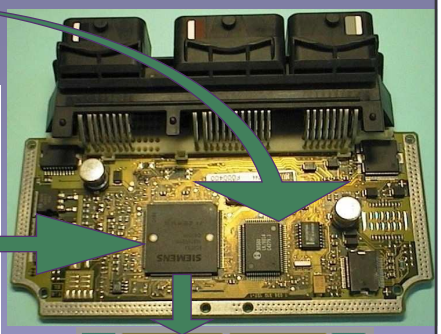
PSA PEUGEOT CITROËN

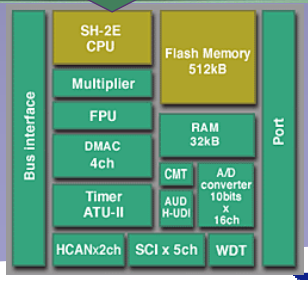
Automotive Safety Concepts : 10^{-9}/h for less than 100 € a piece.

Jean-Louis DUFOUR

Safety of Powertrain / Chassis electronics

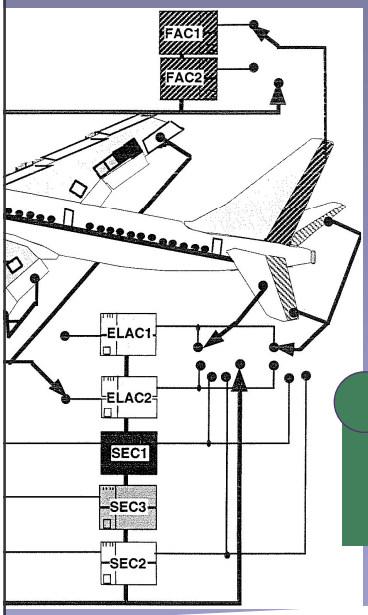
Automotive context (1/2)





PSA PEUGEOT CITROËN

Automotive context (2/2)

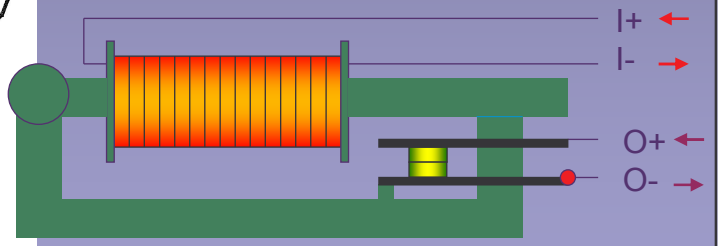


Fail-operational

either
or

Fault-tolerant

Fail-safe



PSA PEUGEOT CITROËN

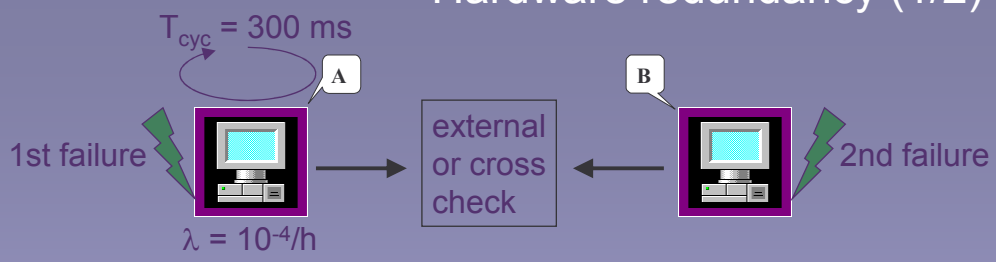
First Part

1. Classical safety concepts

2. Automotive safety concepts
3. IEC 61508 point of view

PSA PEUGEOT CITROËN

Hardware redundancy (1/2)



Question : Hazardous Failure Rate ≤ 10^{-9}/h ???

- **First failure : 2λ**
- **Second failure <u>before detection</u> : λT_{cyc}** (HYPOTHESIS : no common mode)

HFR = $2\lambda^2 T_{cyc}$

$\lambda = 10^{-4}/h$, $T_{cyc} = 10^{-4}$ h $\Rightarrow$ HFR = $2.10^{-12}/h$!!!

PSA PEUGEOT CITROËN

Hardware redundancy (2/2)

Question : has every fault an IMMEDIATE effect ???

Latent fault sites :

- **RAM of a railway onboard controller : emergency stop request**
- **FLASH/data of a wayside railway controller : curve and site of bends**
- **FLASH/code of an airliner : control of the undercarriage**
- **ALU of an ABS : unsigned multiply op. used for the unlocking duration**

- **…**
- **Second failure <u>before detection</u> : λT_{lat}**

⇒ **<u>2nd question : what is the maximum latency ????</u>**

« Latent fault hunter » : periodic self-test (HYP. : «exhaustive» enough)

$\lambda = 10^{-4}/h$, T_{lat} = 3 mn= 1/20 h $\Rightarrow$ HFR ≤ $2\lambda^2 T_{lat} = 10^{-9}/h$!!!

PSA PEUGEOT CITROËN

SW redundancy : (source) code diversity (1/2)

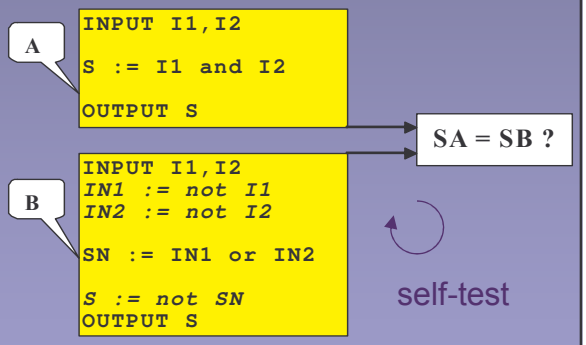
- **Failure : λ**
- **Common effect : p**

$\lambda = 10^{-6}/h$ & HFR $\leq 10^{-9}/h \Rightarrow p \leq 10^{-3}$

- Question : How to do ?
- More precisely : What about the **remaining common effects** ?

➔ *Answer (part 1) : self-tests*
- ➔ ***In the front line***
  - ☹ ***(very) CPU intensive***

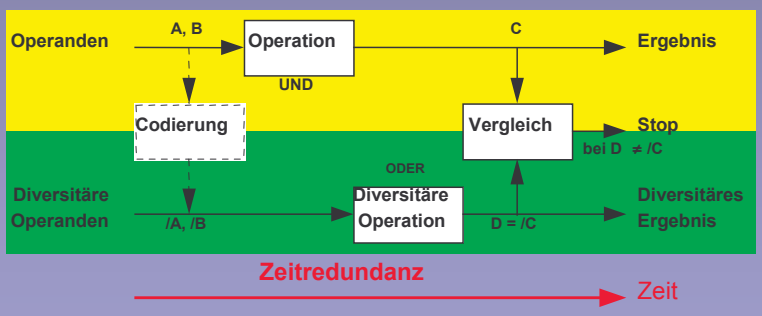
➔ *Answer (part 2) : fault injection*
- ➔ ***Fault model ?***
- ➔ ***Tests size ?*** (confidence interval)
- ☹ ***Industrial evolutivity?***



PSA PEUGEOT CITROËN

SW redundancy : (source) code diversity (2/2)

- **Use :**
  - European Railway (Sweden, France, … ?)
  - French nuclear propulsion (submarines, aircraft carrier)
- **Odd / Eccentric ?**



© Siemens

PSA PEUGEOT CITROËN

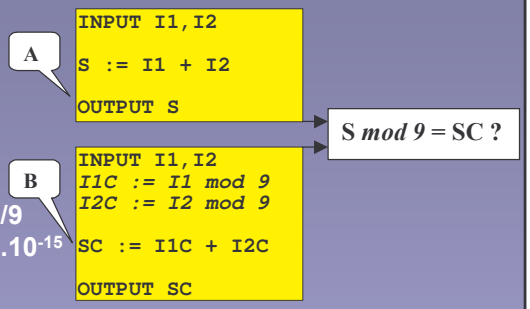
Software redundancy : (error-detecting) code

- Failure : λ
- Common effect : p

- « Coded processor »
  - Nothing to do with HW
- « to cast out the nines »

A = 9 => p = 1/9

A = (C5E975h, BAC239h) => p = 6.10^{-15}

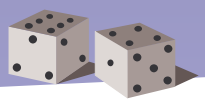


☹ 10 times slower, …

☺ … but NO NEED FOR SELF-TESTS !!!

2 independant discoveries :

- GRS (USA, now Alstom)
- Matra (Fr, now Siemens)
  - Meteor line (Paris), Canarsie line (N.Y.C.)



PSA PEUGEOT CITROËN

Summary

- **Even in the case HW redundancy, periodic self-tests are mandatory.**
- **Even with intensive self-tests, the front line is (some form of) redundancy.**

PSA PEUGEOT CITROËN

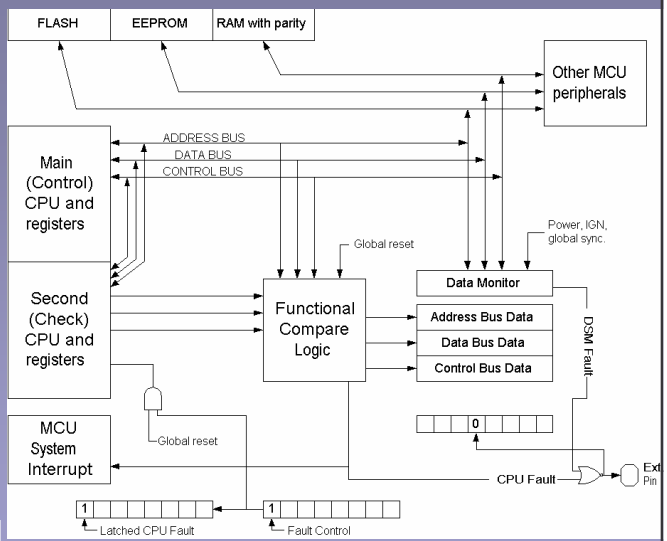
Second part

1. Classical safety concepts
2. **Automotive safety concepts**
3. IEC 61508 point of view

PSA PEUGEOT CITROËN

True redundancy in automotive computers

- **Small functions :**
  - Active sensors
    - Accel. Pedal
    - 2 ASICs
  - Intelligent sensors
    - Steering angle
    - 2 8-bits micros
- **Dual-core micros**
  - FLASH/RAM shared (price = chip area)
  - ☹ Very Specific
  - ☺ Safety level
  - Not very widespread (2 suppliers ?)



T. Fruehling *Delphi secured microcontroller architecture* SAE 2000-01-1052

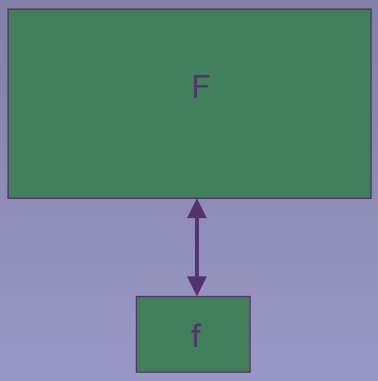
PSA PEUGEOT CITROËN

Asymmetric redundancy

- **f is an approximation of F**
  - F : 1000 lines, algorithms, 10 ms
  - f : 100 lines, look-up tables, 100ms

☺ **Safety level**

☹ **Safety micro application-dependent**
  ☹ 8-bits micro and Flash : inconsistent



PSA PEUGEOT CITROËN

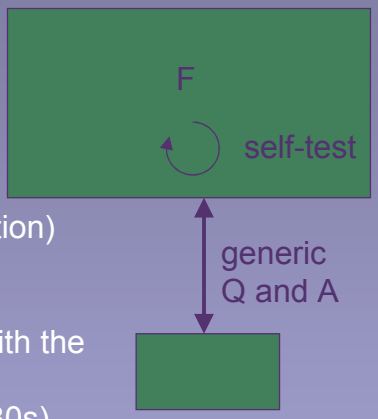
HW monitoring

- **F is no more duplicated**

⇒ **Relies only on HW monitoring :**
"don't wait for the effects of faults (on F), but look at the source (the HW)"
Wrong good idea !

☺ **Safety micro application-independent**

☹ **Safety level**
  ☹ are the hazardous faults (to the application) detected by the (generic) test ?
    ⇒ coverage rate
  ☹ If so, is the detection time compatible with the system effect ?
    ⇒ CPU load allocation (512K Flash : 30s)
  ☹ What about **transient faults** (more and more important with thinner and thinner VLSI geometries)
    ⇒ **no satisfactory answer !!!**



PSA PEUGEOT CITROËN

VDA recommendation (“Function monitoring”)

☺ **Safety micro application-independent**

- **What about common modes/effects ?**

⇒**As usual : self-tests**

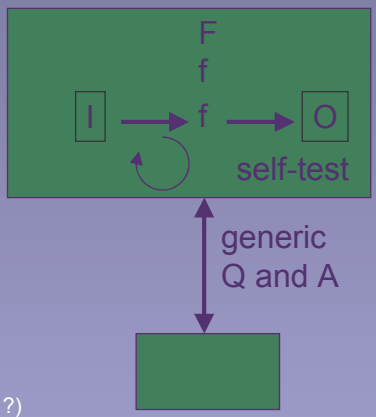
☺FLASH and RAM on f only

⇒**But also : online application tests !!!**

☺ “portable instructions test”

☺ 100% useful

☹Check the code coverage



“Standardized E-Gas monitoring concept for engine management systems of gasoline and diesel engines” V2.0 (2004-04-29)

- BMW DC VW Porsche Audi
- Basic concept comes from Robert Bosch GmbH (patents ?)

PSA recommendation :

PUT IT ON THE WEB !

PSA PEUGEOT CITROËN

Third part

1. **Classical safety concepts**
2. **Automotive safety concepts**
3. **IEC 61508 point of view**

Not presented in Braunschweig

PSA PEUGEOT CITROËN