Some lesser-known contributions of Paul Caspi

Jacques pulou

With some help from E. Closse and D. Weil

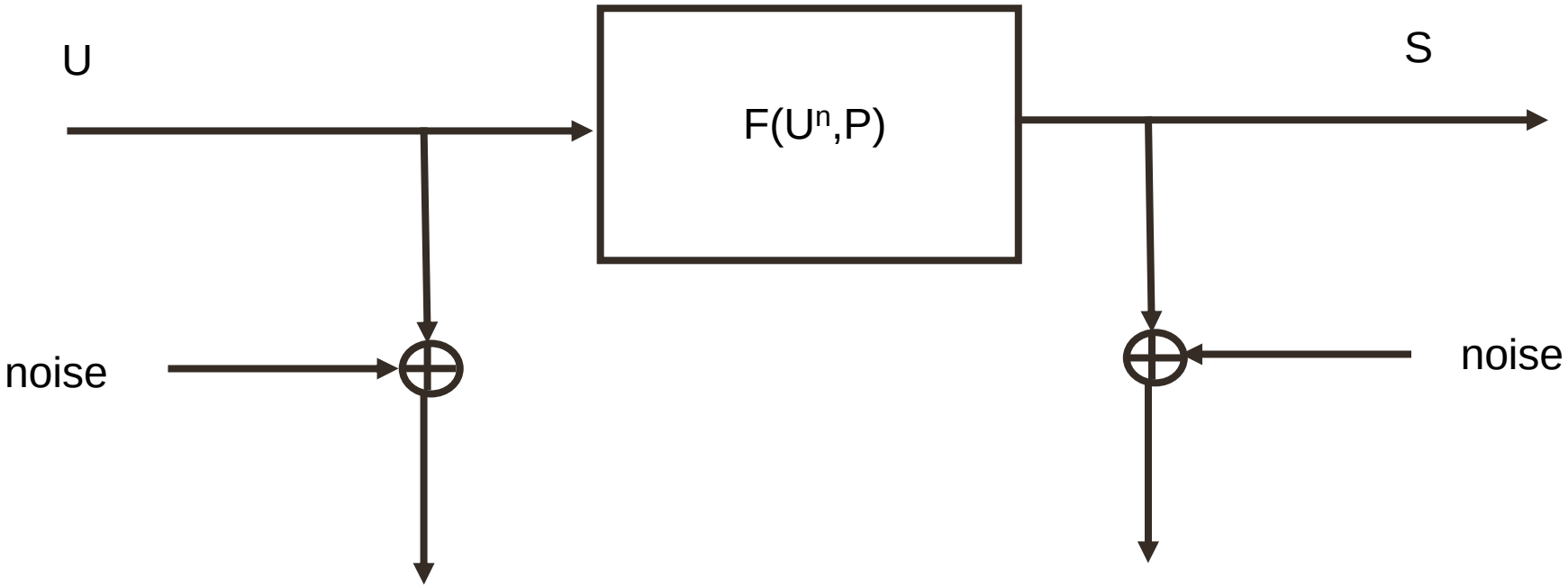
DASSAULT SYSTEMES

France Telecom R&D MAPS/AMS/SUME

orange™

research & development

Paul 's Doctorate Thesis : identifying unstable deterministic linear systems



Crucial moment during Paul's defense :
(1979 May 25th 1979, IEG-INPG)

One examiner of the Paul Caspi Doctoral Thesis defence :

"Mister Caspi: what good are non stable systems ?"

Paul Caspi :

"Imagine that each cow produces 0,9 calf by year on the average"

Two exemple of linear deterministic and unstable systems

Country beef herd

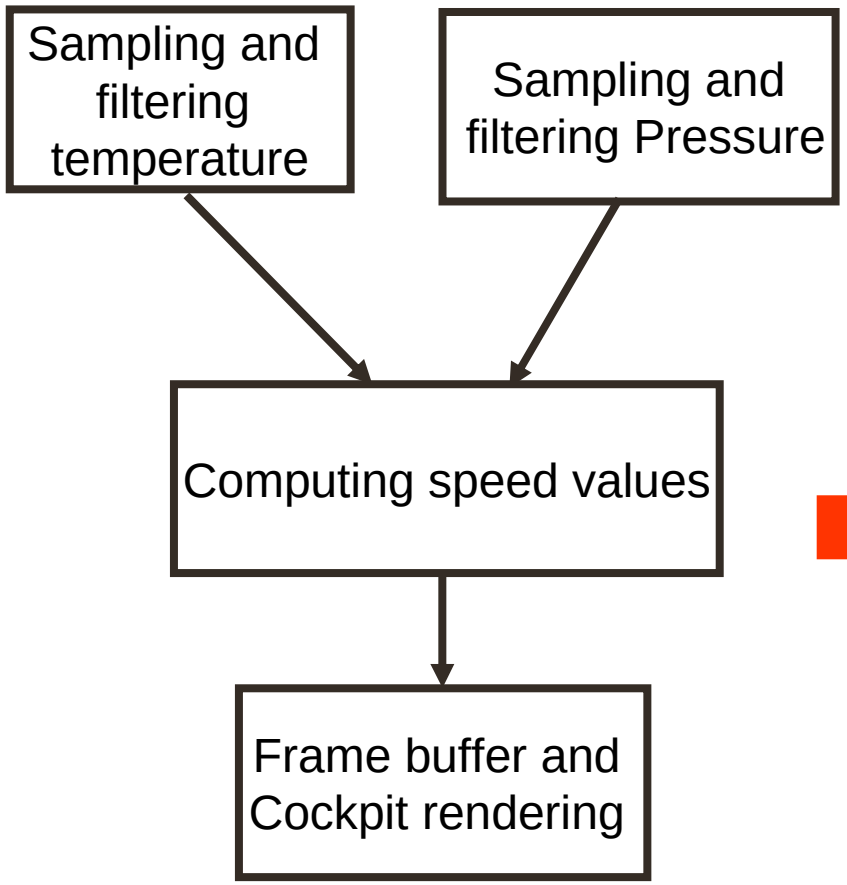
hydroptere

1 : first encounter with safety critical applications

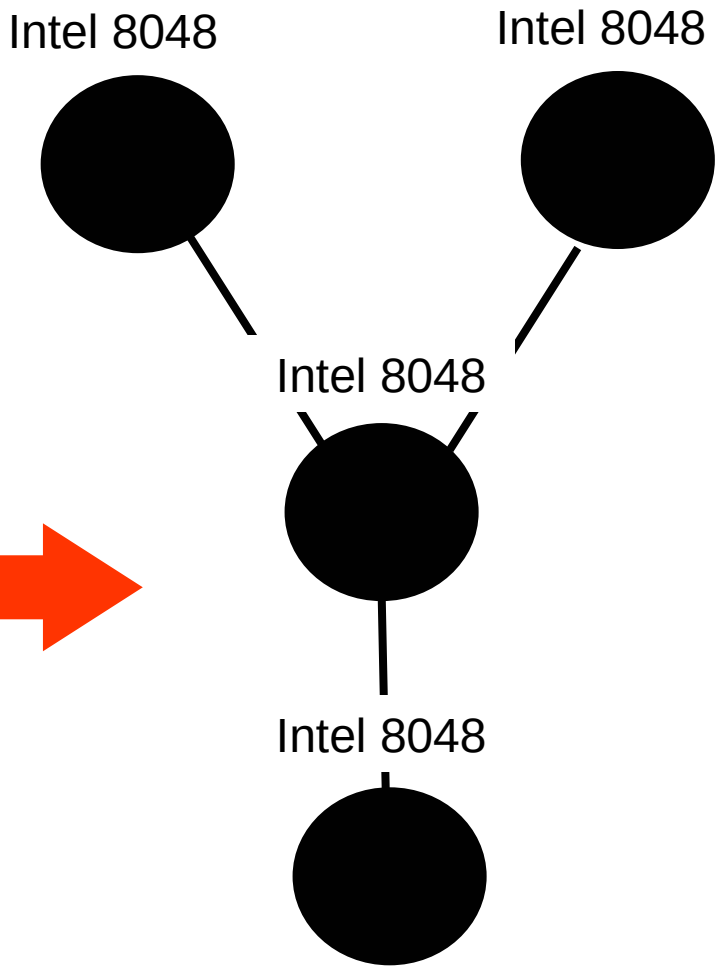
- Crouzet Aviation (now subsidiary of Schneider Electric)

- Crouzet (Valence near Grenoble) wants to experiment SC systems
- Crouzet proposes to study a concrete example :

  - Airborne anemometric station (sampling pressure-s and temperature sampling to compute aircraft speed)
  - The goal was to be better than 10^{-7} fault / hour
  - On the average – 10 hour flight – 1 default for 1Million flights

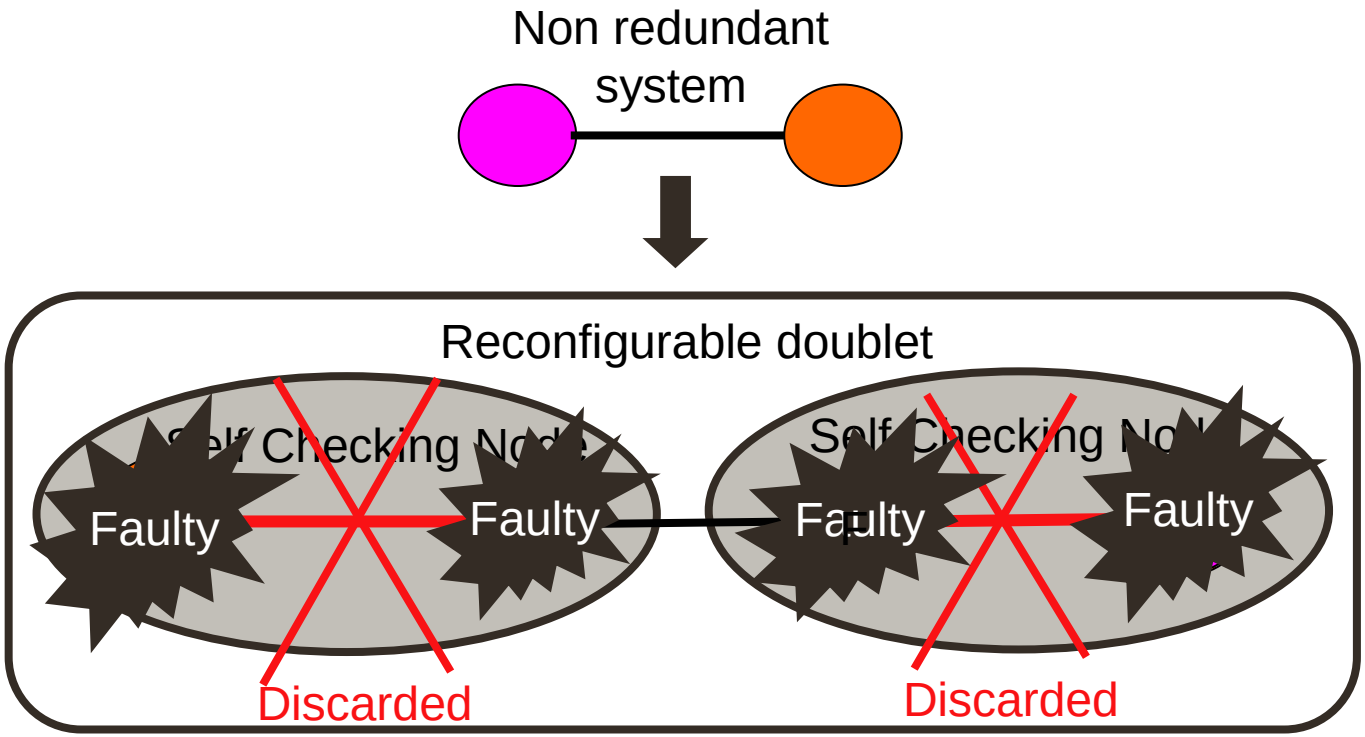


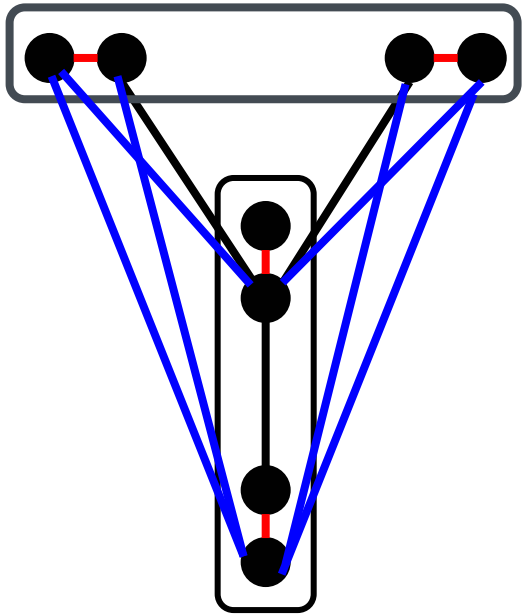
Computation Graph

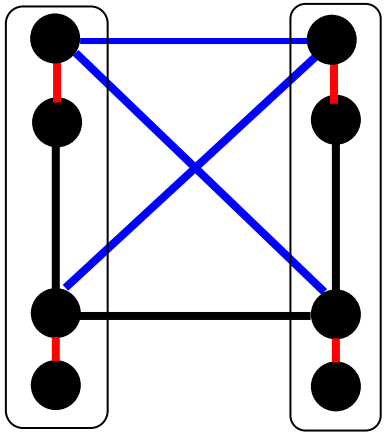


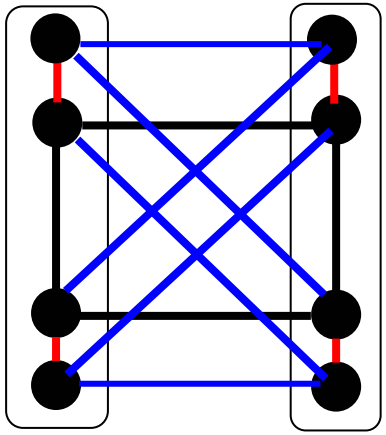
Ad hoc network of controllers

Self checking and reconfigurable systems

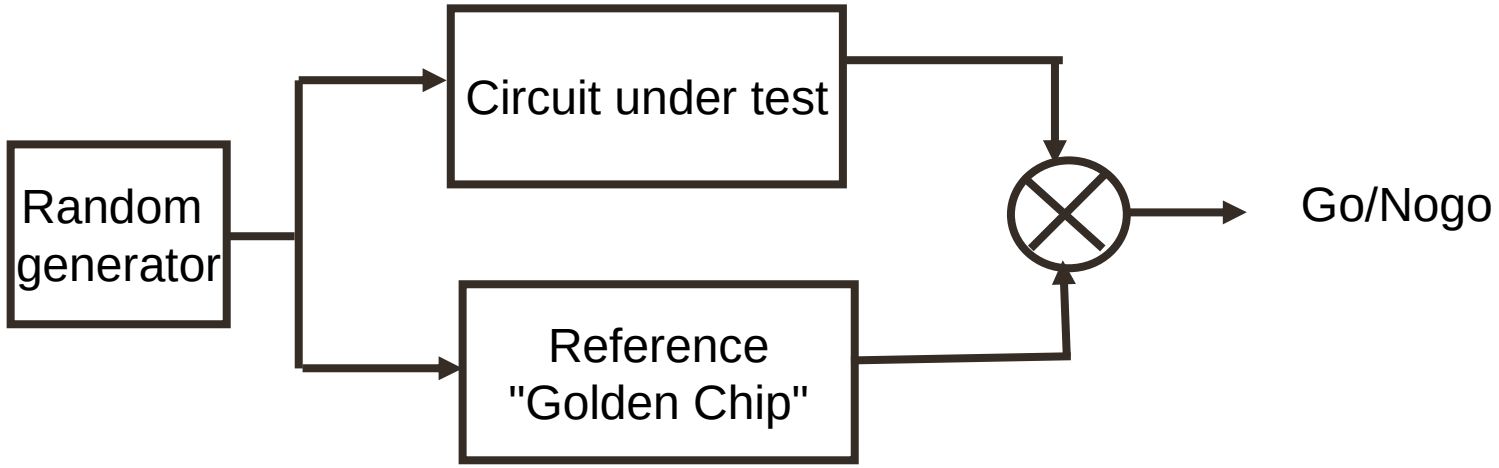








2 : Meeting IC Random Testing

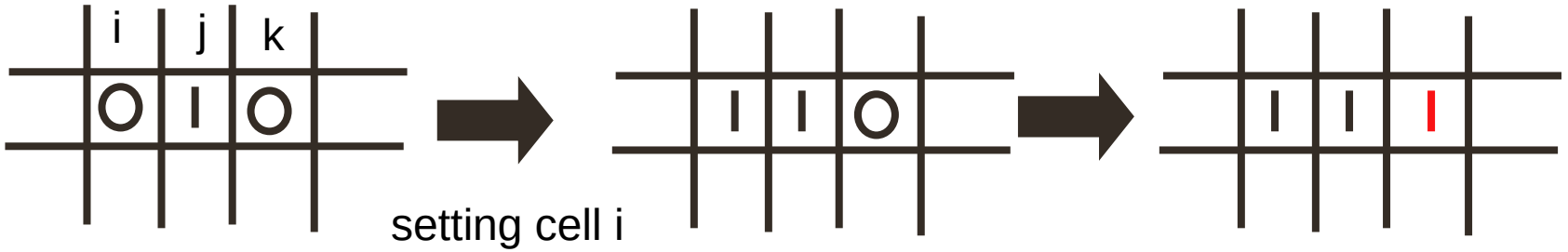


- Given a **set of fault F** and a **level of confidence** 1-ε
- Find the **minimal number of inputs** L that decreases the risk to get a "false positive" under ε
- If **Pf** is the probability that an input detect the "**most difficult to detect**" fault f within F then :

$$L = \log(\varepsilon) / \log(1-pf) \qquad pf = \min_{f \in F} \Pr\{\text{a random input detect } f\}$$

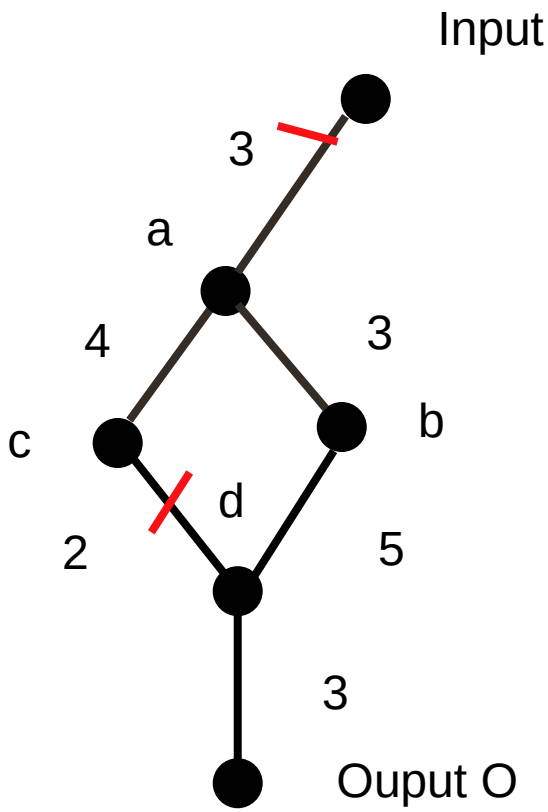
Random Testing of RAM

- Fault hypothesis on RAM take into account RAM cell plane geometry or its word structure.
  - Suppose cells i, ,j, k = (0,1,0) when i is set then k is upset too



- Such fault are denoted as finite pattern sensitive fault (PSF)
- Paul give the rather simple demonstration that test length (at a given confidence level) for any PSF behaves linearly with the size of memory: $L = \alpha + \beta n$

3: Hardware Testability Measure



Module netlist of an harware system

Consider node c :

Minimal Cut from circuit input i to c

Commandability of c =3

Minimal cut from c to circuit output o
Observability of c =2

Introducing Information theorie based testability measure

- Module Observability and Commandability are based on a "new Entropy " function with respect to the one from C.E Shannon (this is an upper bound of it)

- Defining Module Commandability and Observability as upper bounds of the amount of information that can be brings respectively:
  - to the module inputs from circuit inputs
  - from the module outputs to circuit outputs

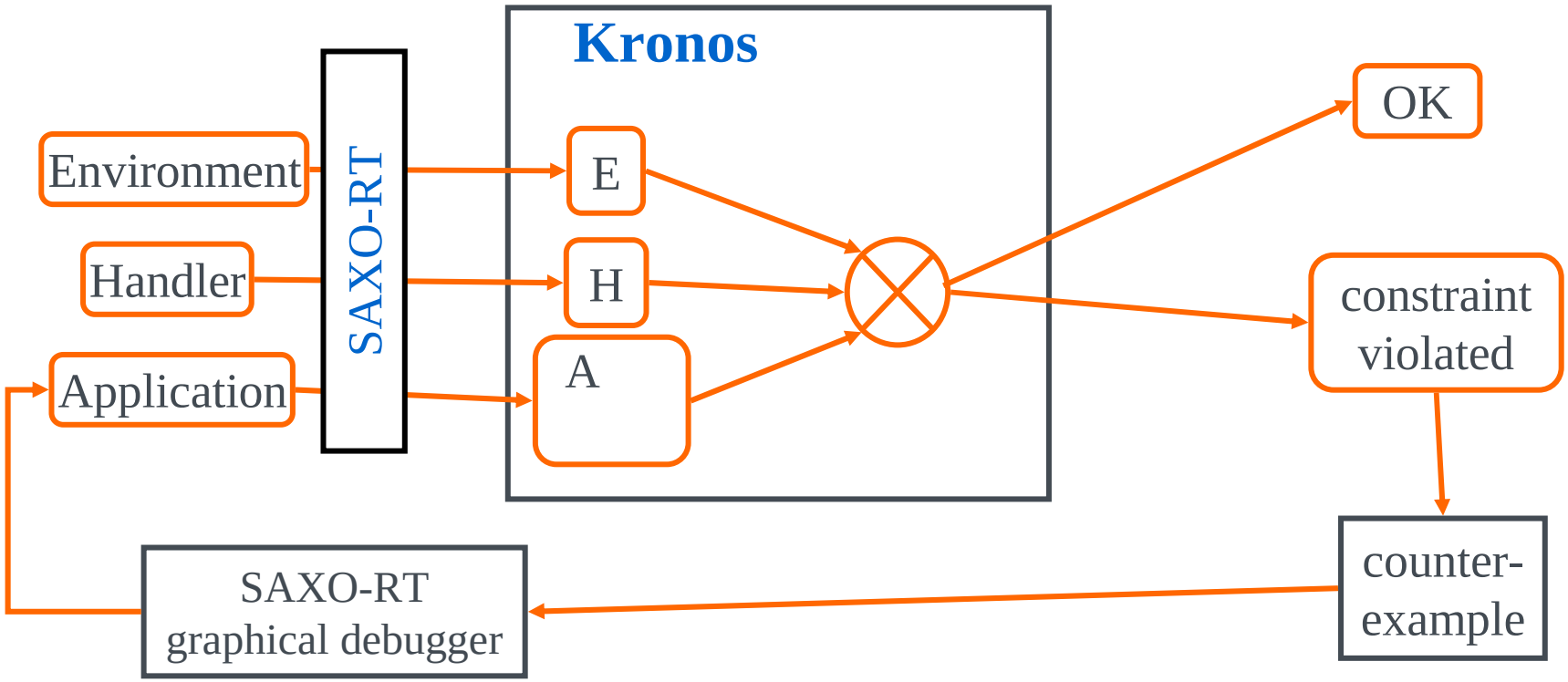
- This very basic (precise module function are not taken into account) but seminal work has been further extended to software issue …
  - New testability measure beside classical NPATH and McCabe'cyclomatic number
  - Promising application to testability measurement of …. LUSTRE synchronous data flow programs . (SATAN Tool)

4 : Triggering the France Telecom branch of the synchronous evolution

- An existing target for code execution, but without high level specification (GSM MAC layer of ALCATEL one touch mobile)
- Paul Caspi advice: the Esterel formulation is well adapted
- A new kind of Esterel compilation method : the SAXO-RT compiler
  - Efficient
  - For a subset of Esterel in a first step, then a complete compiler
- Transfer to Dassaut Systems (E.Closse and D.Weil)
  - Development of LCM: Esterel semantic + ML features
  - Evolution of LCM:
    - Convergence data flow and state machine
    - back to Lustre branch in the Lucid form (collaboration with M.Pouzet)

TAXYS = Kronos + Esterel
➔ Assigning timed behaviour to Esterel

- Kronos : model-checking of timed-automata (VERIMAG)
- TAXYS : annotated ESTEREL as high-level language for writing timed automata.



THANK YOU PAUL…

Between Control and (not only !) Software

Stop Malville,non à Superphénix


Welcome in a Synchronous World !
?
?
Copyright Hergé
& G. Berry

Assuming perfect observability of subsystem

Information based Testability

$$\sum p_i \log_2 p_i$$

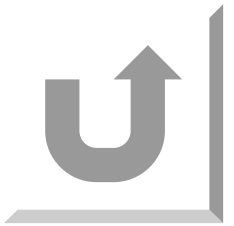
$i \in$ set of input s of a given (sub)-system

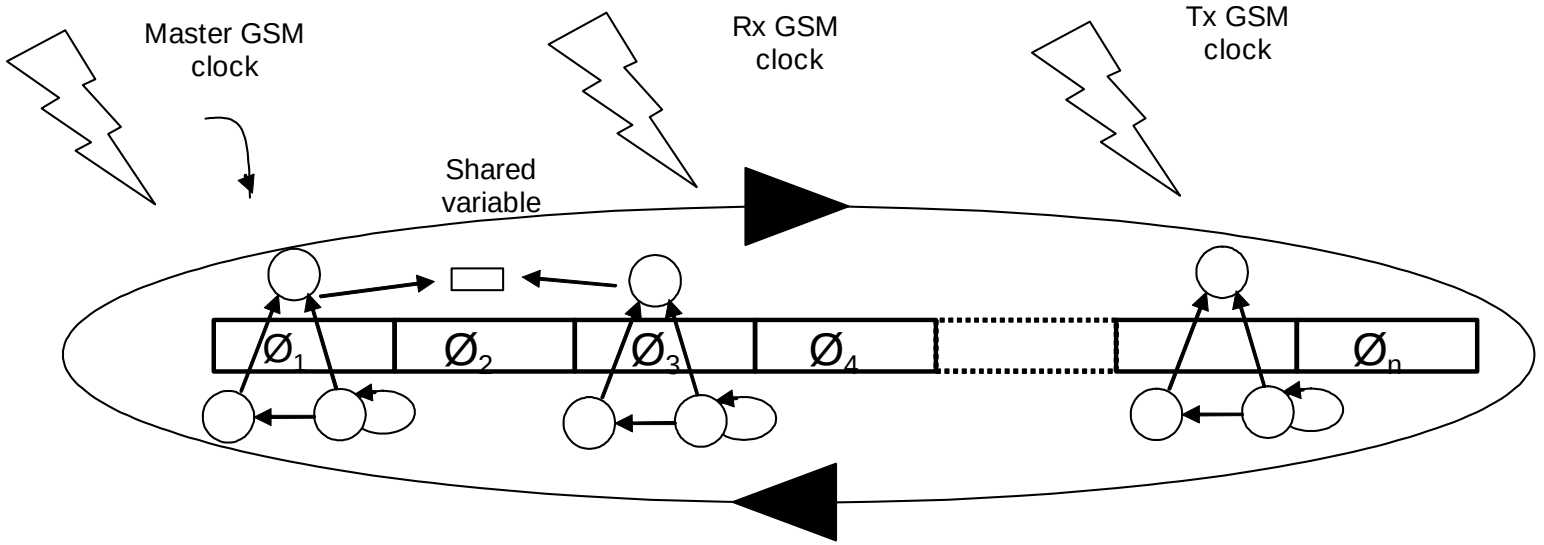
"Random" Testability

$$\text{Min}\ (p_i)$$

$i \in$ set of input s of a given (sub)-system

p_i = Probability that input of (sub) system = i




Master GSM clock
Rx GSM clock
Tx GSM clock
Shared variable
Ø1
Ø2
Ø3
Ø4
Øn

Selected References

[1] P. Caspi *"Sur l'identification des systèmes linéaires déterministes instables"* ("identification of non stable deterministic linear systems") Doctorat ès Sciences Physiques, INPG/UJF 25 mai 1979

[2] P. Caspi J. Pulou *« A method for improving the reliability of functionally distributed networks »* Journal of Digital Systems, Vol IV, Issue 4,

[3] P. Caspi, E. Pilaud, J. Pulou *« Some validation methods for fail safe or fault tolerant systems »* Digest of 4th Fail FTSD Conference Brno,

[4] P. Caspi, A. Mili, C. Robach « *An Information Measure on Nets* » Proceeding of IFAC Workshop On Information and Systems, Compiégne France, Octobre 1977, pp 35- 39

[5] Y. Le Traon and C. Robach, " **Testability Measurements for Dataflow Designs,** " *Proc. of the 4th International Software Metrics Symposium (Metrics 97)*, Albuquerque (New Mexico), 1997, pp. 91-98

[6] R. David *« Random Testing of Digital Circuits, theory and applications"* Marcel Dekkers, ISBN 0 8247 0182 8

[7] R. David, H. Alla *« Discrete, Continuous and Hybrid Petri Nets*, springer, ISBN 3-540-22480-7

[8] E. Flamand and all, « *SAXO, a retargetable optimized compiler for DSPS* »Proceedings of the 8th international Conference on Signal Processing Applications & Technology, San Diego, California,USA, , pp 1032-1036.

[9] Bertin, V., Poize, M., and Pulou, J. 1999. "*Une nouvelle méthode de compilation pour le language ESTEREL"* {A new method for compiling the Esterel language}. In Proceedings of GRAISyHM-AAA (Lille, France) (in French).

[10] Etienne Closse, Michel Poize, Jacques Pulou, Patrick Venier, and Daniel Weil. Saxo-RT: Interpreting Esterel semantics on a sequential execution structure. In Proc. SLAP'02, volume 65 of Electronic Notes in Theoretical Computer Science. Elsevier, 2002

.[11] Bertin, V., Poize, M., and Pulou, J. Sifakis *"Towards Validated Real-Time Software", Euromicro conference on Real Time Systems, Stokholm Suede, Juin 2000*

[12] *E. Closse, M. Poize, J. Pulou, J. Sifakis, P. Venier, D. Weil, and S. Yovine. Taxys : a tool for the development and verification of real-time embedded systems*

In CAV'01. LNCS 2102, Springer, 2001.