4ème Atelier Thématique du RIS
"Nlles architectures & techno des processeurs et SdF"
Aix-en-Provence *20 novembre 2002*

CENTRE NATIONAL D'ETUDES SPATIALES

CNES fault tolerant architectures intended for electronic COTS components in space applications

Michel PIGNOL

CNES

DTS/AE/SEA/IL
18 avenue Edouard Belin
31401 Toulouse Cedex 4 - FRANCE
Tel.: +33 (0)5 61 27 43 61
michel.pignol@cnes.fr

CENTRE NATIONAL D'ETUDES SPATIALES

Outline

- Motivation with regard to electronic commercial components (COTS) embedded in satellites
- Needs for low cost fault tolerant architectures
- Presentation of two CNES low cost fault tolerant architectures
- Conclusion

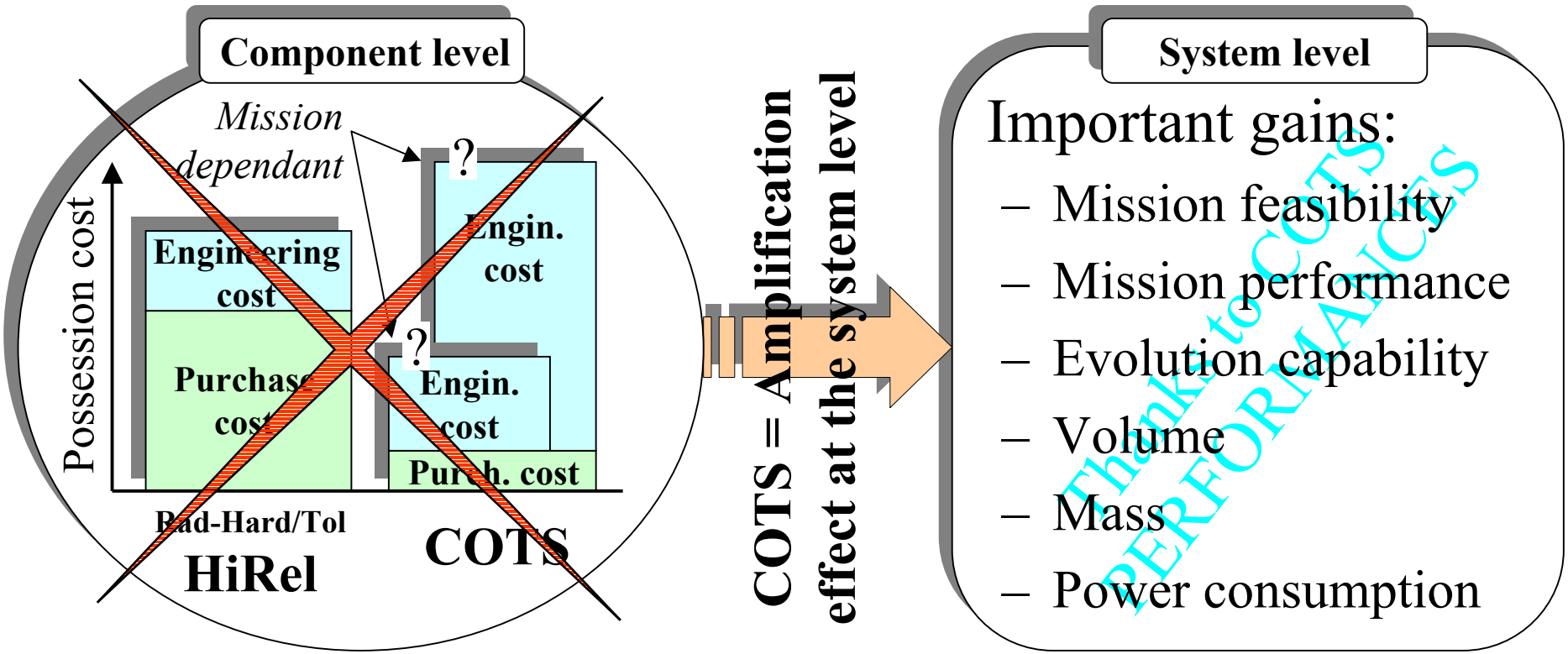
Motivation wrt HW COTS (1/2)

- ⇓ of choice in HiRel (RadHard - RadTol) ICs
  - ⇓ accelerated since W. Perry memorandum
- RadHard ICs perfo. << COTS perfo.
  - Ambitious satellite missions will require higher and higher performances
- Needs for next satellite generation
  - ⇓ mass / power consumption / cost / planning

A possible solution is:

☞ electronic commercial components (COTS)

Motivation wrt HW COTS (2/2)



☞ Main motivation = System level gains

Fault tolerant architecture needs

- Total integrated dose
  - COTS techno. OK ➪ ICs selection, local shielding
- SEL
  - COTS techno. OK ➪ ICs selection, local anti-latching system
- SEE (upset + transient inside combinational logic)
  - COTS are sensitive ➪ We have to live with!

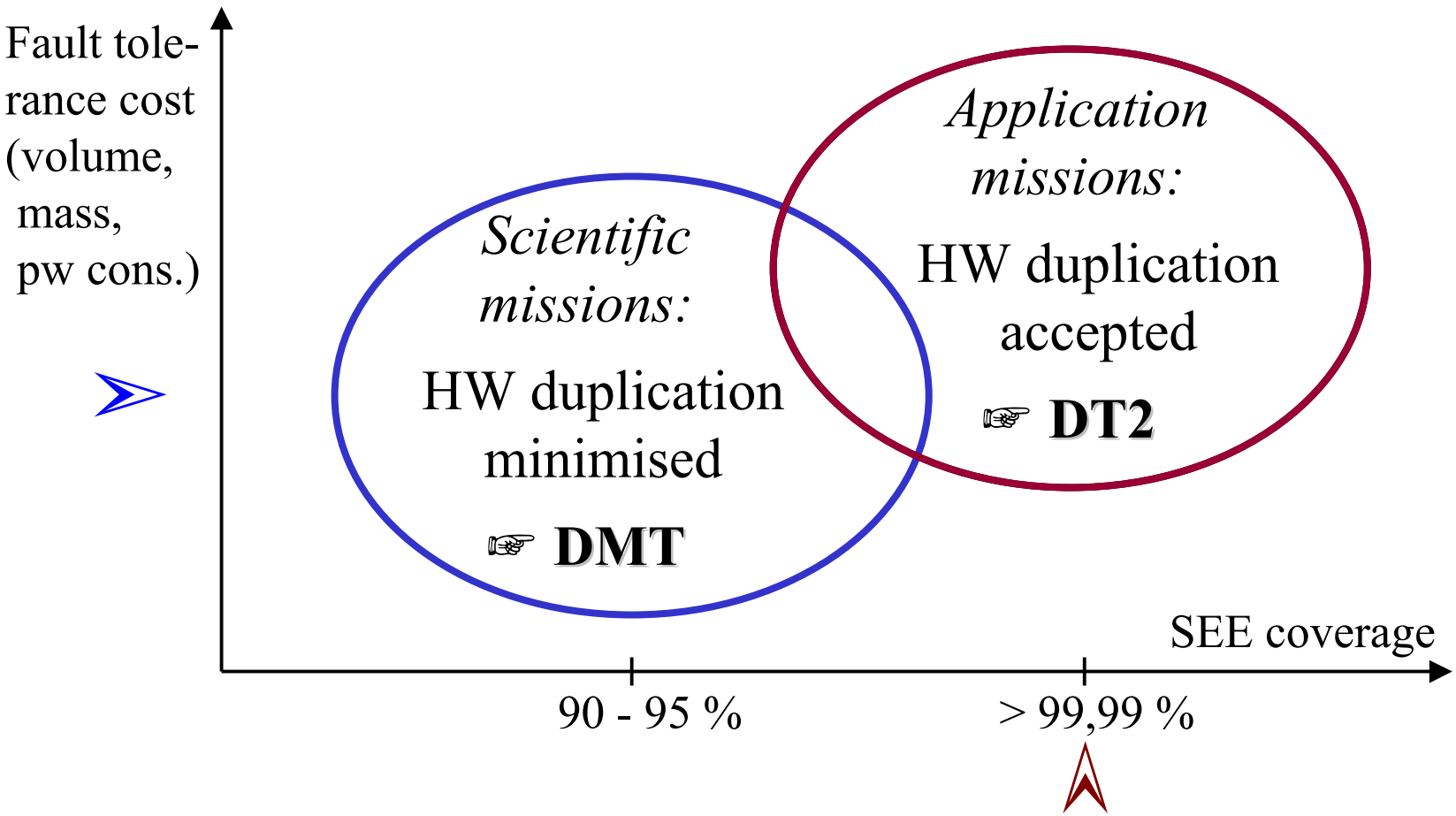
☞ HW COTS requires fault tolerant architectures

☞ Need for **low cost** fault tolerant architectures

Two CNES fault tolerant archi.

CENTRE NATIONAL D'ETUDES SPATIALES

Avoid "heavy" triplication



DMT key elements

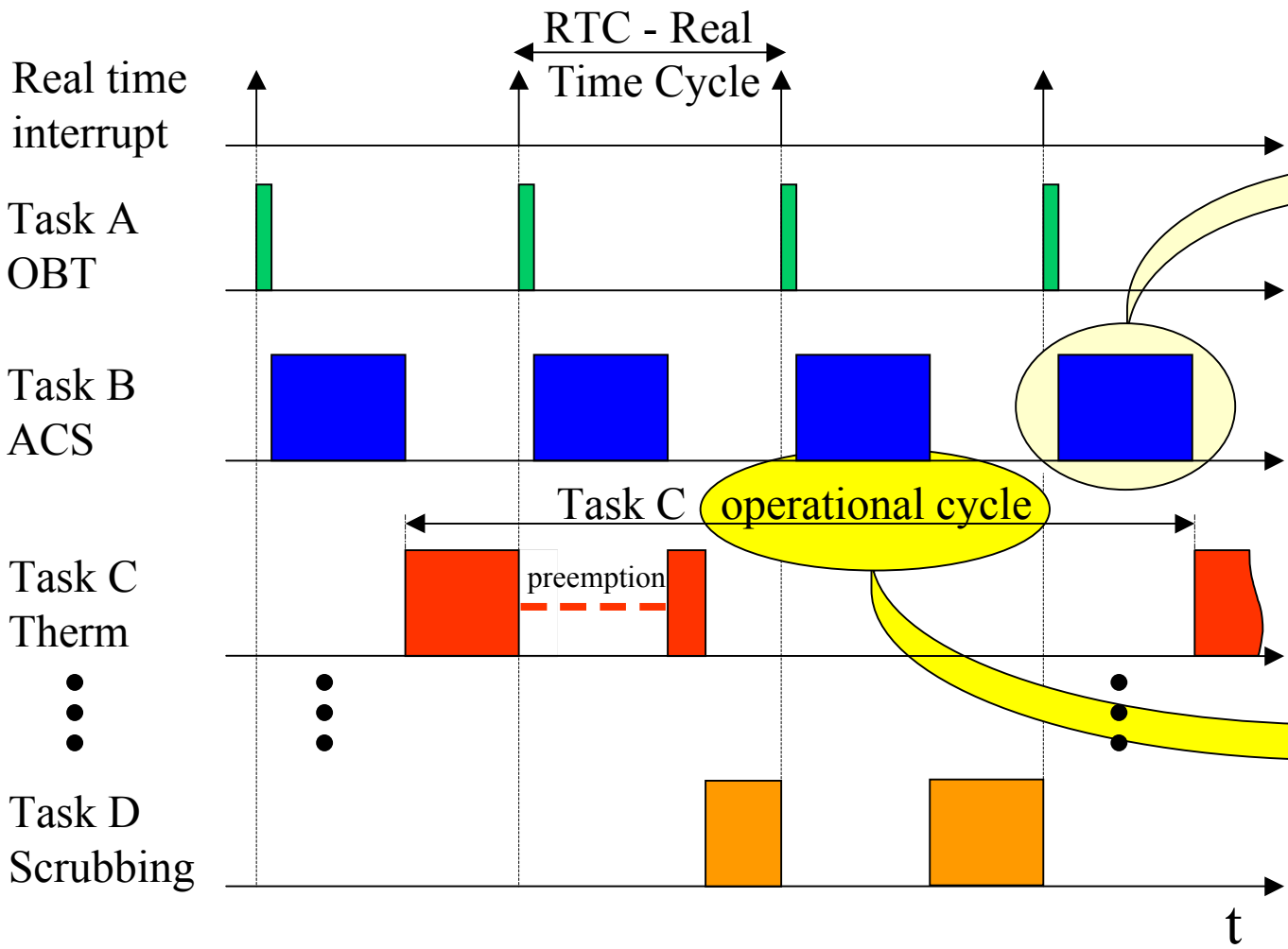
CENTRE NATIONAL D'ETUDES SPATIALES

DMT - Duplex Multiplexé dans le Temps (duplex in time)

- DMT technology = time replication
- Concept
  - Up-to-date COTS µP ➪ High processing perfo.
  - Detection ➪ Two virtual channels run on a single physical channel (a single µP)
  - Recovery ➪ Based on a safe context storage (safe wrt direct SEE and not accessible by a faulty µP)
  - Granularity for detect./recov. ➪ Macro-granularity

Macro-granularity

Simple example of a real time SW architecture:



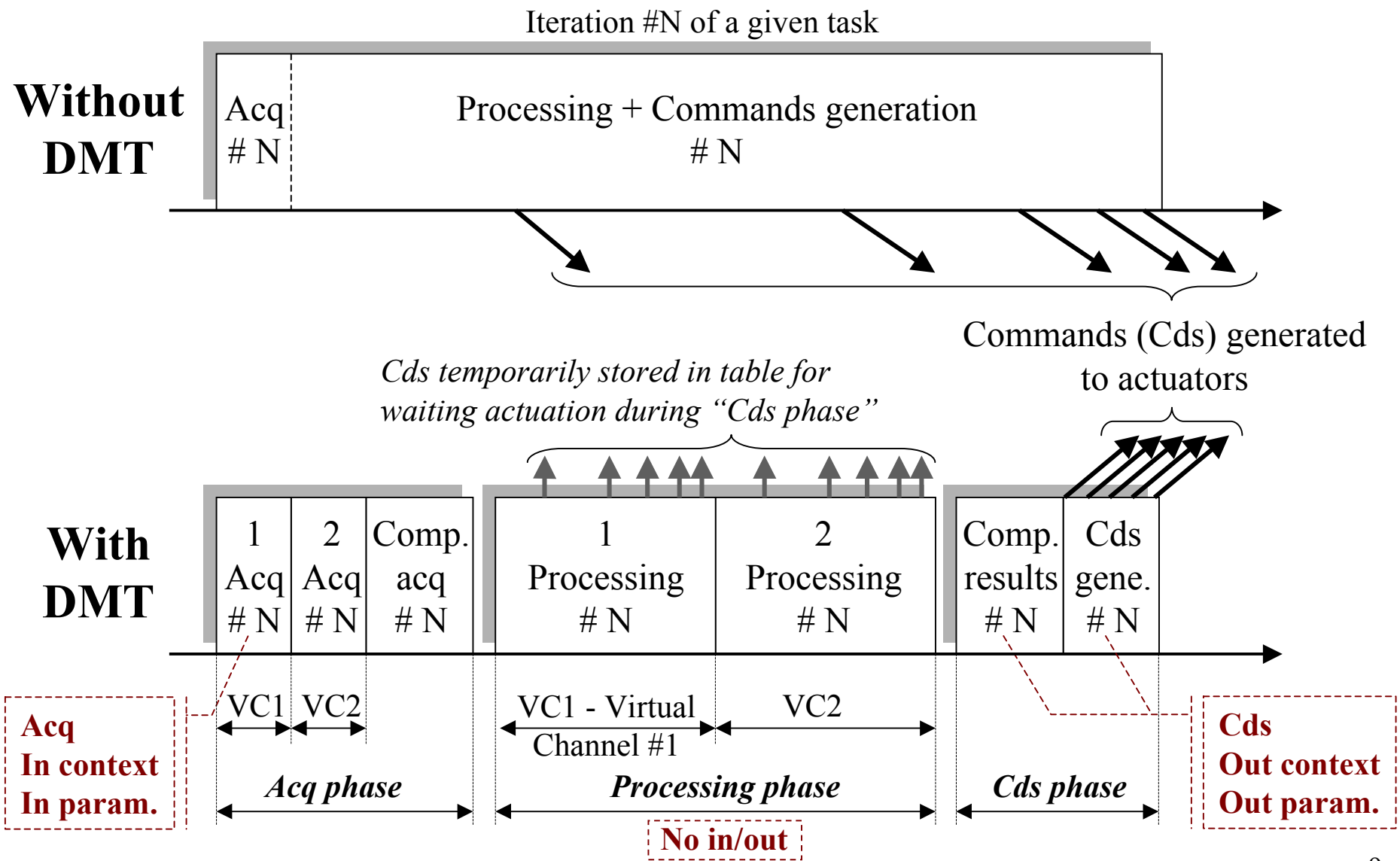
One iteration of a given task (see next slide)

Macro-granularity for detection and recovery

⇩

easiness of the implementation

Detection: DMT sequencing



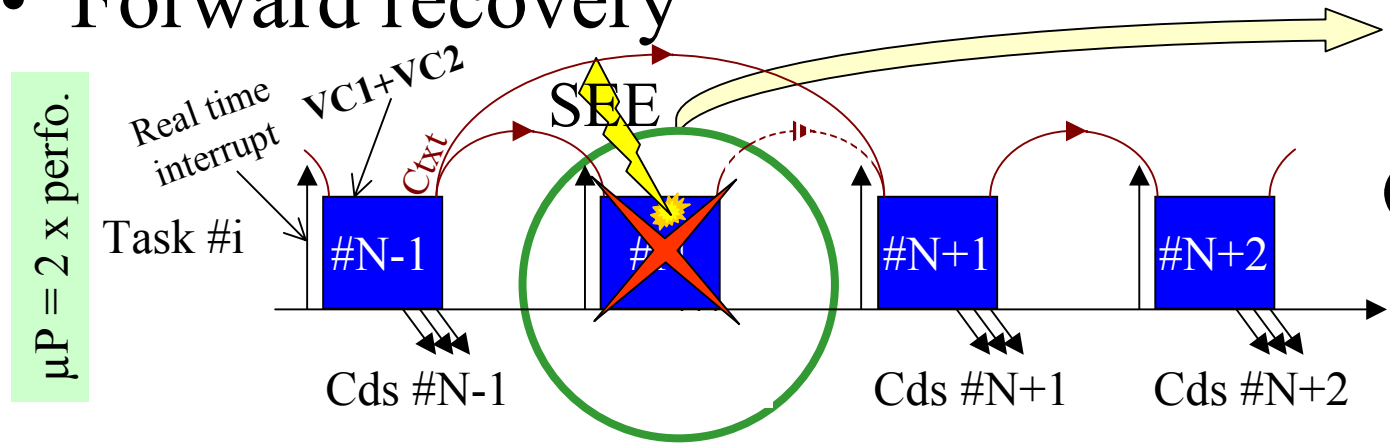
Problem of recovery wrt duplex

- A duplex is able to **detect**
  - comparison (cf. previous slide)
- A duplex is not able to **recover**
  - no information is available for determining which is the healthy/faulty channel (unlike within a triplex architecture)

☞ Specific mechanisms are required for implementing a **recovery** within a **duplex** architecture

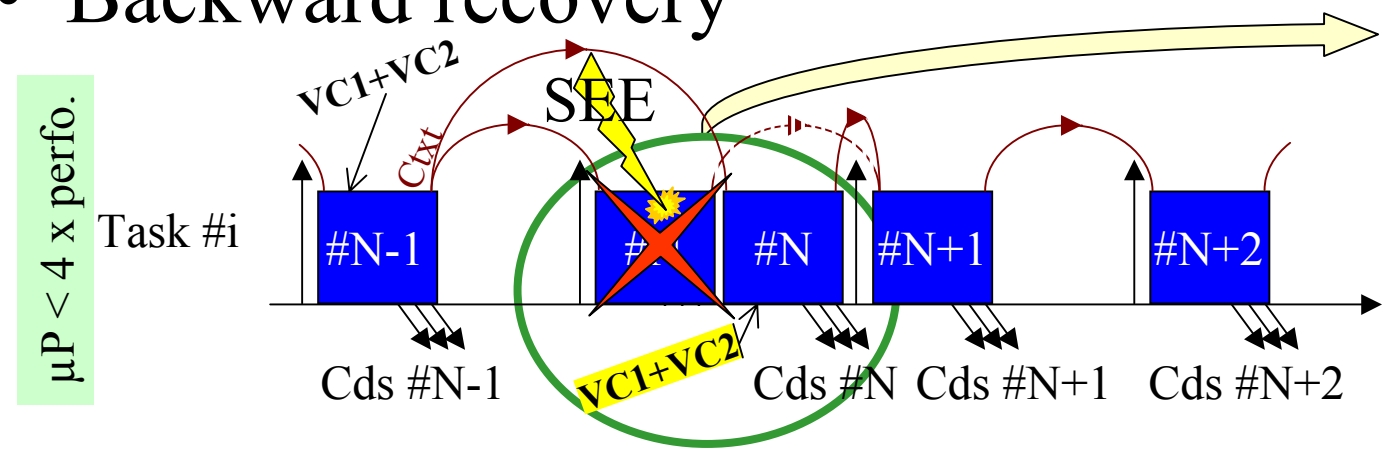
Two recovery modes

- Forward recovery



Cds #N are missing (e.g. tasks with control-loop)

- Backward recovery



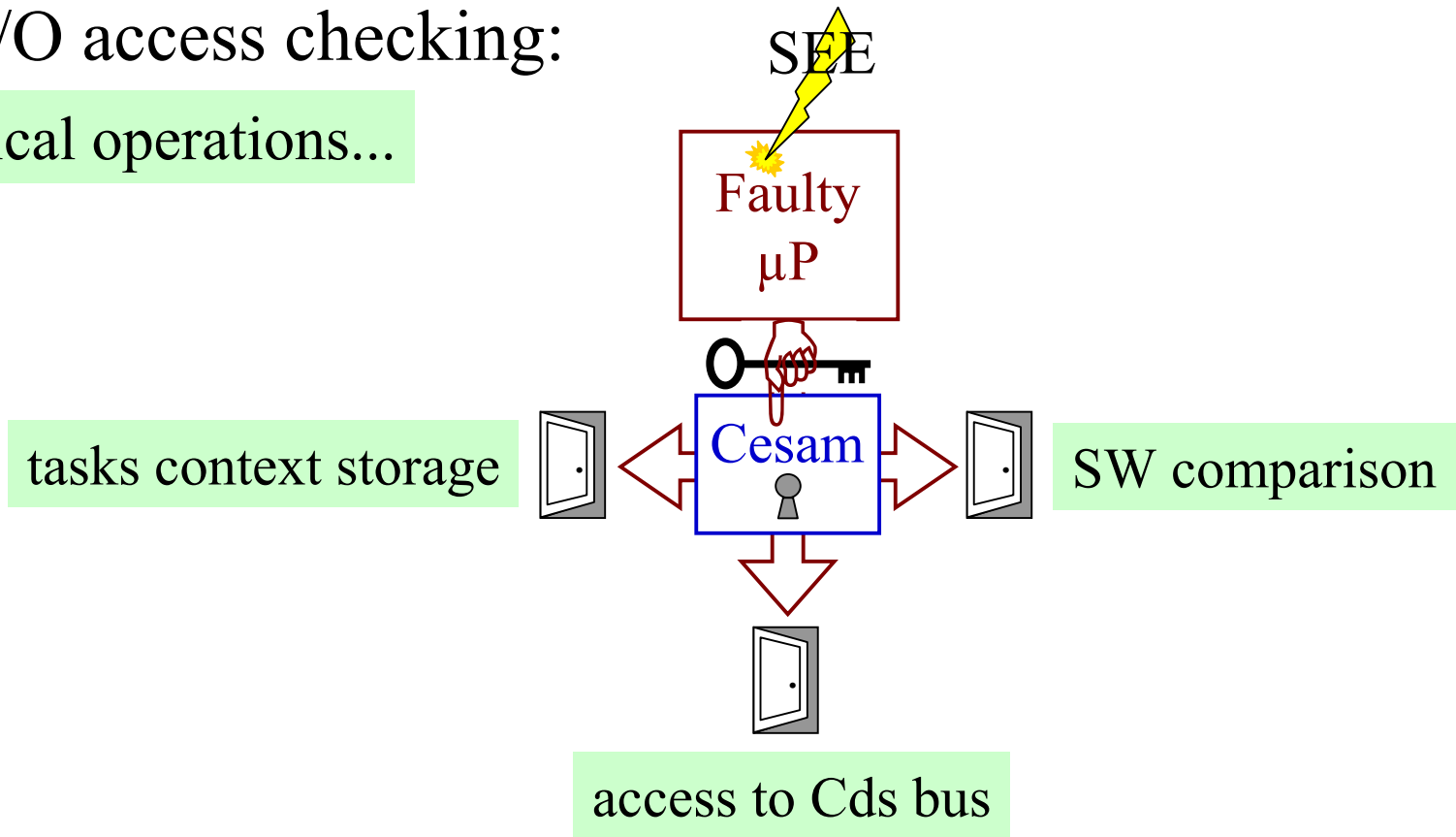
Iteration #N (i.e. VC1 + VC2) is played again (tasks having specific time relationship)

- Mix: forward and backward recovery

HW Address checking

- Mem & I/O access checking:

  Three critical operations...



… performed with a **high level of safety**, thanks to an HW address monitoring (FPGA / ASIC named CESAM, designed to be SEU free)

DMT features (1/2)

- Microprocessor impact
  - The SEE tolerance requires 50 % of the computing performance ...
  - … thus the µP must have twice the nominal computing performance
- Detection
  - SEE wrt acq. ➪ Acquisitions replication & comparison
  - SEE wrt processing ➪ Processing replication & comparison of the main processing results (task context, out parameters, Cds)
  - A single µP with error free comparison even in presence of faults [thanks to CESAM]
- Safety
  - Erroneous Cds can't be generated ➪ No Cds issued before a complete check of proces. results & HW monitoring [CESAM]

    Between "Cds computation" and "Cds generation", Cds are stored inside internal tables

DMT features (2/2)

- Real time recovery
  - A given iteration of a task where an error is detected:
    - is cancelled (**forward recovery**) ➪ It is like if the iteration #N of this task is missing, the task having an "hole" inside its commands generation cycle (typically for tasks with "control loop algorithms")
    - or is executed again (**backward recovery**) ➪ But, in this case, the µP must have up to 4 time the computing perfo. (typically for tasks having specific time relationship not compatible with one RTC delay)
  - Mix: e.g. task#i with forward, task#j with backward
  - Recovery modes are allowed thanks to a safe storage of context data [thanks to CESAM]
- I/O must be centralised at the beginning (for acquisition) and at the end (for actuation) of each task

DMT performances

- Tolerance performance
  - Fail operational: > 95 % (measured)
  - Fail op. if ETR protected: > 98 to 99 % (theory)
  - Fail safe: > 99,99 % (theory, measure in course)
- DMT requires a µP having about twice the nominal computing performance
- The recurring cost is not impacted by DMT
- The SW development cost is impacted, but not a lot thanks to a "DMT pre-compiler"

DT2 key elements

CENTRE NATIONAL D'ETUDES SPATIALES

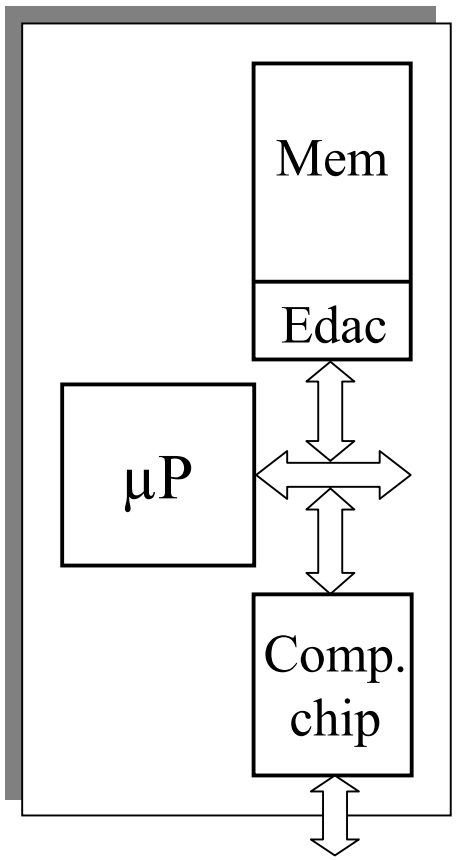
DT2 - Dual Duplex Tolerant to Transients

- DT2 technology = macro-synchronised master/checker archi. & minimal HW duplic.
- Concept
  - The duplication is limited to the PUC (Processing Unit Core) ➪ µP + companion chip + µP's mem
  - Detection ➪ Two minimun physical channels (PUC)
  - Recovery ➪ Based on a safe context storage (safe wrt direct SEE and not accessible by a faulty µP)
  - Granularity for detect./recov. ➪ Macro-granularity

DT2 architecture

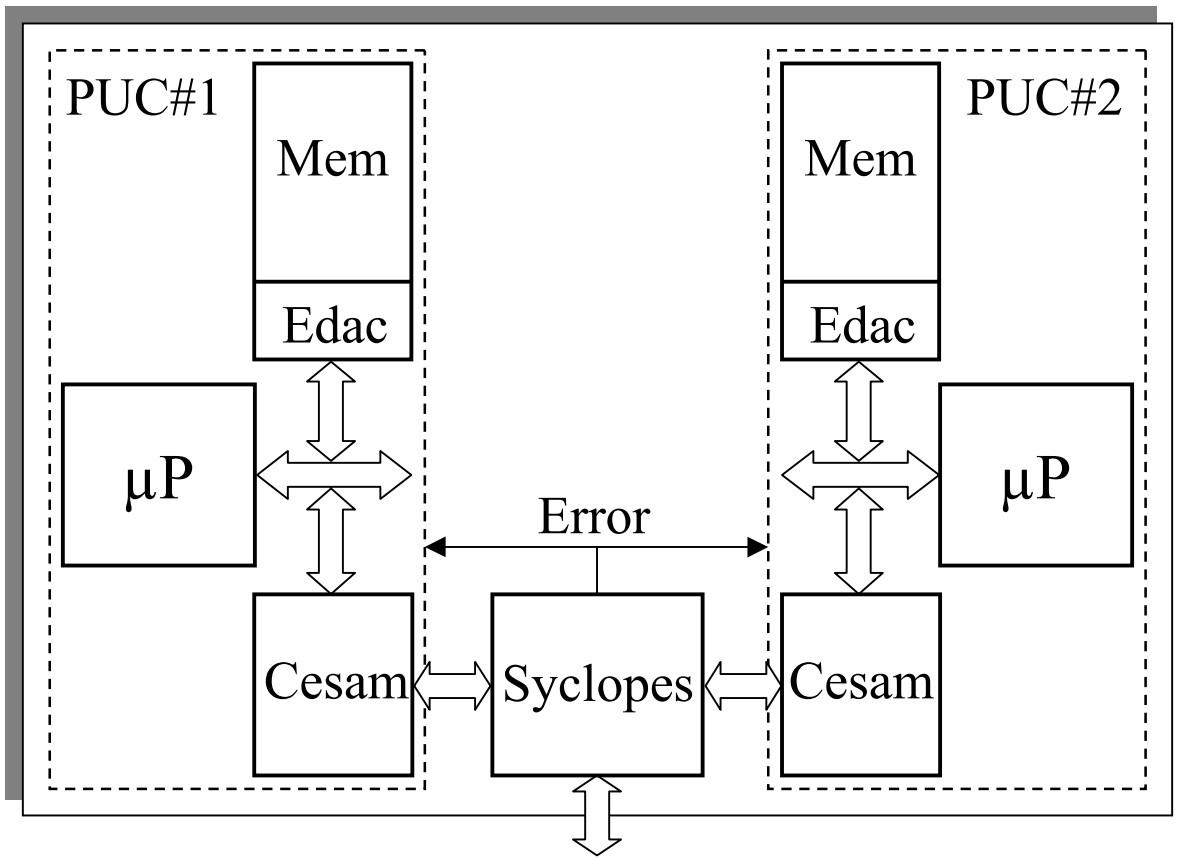
CENTRE NATIONAL D'ETUDES SPATIALES

PUC without DT2



Other parts
(Bckpl bus - I/O bus)

Processing Unit Core with DT2



Other parts of the computer
(Backplane bus - I/O bus)

DT2 features

A large part of DMT features are also true for DT2 except the following ones:

- Microprocessor impact
  - No more impact on the µP computing performance but …
  - … the SEE tolerance requires 50 % of the total computing perfo.
- Detection
  - SEE wrt processing ➪ Processing duplication & comparison of the main processing results (task context, out parameters, Cds)
- Memory and I/O access checking
  - Limited to the tasks context storage function
- CESAM (Mem. access check) / SYCLOPES (Synchro. & Comp. & I/O)
  - FPGAs / ASICs designed to be SEU free

DT2 performances

- Tolerance performance
  - Fail operational & safe: > 99,99 % (theory)
- The recurring cost is a little bit increased by DT2, but less than an “heavy” triplex
- The SW development cost is less impacted than with DMT
- The protection of a COTS RTOS needs specific mechanisms (CNES mechanisms validation through breadboard in course)

Conclusion

- Main motivation for HW COTS is system level gains
- **Low cost** fault tolerant architectures are required to be able to embed electronic commercial components inside satellites
- The CNES **DMT** and **DT2** patented architectures minimise costly HW expansion; SW impact (mainly for DMT) is reduced thanks to a “pre-compiler”
- **DMT** and **DT2** don’t require costly developments
- **DMT** and **DT2** are application generic