# Study and development of fault tolerant operating systems for aerospace applications

Summary

**Candidate**:
Salvatore Gabriele La Greca
**Supervisors**:
prof. Luca Sterpone
ing. Daniele Rizzieri
ing. Sarah Azimi

July 2022

In the last few years, the number of missions devoted to the exploration of the universe has increased. Predictions show that the number of missions in the current decade is expected to be almost three times the number of missions in the previous decade, without considering low-cost and low-weight missions, like the ones including CubeSats. Therefore, the number of electronic devices and the job complexity assigned to them is increasing as well.

Electronic devices must be tailored to work in a reliable way. Whatever is the purpose of a spacecraft, from the smallest one to a complete rover exploring another planet. Particularly, in a complex environment like space, where there are many disturbances such as diverse temperature variations or radiations. The latter is one of the most common causes of failure in spacecrafts and greatest enemy of electronic components. Thus, a system needs to be as dependable as possible. The dependability of a system is mainly affected by aspects like reliability, availability and safety, especially for space applications.

Nowadays, FPGAs is increasingly being used in aerospace applications due to their flexibility. The flexibility given by this kind of hardware is a key aspect in the success of a mission because of their high costs, high duration and high complexity. As an example, the Mars Perseverance Rover is almost based on FPGAs. In this rover, one FPGA can be found in the automatic entry unit. This unit is responsible for the automatic entry, descent and landing on Mars. Once the rover is landed, this unit would be useless and would become a dead hardware. However, it is based on a FPGA hardware so it has been reprogrammed by NASA engineers from Earth to handle computer vision tasks.

Consequently, this thesis aims to develop some techniques to create FPGA designs tolerant to "Single Event Upset" faults (that are very common, especially in FPGAs). Taking this into consideration, the proposed solution aims to detect faults caused by SEUs in the Xilinx Microblaze CPU by using a custom peripheral. The custom peripheral has been developed in order to be fault-tolerant itself thanks to a Triple Module Redundancy design.

Finally, when a fault is detected, a partial reconfiguration of the FPGA is triggered. This action will upload a partial bitstream only in a subportion of the FPGA, aiming to reconfigure only the CPU area of the design and to restore the original behaviour. This partial reconfiguration

allows to achieve a faster down-time, and consequently a higher availability of the system. This process is entirely managed by the DFX (Dynamic Function Exchange) Controller IP. The DFX Controller loads the configuration file from the memory and sends it to the configuration port of the FPGA.

Moreover, a custom script has been developed providing to designers and developers an easy and most automatized way to convert an existing Xilinx design into a design that supports the partial reconfiguration of the Microblaze.