SCHAEFFLER

Leibniz Universität Hannover

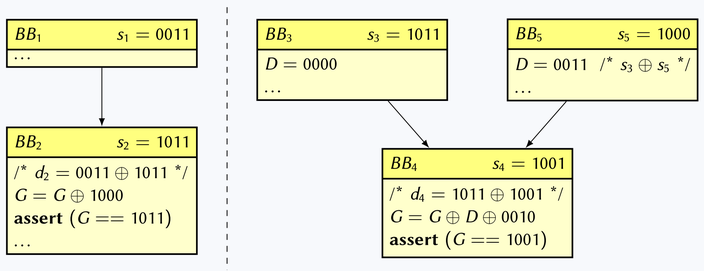
FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

FACULTY OF ENGINEERING

# Demystifying Soft-Error Mitigation by Control-Flow Checking
# A New Perspective on its Effectiveness

Simon Schuster[1], Peter Ulbrich[1], Isabella Stilkerich[2], Christian Dietrich[3], Wolfgang Schröder-Preikschat[1]

## Trailhead

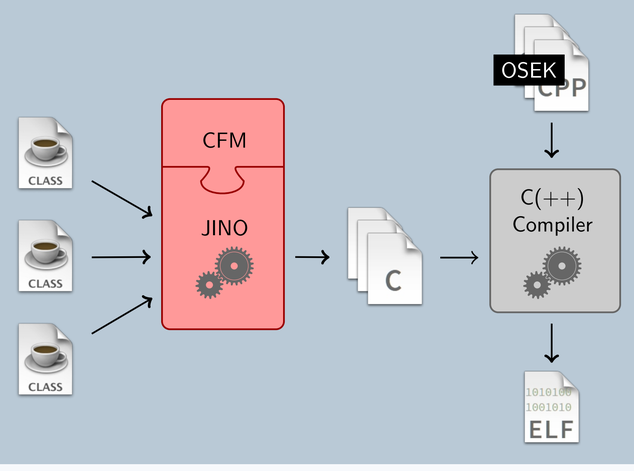


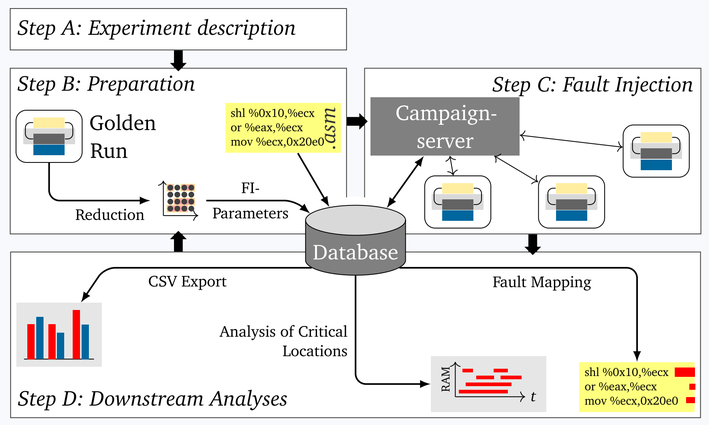

### Motivation

**Soft errors are an urging problem** in the domain of safety-critical embedded systems. For decades, **control-flow checking schemes** have been investigated and improved to mitigate soft-error effects for control-flow faults and **are strongly recommended by current industrial standards**.

### Testbed: KESO Multi-JVM for OSEK-based Systems

- Source-to-source compiler: JVM bytecode to C
- Common ground for our case study on CFC schemes
- Automated application analysis and CFC weaving

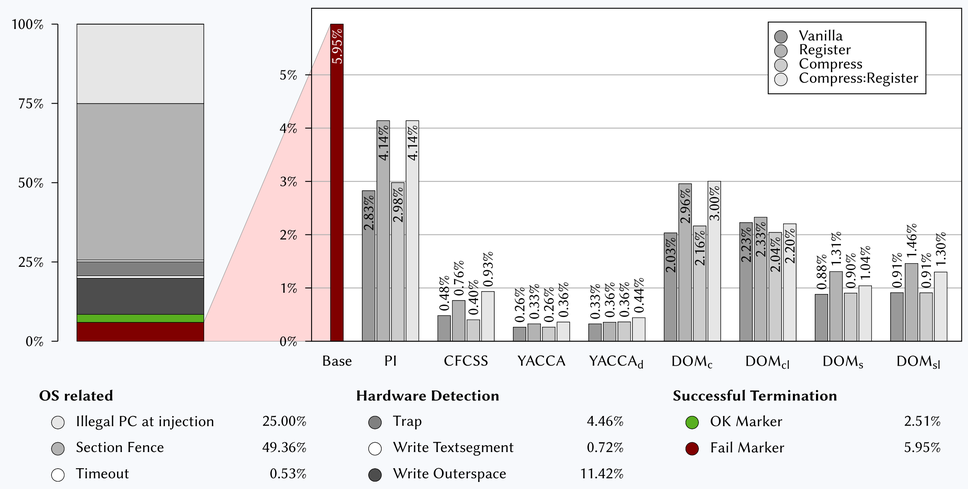



### Fault-Injection Methodology

Based on the FI framework Fail*, a **simulator-based approach** that **performs a full scan** of all relevant registers, memory locations and values (i.e., fault space) at ISA level.

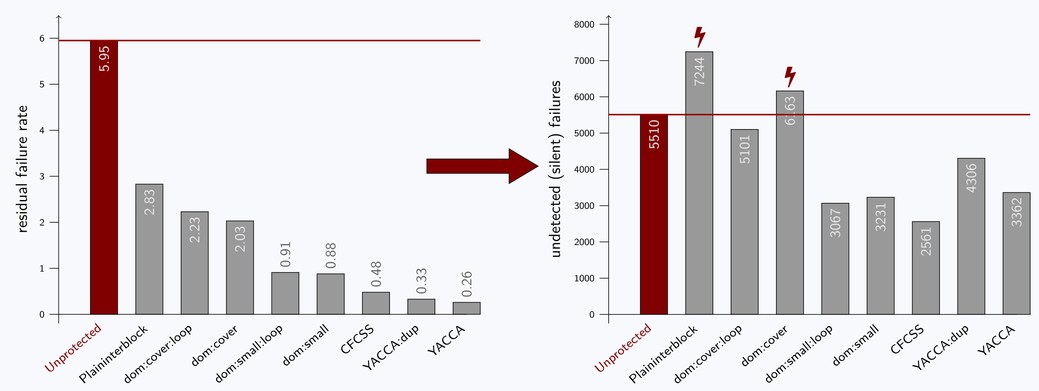
## State-of-the-Art: Relative Failure Counts




### Reevaluation with Residual Failure Rates

Results **match literature and apparently demonstrate the effectiveness** of software-based CFC on faults not caught by OS and hardware.

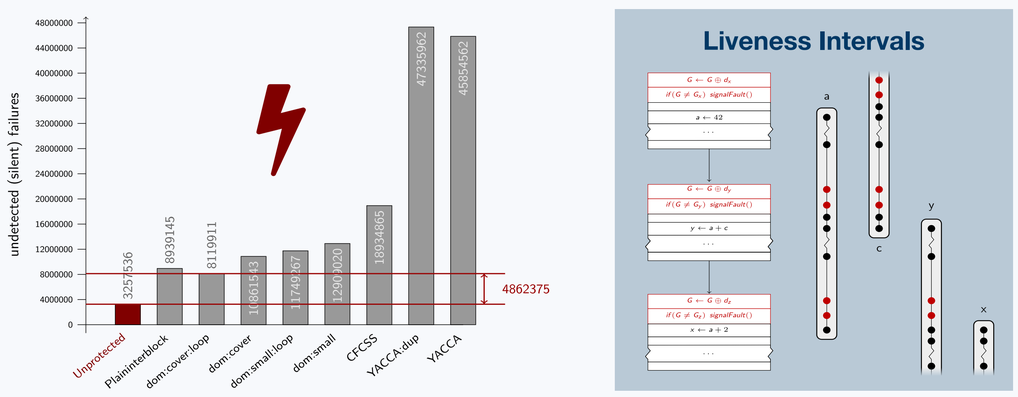
## New Perspective: Absolute Failure Counts




### Assessment with Absolute Failure Counts

**Failure rates are unsuitable** to compare fault-tolerance variants. Fault probabilities are always expressed in relation to both space and time. As all **CFC techniques induce overhead their fault space increases**. The failure count is an alternative, which respects the changed fault space.

## An Underestimated Threat: Data Faults







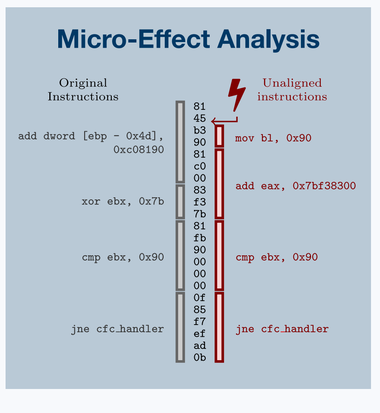
### General Fault Injection Reveals True CFC Efficiency

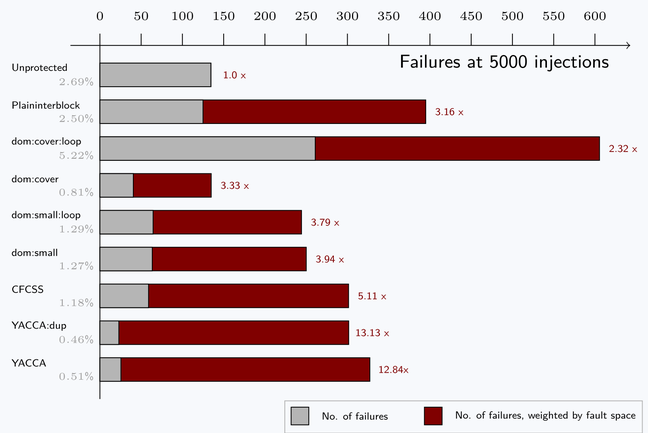
Also considering data faults, **CFC dangerously fails the reality check** with the reliability decreased in virtually all test scenarios: the **reason being the overhead induced**, which substantially enlarges the fault space especially for the typically neglected data faults.

## Bottom Line

### CFC Schemes are Mostly Ineffective or Even Dangerous

We disclosed various **latent deficiencies of both the residual failure rate metric as well as software-implemented CFC**, which potentially compromise their general use when used without further measures.




Supported by

DFG SCHR 603/9-2 SFB/TR89 (Project C1), Invasive Computing

Federal Ministry of Education and Research ID 01IS16025 (ARAMiS II)

Bavarian Ministry of Economic Affairs and Media, Energy and Technology 0704/883 25 (EU EFRE funds)

www4.cs.fau.de/Research/Soft-Errors

1 Friedrich-Alexander-Universität Erlangen-Nürnberg 2 Schaeffer Technologies AG & Co. KG 3 Leibniz Universität Hannover

Presented at EMSOFT 2017, Seoul