PhD Seminar Talk-1

Fault Tolerant Control Path Design
using Evolvable Hardware for Space Applications

Deepanjali.S (CS21D0001)
Research Scholar, Department of Computer Science and Engineering
Indian Institute of Information Technology Design and Manufacturing, Kancheepuram

October 12, 2023

Abstract

Digital systems operating in Lower Earth Orbit (LEO) confront heightened risks of Single-Event Transient (SET) errors due to ionizing particles. The downsizing of electronics has led to operating voltages lower than those experienced in space. These particles can impact sensitive nodes, such as logical components, resulting in transient bit flips in memory elements, commonly called Single Event Upsets (SEUs). SEUs predominantly manifest during circuit operation. Given the inevitability of memory elements in control path hardware implementation, a compelling need exists to propose mitigation approaches to safeguard control path elements. This is crucial as a bit-flip in the control path can give rise to erroneous control signals or faulty operations, potentially leading to mission failure. From an architectural perspective, the control path hardware design falls into two categories: Hard Wired Control (HWC) circuit and Micro-Programmed Control Unit (MPCU). The design approaches differ significantly in terms of how control signals are generated. In HWC, a sequential circuitry approach generates control signals, while in MPCU, a stored memory concept is employed, storing control bits for individuals or groups of instructions in the control store. Consequently, distinct mitigation methodologies are selected to address SEU and Multiple Bit Upset (MBU) for both implementations simultaneously. The fault recovery procedure in HWC is exponential, necessitating a bio-inspired approach for effective transition from a faulty to a non-faulty state. This motivates the utilization of Evolutionary Algorithms (EA) for upset mitigation in HWC. In high-security applications employing Evolvable Hardware (EHW), native reconfiguration proves impractical due to encrypted configuration memory and limited tools for accessing configuration bits. Consequently, an essential alternative reconfiguration technology, Virtual Reconfigurable Circuit (VRC), is employed for native reconfiguration at the application level. Our research addresses challenges in standard VRC architecture, such as Extensive VRC architecture and Non-Partial Reconfiguration, enhancing scalability and acceleration for effectively mitigating both SEU and MBU in control path hardware.