HIGH RELIABILITY COTS BASED COMPUTER, STEP 2 (PROTOTYPING AND VALIDATION)

This project is the continuation of previous ESA Contract 21863/08/NL/GLC "Hi-Reliable COTS Based Computer", in the frame of which the overall computer has been studied, having as reference application a platform control computer of a satellite. During this Phase 2, the activities focused on the development of the Processing Module.

The Processing Module, based on the powerful PC7448 processor actually represents a General Purpose High Performance Processing Module, suitable for a wide range of applications, either in Platform or Payload computers, when a high amount of processing power is needed. As such it can find application in various areas, such as:

- Hi-Rel Platform Computers
- Any application requiring high processing performances
- Earth Observation and Payloads
- Scientific Payloads
- Planetary exploration Computers

The main elements constituting the Processing Module are:

- The PowerPC PC7448 CPU running at 1GHz thus resulting in 2300 MIPS (Drystone 2.1) processing performance.
- The Bridge FPGA implementing high speed interfaces and working memory controller. The High speed interfaces include 6 SpaceWire Links operating at 200 Mbps and 2 High Speed Serial Links operating at 1 Gbps.
- Health Control FPGA implementing fault mitigation and control functions, as well as non volatile memories interfaces.
- The Memories including 512 Mbytes working memory RSE protected DDR-II type and 32 Mbytes NOR Flash for SW Storage.

Benchmarks have been run while an heavy IO traffic on SpaceWire and HSSL Links was activated. No difference from those without I/O traffic as been detected, confirming the good architecture and design of the board, granting adequate bandwidth to all memory users.

An extensive test campaign has been carried-on on the PM Board using specific versions of benchmarks and through faults injection into CPU in order to evaluate the system capability to recover from induced malfunctions. The benchmark software is protected from Single Event Upsets that may affect the processor during software execution using a combination of time redundancy and watchdog. Two types of recovery operation are possible when an error is detected: Backward recovery where the execution of the benchmark is restarted and Forward recovery where a new instance of the benchmark is executed and the outputs generated by the three benchmark instances are voted according to a majority scheme. As result of this activity, we could observe the percentage of faults injected causing no effect on the processing results, to rise from about 70 % on plain code to more than 92% on mitigated code.