Design of a dependable RISC-V processor for safe and secure applications in collaboration with ESA-ESTEC

Current advances of computing architectures and VLSI technology has ushered the so-called digital revolution bringing the ubiquitous presence of embedded computing cores in every aspect of our lives. Therefore, the sheer number of devices makes the introduction of design for reliability techniques quite important as, even with a small probability of failure, the failure of many potentially safety critical devices becomes unavoidable. Furthermore, in most cases, the devices are interconnected in what is called the "internet of things" thus opening them also to potential security related attacks.

The proposed activities can be framed in several different related threads that will investigate of **dual purpose modifications** (e.g. for both security and reliability enhancement) to an open core RISC-V architecture

The following thesis projects are available:

1. Introduction of techniques to increase reliability by detecting and correcting random or maliciously induced errors in the control flow (DUE: detected unrecoverable error) to prevent exceptions and system hangs/crash
2. Introduction of techniques to increase reliability by detecting and correcting random or maliciously induced errors in the data flow (SDC: Silent Data Corruption) to prevent unintended and potentially harmful execution of the programs
3. Setup and execution of irradiation campaigns (e.g. neutrons protons or heavy ions) to validate the vulnerability of DRAM and emerging memory technologies and definition of ad-hoc techniques for the memory controller to mitigate these effects.
4. Setup and execution of irradiation campaigns (e.g. neutrons protons or heavy ions) to validate dependability techniques in a RISCV architecture using a flash based FPGA (whose configuration memory could be considered immune to soft errors)

The proposed activities will be carried out in collaboration with ESA-ESTEC Noordwijk.