Paper ID: 47503
oral
student

25th IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Generic Technologies for Nano/Pico Platforms (6B)

Author: Mr. Reinhard Zeif
Graz University of Technology (TU Graz), Austria, reinhard.zeif@tugraz.at

Mr. Maximilian Henkel
TU Graz, Austria, henkel@tugraz.at
Mr. Andreas Johann Hörmer
Graz University of Technology (TU Graz), Austria, hoermer@tugraz.at
Mr. Manuel Kubicka
Graz University of Technology (TU Graz), Austria, manuel.kubicka@tugraz.at
Mrs. Manuela Wenger
Graz University of Technology (TU Graz), Austria, manuela.wenger@tugraz.at
Prof. Otto Koudelka
Graz University of Technology (TU Graz), Austria, koudelka@tugraz.at

THE REDUNDANCY AND FAIL-SAFE CONCEPT OF THE OPS-SAT PAYLOAD PROCESSING PLATFORM

Abstract

The ESA OPS-SAT Satellite Experimental Processing Platform (SEPP) is a highly integrated high performance embedded payload system. Its outstanding computational power allows the execution of any type of on-board experiments during the OPS-SAT mission. This implies the ability to control and monitor all other payload systems that are used for experiment execution, ground communication, software update, file transfer and data processing. The heart of the SEPP is a multi-purpose high performance System-on-Chip (SoC) integrated circuit (IC) that consists of a built-in dual core 800 MHz ARM Cortex A9 CPU and a Field Programmable Gate Array (FPGA).

Due to the importance of the SEPP for the mission it was decided to implement advanced fail-safe and redundancy concepts. An important aspect of the SEPP design was the realization of a failure tolerant system that uses a hierarchical fault detection and mitigation strategy. Different levels of power supply, data interface and component failure protection and detection methods were realized. Another aspect was the introduction of a safe board level redundancy concept that guarantees mission success even if one mainboard has a critical hardware failure.

As basis, a modular stack with redundant mainboards and peripheral boards was introduced. The resulting SEPP module contains at least two identical mainboards that can be operated in so-called cold redundancy (CR) or dual modular redundancy (DMR). In CR mode only one mainboard is enabled while the others are spare parts that are used only in case of a critical hardware failure. DMR means that one mainboard monitors another mainboard and takes over control if a failure is detected. This concept typically includes error detection and failure handling methods based on status information exchange between both mainboards.

On the circuit level, each SEPP mainboard contains advanced power protection and monitoring components that generate warnings or fault events if the circuits do not operate nominally. All SEPP interfaces are protected by special data bus switches that connect or disconnect the mainboard from the payload bus whenever required. Different types of memories for on-board software and data storage provide together with the built-in error detection and failure mitigation techniques of the SoC another layer to improve the fault tolerance and redundancy.

All these concepts are highly flexible and provide powerful features to guarantee fail-save operation and robustness of the OPS-SAT SEPP system.