CNES Developments for COTS-based Spacecraft Supercomputers

Michel Pignol
CNES - Toulouse - France
michel.pignol@cnes.fr

Very deep-submicron COTS (Commercial Off-The-Shelf) components are attractive for space applications due to their high performances. However, computer designers will need to solve a main problem as regards their SEE (Single Event Effect) sensitivity.

CNES (the French Space Agency) studies on COTS-based computers are primarily oriented, but not limited, to low-cost missions and to payloads for large scientific missions. These studies have led to the development of two 'light' architectures, **DMT** and **DT2** [1] [4]. These architectures complement more conventional solutions such as e.g. TMR (Triple Modular Redundancy) one and offer a broad range of solutions for projects, thus constituting a fault-tolerant toolbox making it possible to adapt to the specific characteristics and requirements of each type of space mission.

COTS-based solutions complement rad-hard microprocessors and FPGA / ASIC developments.

The upset rate of recent microprocessors remains relatively low, and low-end applications does not required the entire processing capability of such components. This has led CNES to patent the **DMT** architecture ('**D**uplex **M**ultiplexed in **T**ime') [2], primarily intended for but not limited to small-satellites and scientific missions. The DMT architecture is a very low-cost fault-tolerant architecture based on time replication, and compatible with all COTS microprocessors.

A coarse granularity has been selected: the checking procedure is started at the end of each iteration of each software applicative task.

The DMT hardware architecture consists of a single physical channel (i.e. a single microprocessor) without hardware duplication. It is of SIFT (Software Implemented Fault Tolerance) type: an extra hardware function developed to be SEE-free and called CESAM is the only hardware support required.

The approximately theoretical performance of DMT protection against transient faults is 90 to 95 %.

For a single-task (resp. multi-tasks) application, the DMT architecture requires a microprocessor with a performance 4 (resp. 3) times greater than the nominal requirement.

For certain scientific or application missions, the main priority is to obtain a good availability performance, although not necessarily as high as that of a TMR system. This has led CNES to patent the **DT2** architecture ('**D**ual **D**uplex **T**olerant to **T**ransients') [3] based on a mini-duplex structure, and compatible with all COTS microprocessors.

The DT2 architecture is a low-cost and high-performance fault-tolerant architecture: duplication is limited to the PUC (Processing Unit Core), i.e. microprocessor, companion chip and memory. Fault detection is based on two physical channels (i.e. two PUCs) operating like a mini-duplex system, with each PUC running the same software code simultaneously (but asynchronously, using its own memory and companion chip).

The performance of DT2 protection against transient faults is approximately 99.9 %.

In the DMT / DT2 duplex architectures, the recovery capability is of checkpointing type.

References

[1] M. Pignol, "DMT and DT2: Two CNES Fault-Tolerant Architectures Developed by CNES for COTS-based Spacecraft Supercomputers", *Proc. 12th IEEE Int. On-Line Testing Symp. (IOLTS)*, July 10-12, 2006.

[2] M. Pignol, "Processing procedure for an electronic system subject to transient error constraints and a memory access monitoring device", patent US 6 839 868 B1.

[3] M. Pignol, "Software system tolerating transient errors and control process in such a system", patent US 7 024 594 B2.

[4] M. Pignol, "Methodology and Tools Developed for Validation of COTS-based Fault-Tolerant Spacecraft Supercomputers", *Proc. 13th IEEE Int. On-Line Testing Symp. (IOLTS)*, July 8-11, 2007.