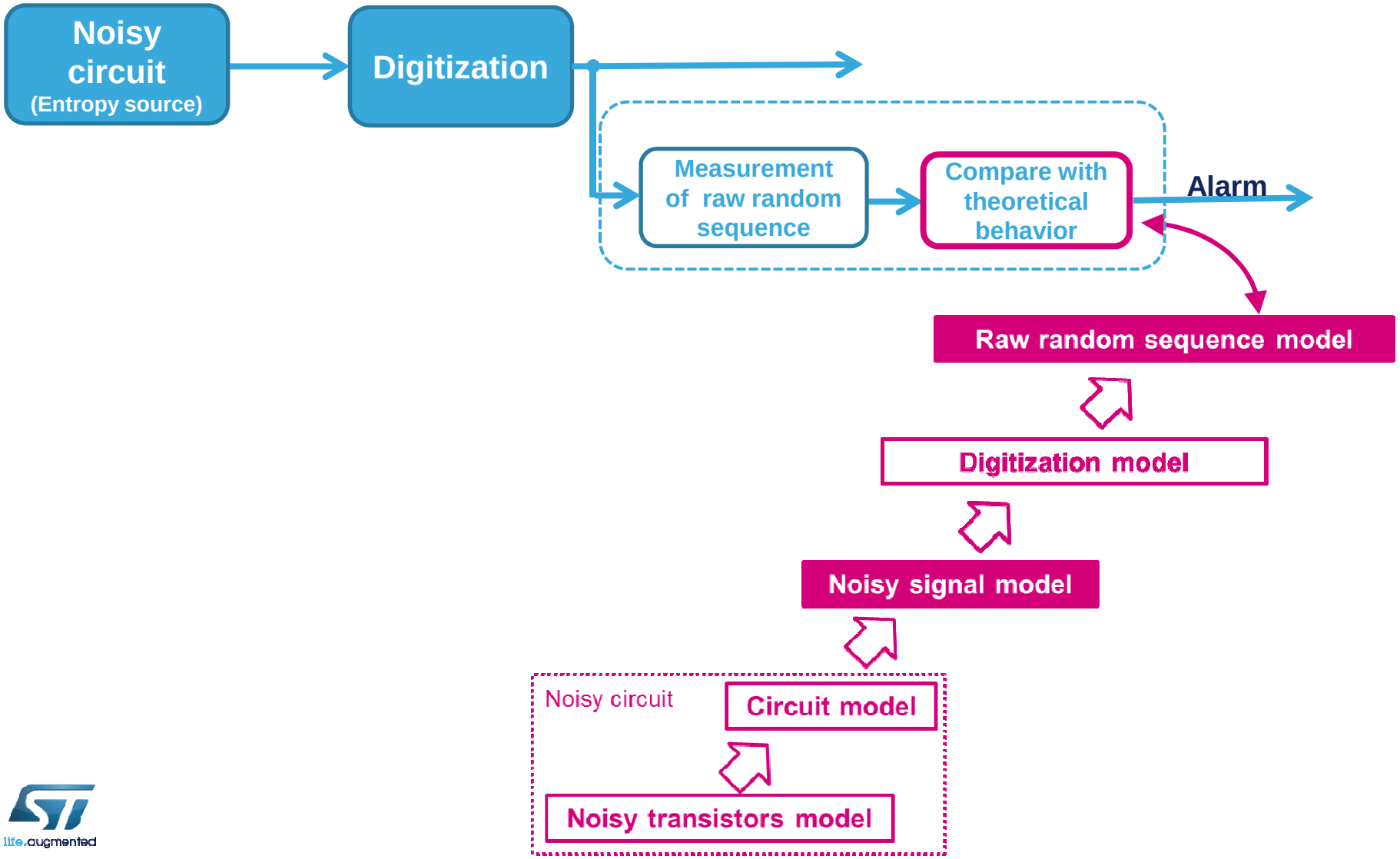
Methodology – a chain of models

Objective: Quantify the impact of noisy transistors on generated raw random sequence



life.augmented

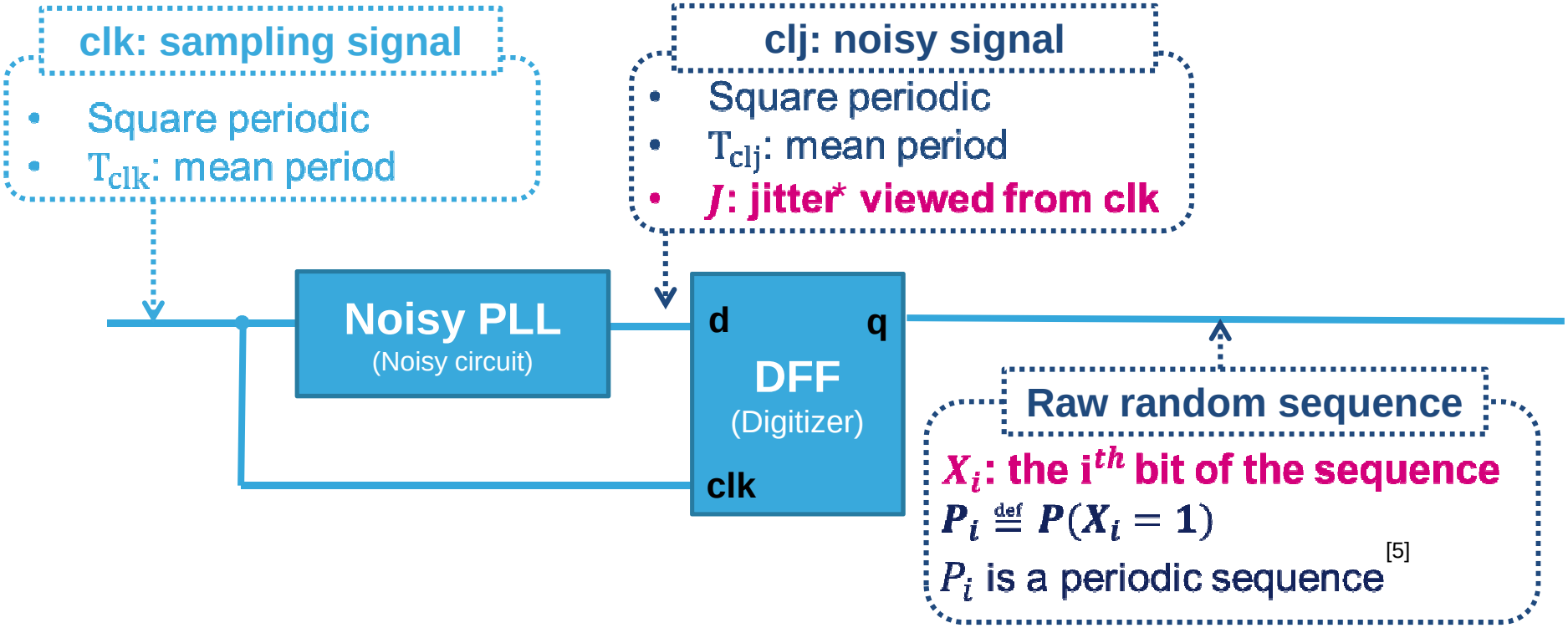
Chain of models & online test



Next step of the presentation

Application of the proposed methodology to a PLL based PTRNG

Application to the PLL based PTRNG



Next step : Establish theoretical values of P_i

- **Quantify the influence of noisy transistors on raw random sequence**
- **Use it as reference for online test**

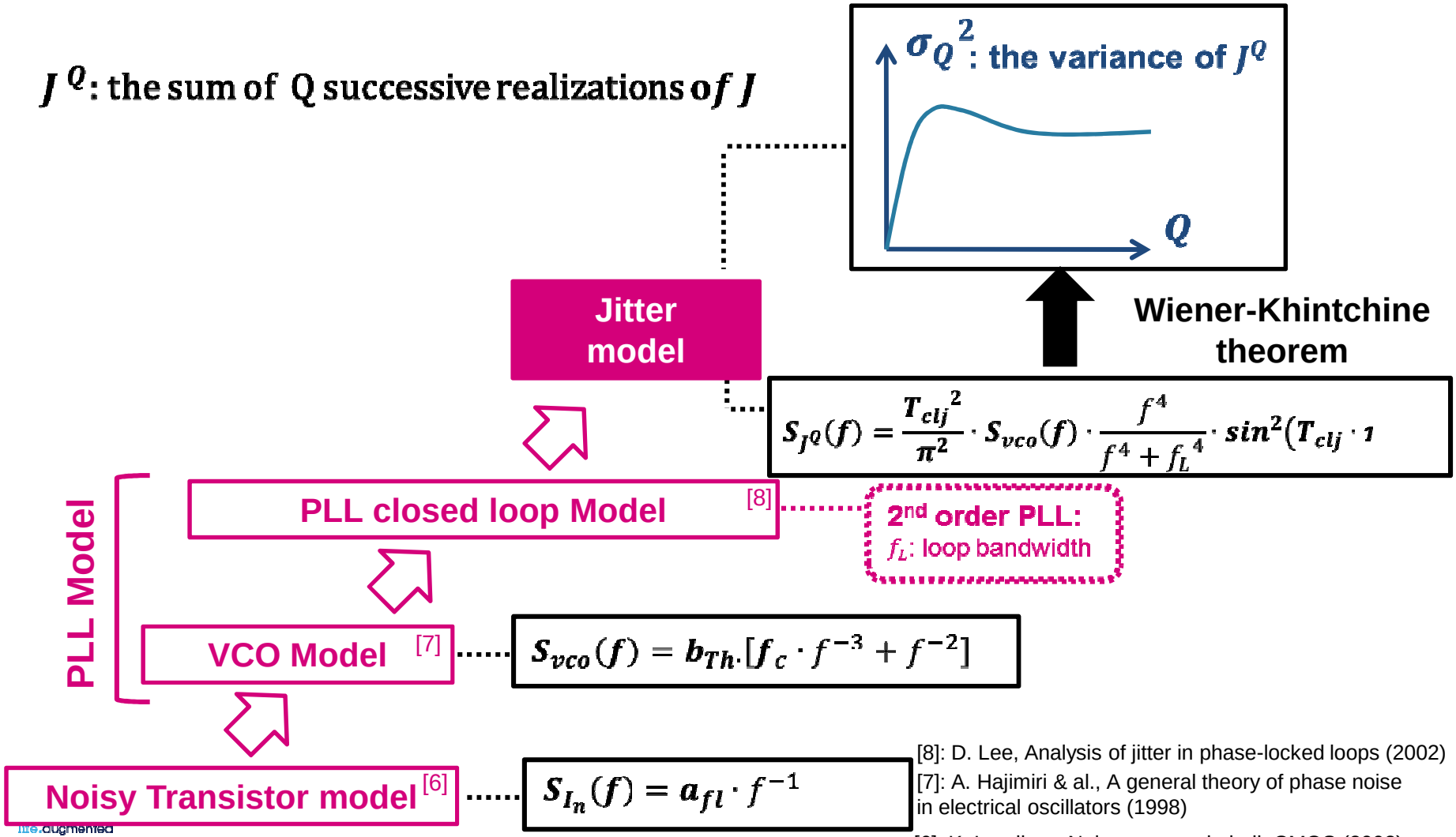
life.augmented

* : undesired instabilities of the period

[5]: V. Fischer & al. True Random Number Generator in Reconfigurable Hardware (2003)

Chain of models for PLL base PTRNG

Low level models

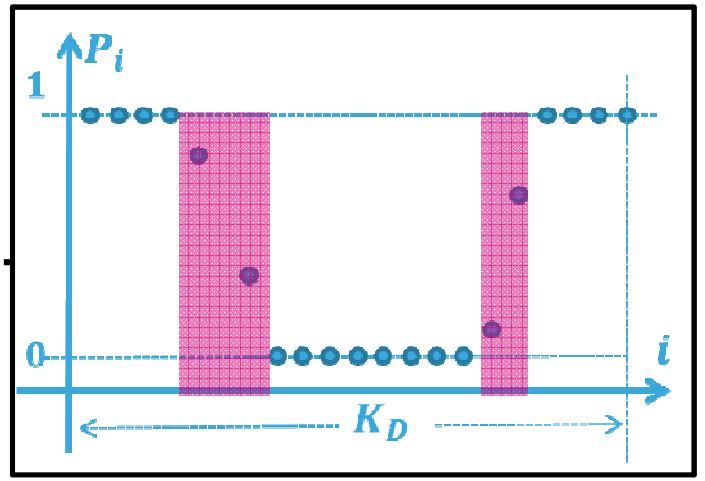


[8]: D. Lee, Analysis of jitter in phase-locked loops (2002)
[7]: A. Hajimiri & al., A general theory of phase noise in electrical oscillators (1998)
[6]: K. Lundberg Noise sources in bulk CMOS (2002)

Chain of models for PLL base PTRNG

Top level models

P_i is the quantification of the influence of noisy transistors on raw random sequence

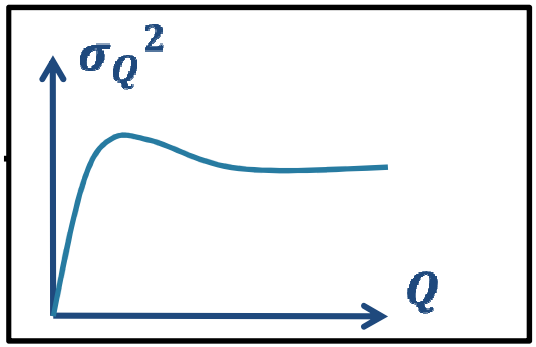


Raw random sequence model

Sampling model

$$P_i = \quad [9]$$

Jitter model

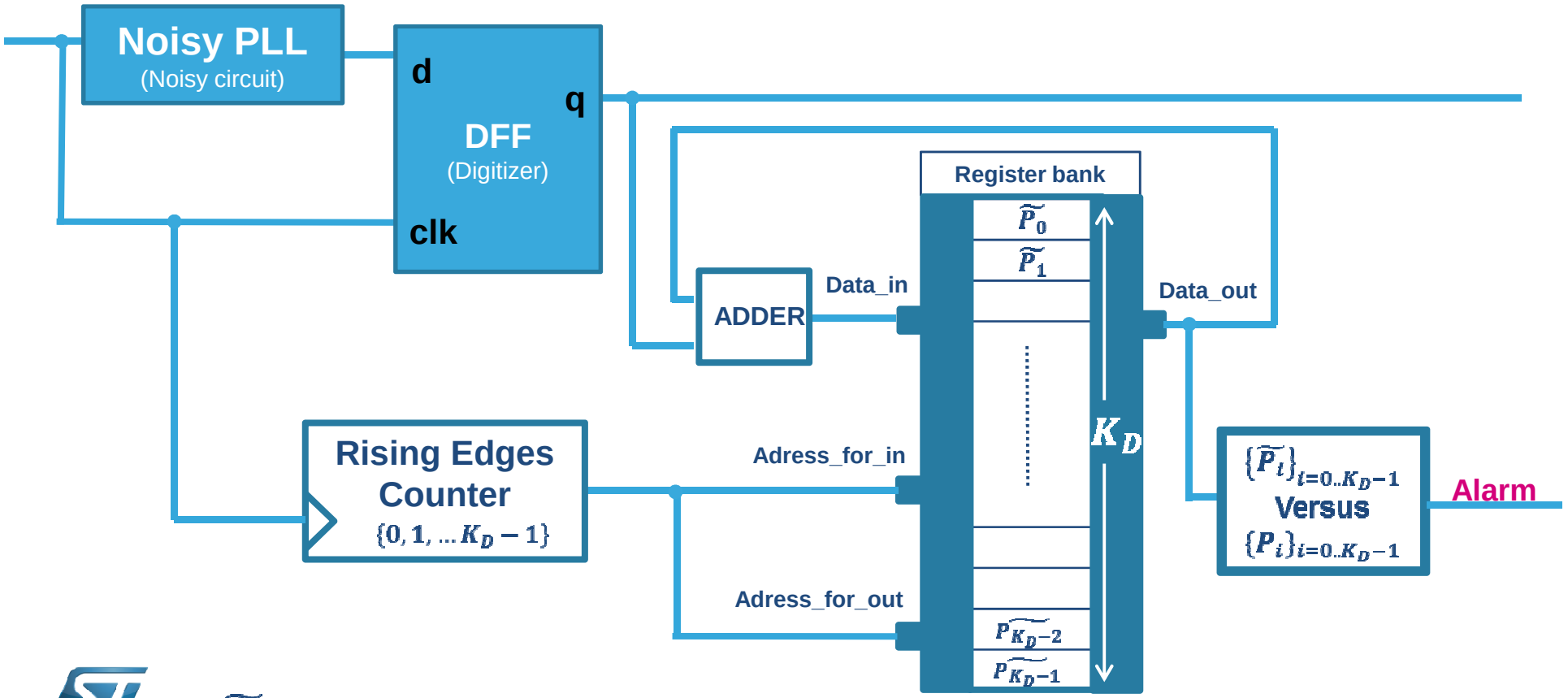


life.augmented

[9]: F. Bernard & al. Mathematical Model of Physical RNGs Based on coherent sampling (2010)

Test of the raw random sequence

For testing the raw random sequence, we estimate a period of P_i and compare it with theoretical values



life.augmented

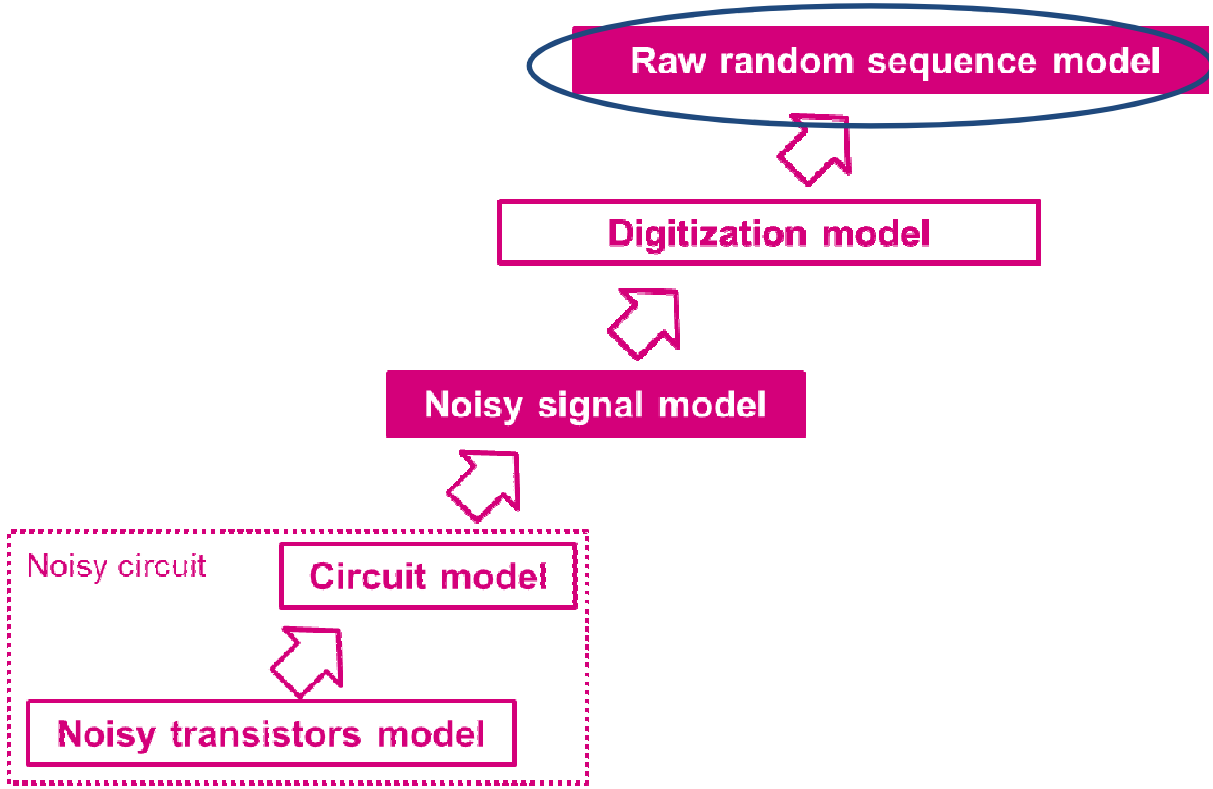
$\widetilde{P_i}$, an estimation of P_i

Summary

We proposed :

A chain of models : from transistor level to raw random bit level

- *Quantify the influence of noisy transistors on raw random sequence*
- *Use a link as reference for online testing*



Summary

We proposed :

A chain of models : from transistor level to raw random bit level

- ***Quantify the influence of noisy transistors on raw random sequence***
- ***Use a link as reference for online testing***

We presented:

- **The chain of models for the PLL based PTRNG**
- **PLL based PTRNG online test using on this chain of models**

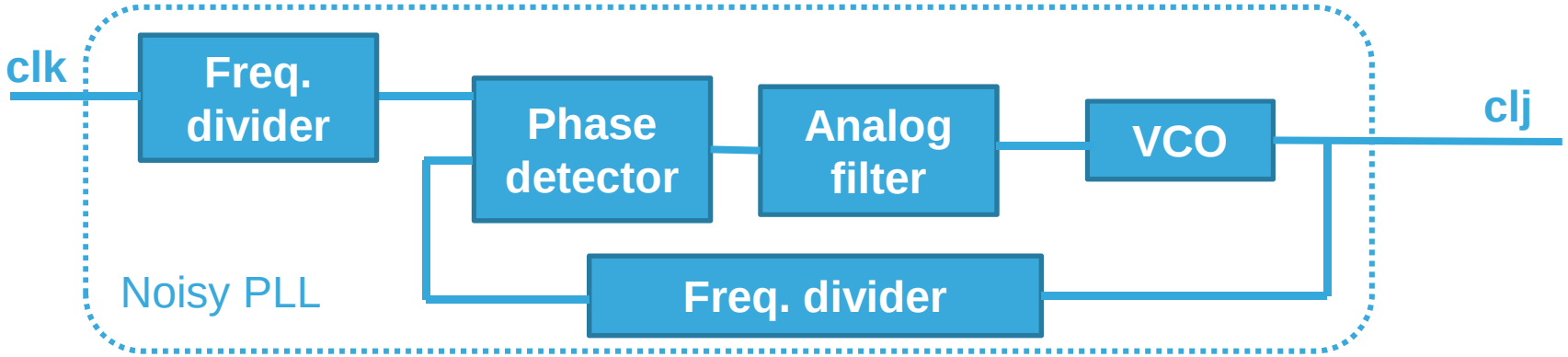
We plan:

- **Establish the chain of models for other PTRNG structures**
- **Design theirs online test using theses chains of models**

Thank You

Noisy PLL

A phase locked loop is an oscillator phase control system.



J^Q: the sum of Q successive realizations of J

$$S_{J^Q}(f) = \frac{T_{clj}^2}{\pi^2} \cdot S_{vco}(f) \cdot |1 - H(f)|^2 \cdot \sin^2(Q \cdot T_{clj} \cdot \pi \cdot f) \quad [7]$$

PSD of J^Q

PSD of phase noise in the VCO

PLL closed loop transfer function

life.augmented

PSD=Power Spectral Density

[7]: D. Lee, Analysis of jitter in phase-locked loops (2002)