A tool for static instruction set architecture analysis

Peer Adelt¹, Bastian Koppelmann², Wolfgang Mueller², Bernd Kleinjohann¹, Christoph Scheytt²

¹C-LAB / ²Heinz-Nixdorf Institute
Fürstenallee 11, D-33102 Paderborn

E-Mail: {firstname.lastname}@upb.de

Safety critical embedded applications are often required to be tolerant or resistant against soft errors, that do not damage the hardware but may adversely affect the software. Soft errors may originate from Single Event Upsets (SEUs), which often manifest themselves as bit flips that change the content of memory cells or registers leading to incorrect data or control flow behavior. Fault effect simulation is a technique to verify the fault tolerance or fault resistance by injecting faults into the system and investigating, how these faults propagate to observable failures at the output.

As such, the effects of binary software are highly dependent of the underlying hardware platform at register level. We focused our research on fast mutation based fault effect simulation with bit flips in target specific binary programs for execution on a virtual prototyping platform. To produce meaningful platform dependent bit flip mutations, we developed a tool for static instruction set architecture (ISA) analysis. It provides an interactive graphical interface, which indicates general and detailed ISA specific statistics of 1-, 2- and 3-bit flip mutations in opcode, data, and address sections of the instructions and their impact on the program execution.

With ISA details as input, our tool analyses all 798 instructions of the TriCore™ microcontroller architecture for mutations of their binary representation. In this context, we also show the tool as a front-end to generate bit flip mutants for automatic fault effect simulation of a TriCore™ binary program in full system mode of the QEMU CPU emulator.