HARV-SoC

Hardened RISC-V System-on-Chip

Université de Montpellier

Douglas A. Santos, Carolina Imianosky, and Luigi Dilillo

Motivation

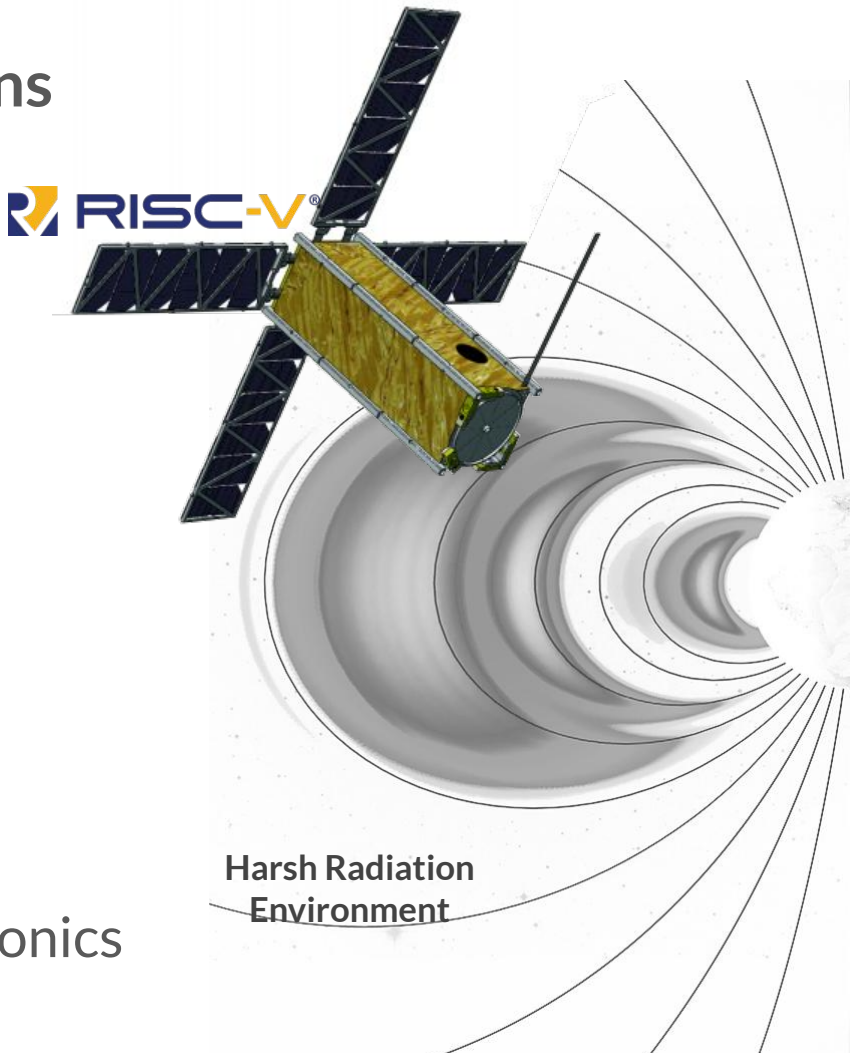
Harsh environments impose challenging design decisions

- Temperature variations
- Mechanical stress
- Ionizing radiation

Radiation harsh environments (e.g. avionics, space)

- Single-Event Effect (SEE)
- Total Ionizing Dose (TID)
- Displacement Damage (DD)

Challenge: Understand the effects of radiation in complex electronics



Outline

System Observability

HARV-SoC design

Irradiation Experiments

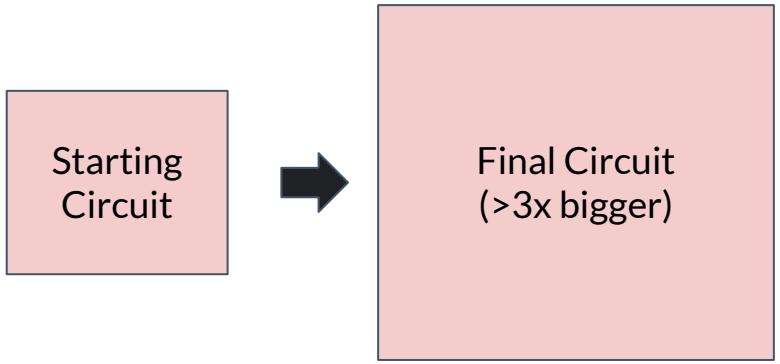
Summary and Conclusions

Design Strategy for HARV

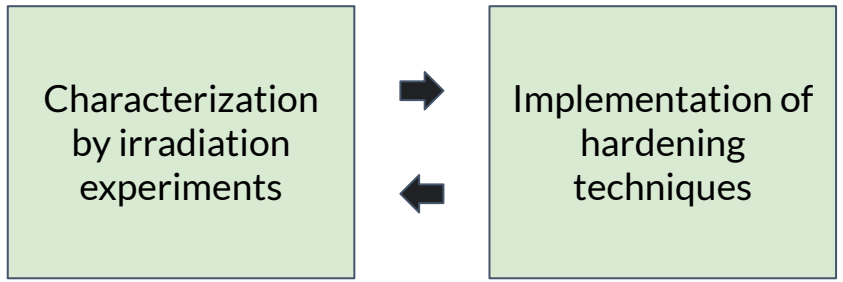
Proposal: Develop a processor with low resource usage that complies with radiation constraints

Result: Agile, Flexible, not resource greedy, proved radiation-hardened

Standard Approach



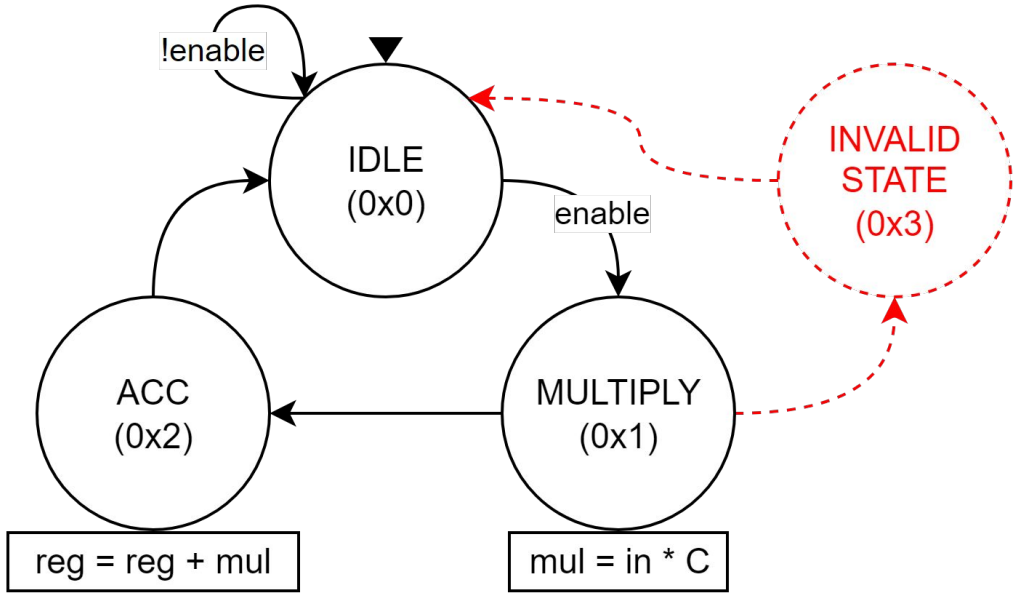
HARV Approach



System Observability

Observability is tooling or a technical solution that allows teams to actively debug their system. Observability is based on **exploring properties and patterns not defined in advance.***

- ➔ consists of collecting and reporting data about the system's execution
- ➔ improves understanding possible unexpected system behavior
- ➔ allows for improved reliability in some system applications

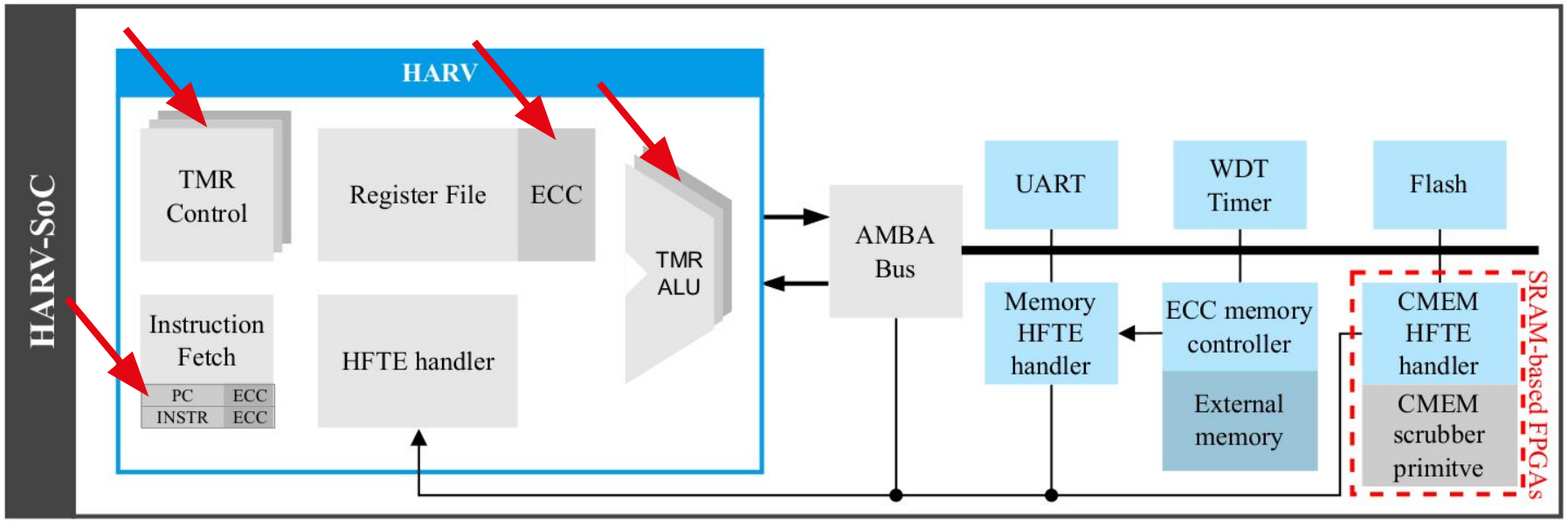


* definition by Google Cloud

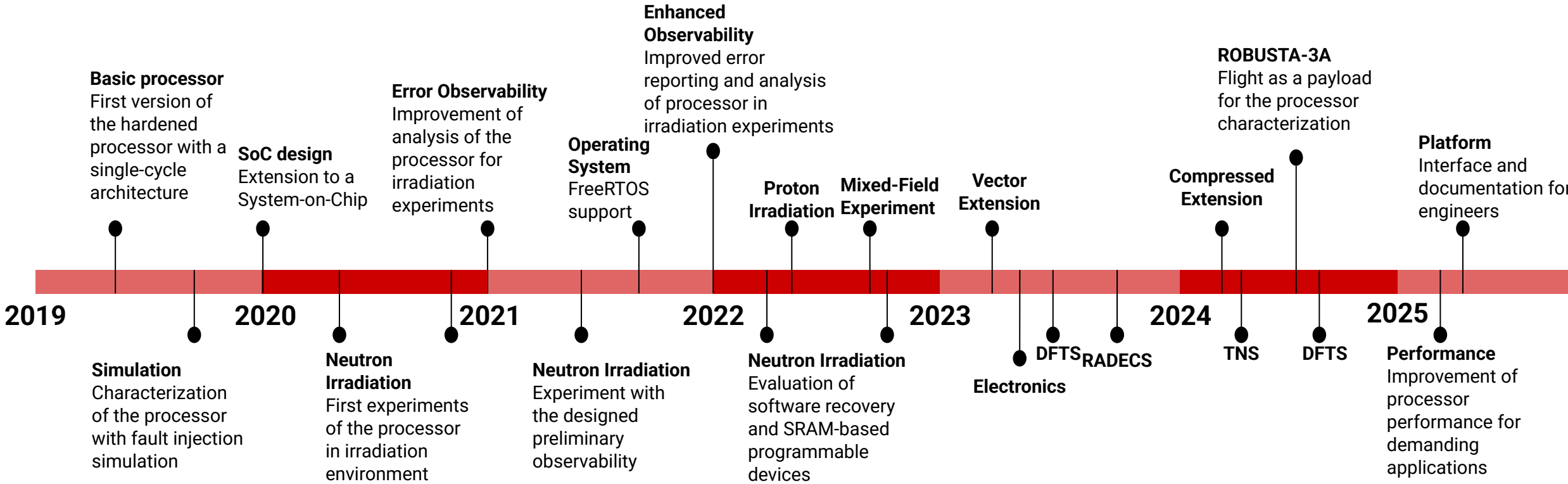
HARV-SoC Overview

HARV-SoC - Hardened RISC-V System-on-Chip

- **Soft-core** SoC developed for FPGAs, with support for different technologies
- Reliable SoC with enhanced **fault observability**
- Based on the **RV32I** specification (supports **RV32E**), and extended with CSR, multiplication/division, compressed, and vector instructions
- Implements hardening in the processor core microarchitecture



HARV-SoC Design Timeline



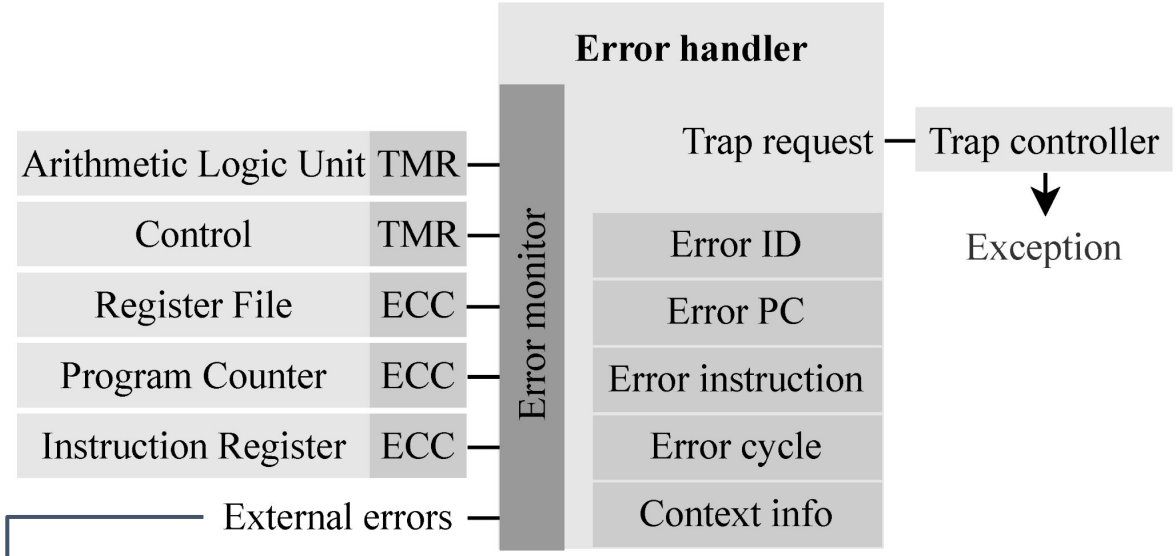
HARV-SoC: Enhanced Observability

HARV implements a combination of TMR and ECC for most critical structures

Adds **observation** of the hardened structures of the processor and SoC

- Provides detailed information about the processor context and errors

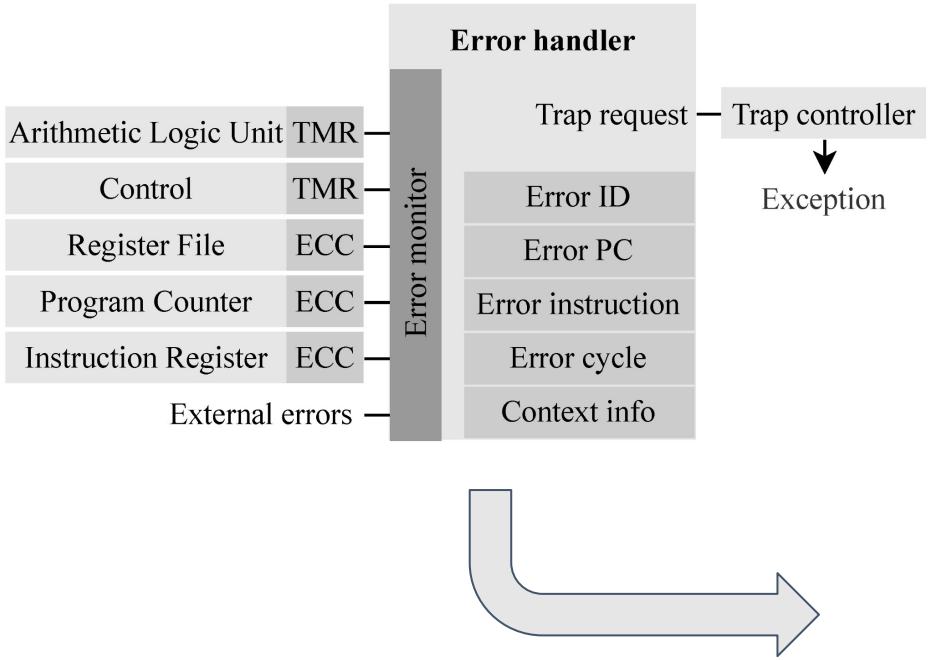
HARV Fault Tolerance Exceptions (HFTE)



SoC Errors

- Upsets in the external memory (SECDED)
- Peripheral access timeout
- Watchdog timer

Enhanced Observability



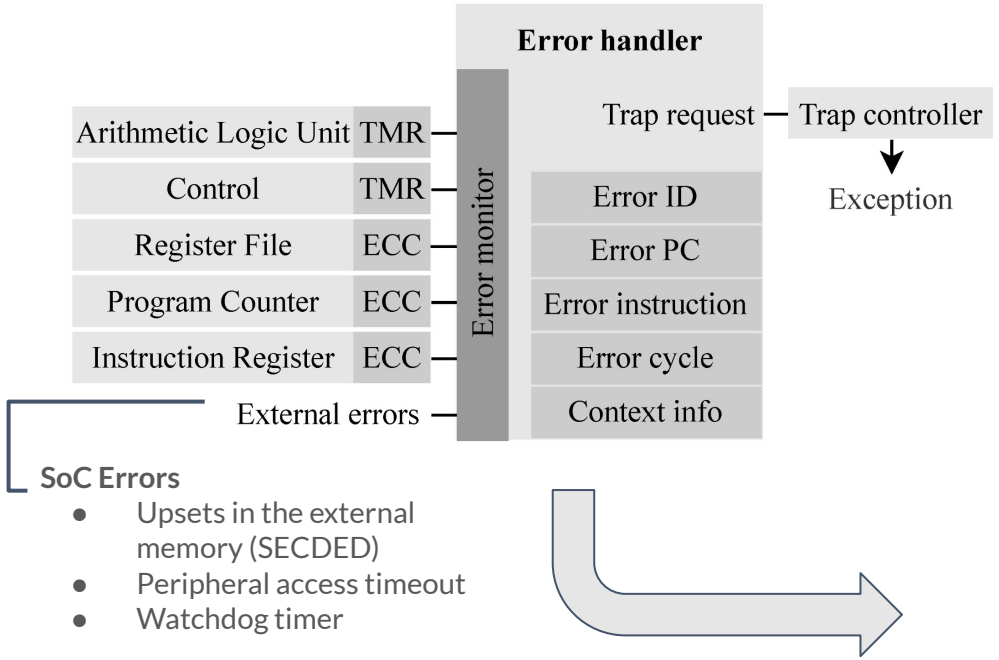
Error reporting

Performed using an exception service routine

Applications may perform actions according to the error severity

- Correct SBU in the memory (rewrite word)
- **Use software recovery techniques**
- Cancel task execution
- Force soft reset
- …

Example Implementation: Software Recovery



Error reporting

Performed using an exception service routine

Applications may perform actions according to the error severity

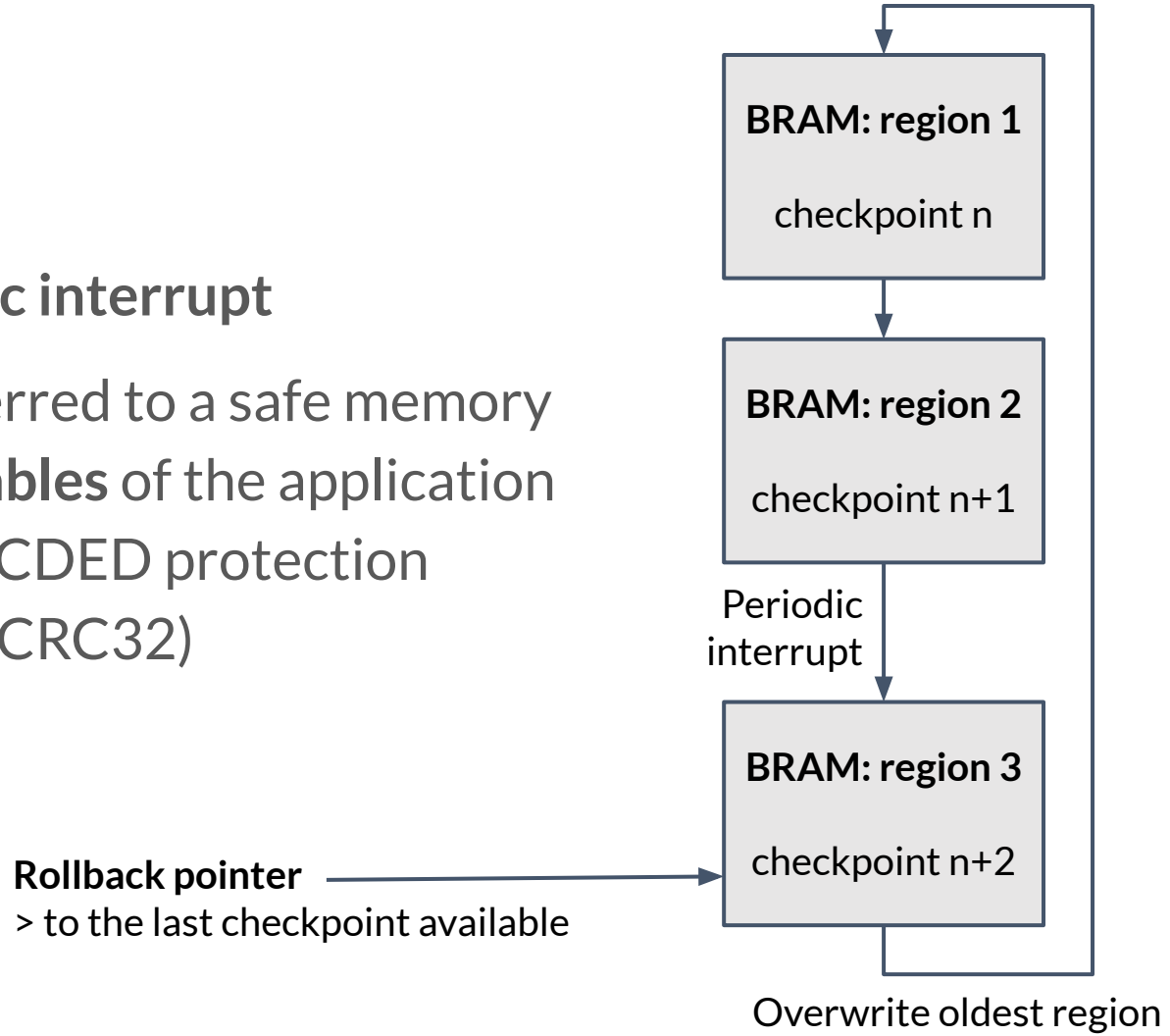
- Correct SBU in the memory (rewrite word)
- **Use software recovery techniques**
- **Cancel task execution**
- Force soft reset
- …

Example Implementation: Software Recovery

Checkpoint

Implemented in software through a **periodic interrupt**

- The context of the application is transferred to a safe memory
- Includes **register file** and the **local variables** of the application
- Saved in BRAM memory blocks with SECDED protection
- Includes an extra error detection code (CRC32)



Irradiation Experiments

Facilities

ChipIr Irradiation Facility

- Similar neutron spectrum to atmospheric environments
- Neutron flux of ~5x10^6 n/cm^2/s

PARTREC Proton Irradiation Facility

- Energy: 184 MeV
- Fluxes: up to 1 × 10^8 p/cm^2/s

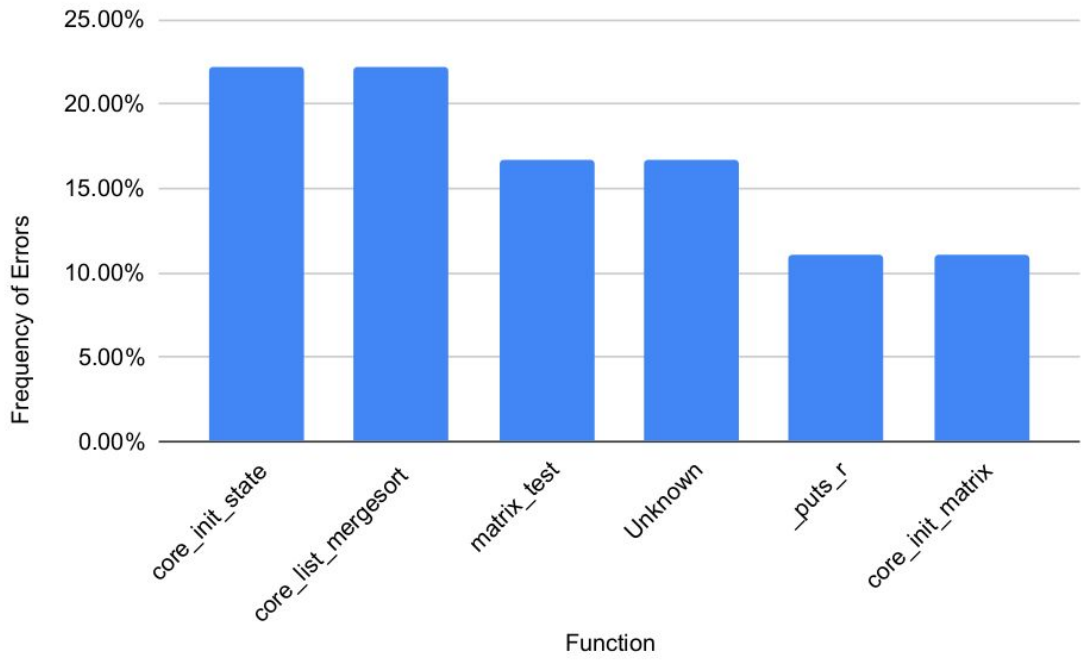
CHARM (CERN)

- Mixed-field irradiation
- Similar to space environment

Results: Neutron Experiment

Identified the execution context using the enhanced observability

- Most errors in core_init_state and core_list_mergesort coremark's functions
- Few errors during print operation



Results: Mixed-Field Experiment

Improved classification of each type of error

- Calculated cross-section for each of them

Most were from the memory, followed by register file

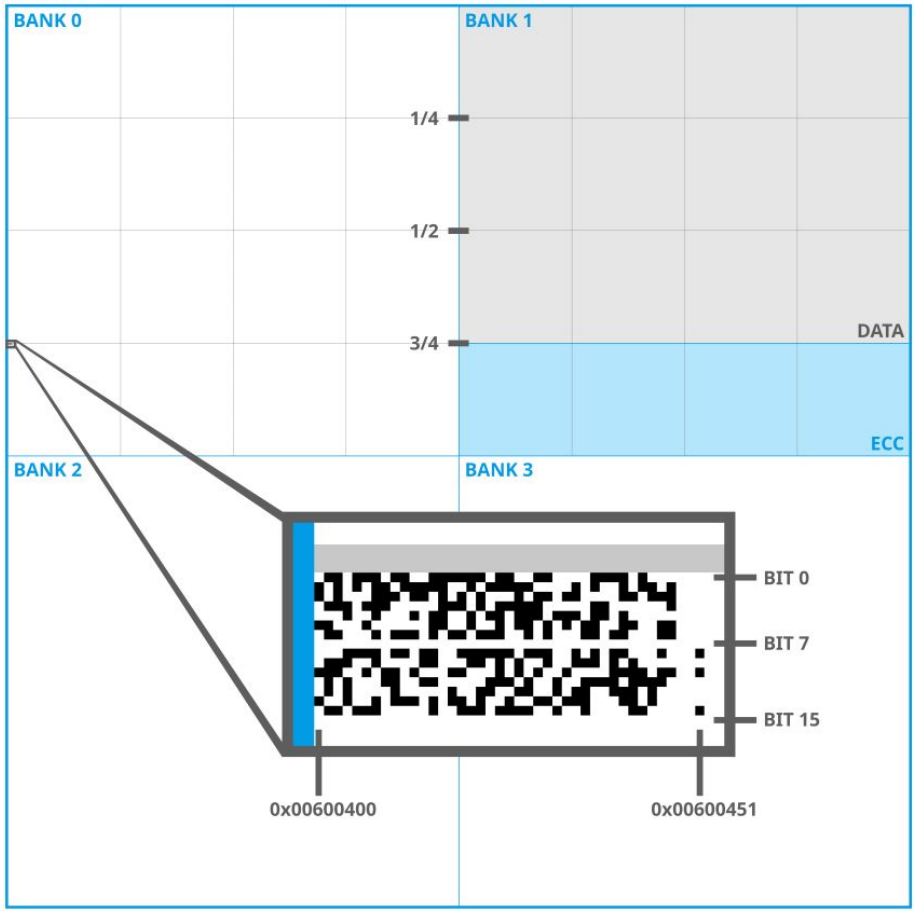
Error	#Errors	Percentage	HEH XS [cm²/device]
Memory single-bit upset	71	52.21%	7.38×10^{-11}
Memory double-bit upset	35	25.74%	3.64×10^{-11}
Register file single-bit upset	21	15.44%	2.18×10^{-11}
Load access fault	6	4.41%	6.24×10^{-12}
Store access fault	2	1.47%	2.08×10^{-12}
Program counter double-bit upset	1	0.74%	1.04×10^{-12}

Mixed-Field Experiment: Detected Block Error

Detected a block error in the SDRAM memory

- Did not affect the execution
- ECC part of the memory

Reported by using several traps



Mixed-Field: Error Propagation

Error propagation reduced in 2.7x

Configuration	Error	#Errors	#Prop. Errors	Error Prop. HEH XS [cm²/device]
Baseline	Register file single-bit upset	13	3	3.12×10^{-12}
	PC double-bit upset	1	1	1.04×10^{-12}
	Load access fault	4	4	4.16×10^{-12}
Hardened	Store access fault	2	2	2.08×10^{-12}
	Memory double-bit upset	1	1	1.04×10^{-12}

2.7x reduction

Proton Experiment: Error Propagation

Error propagation reduced in 4.5x

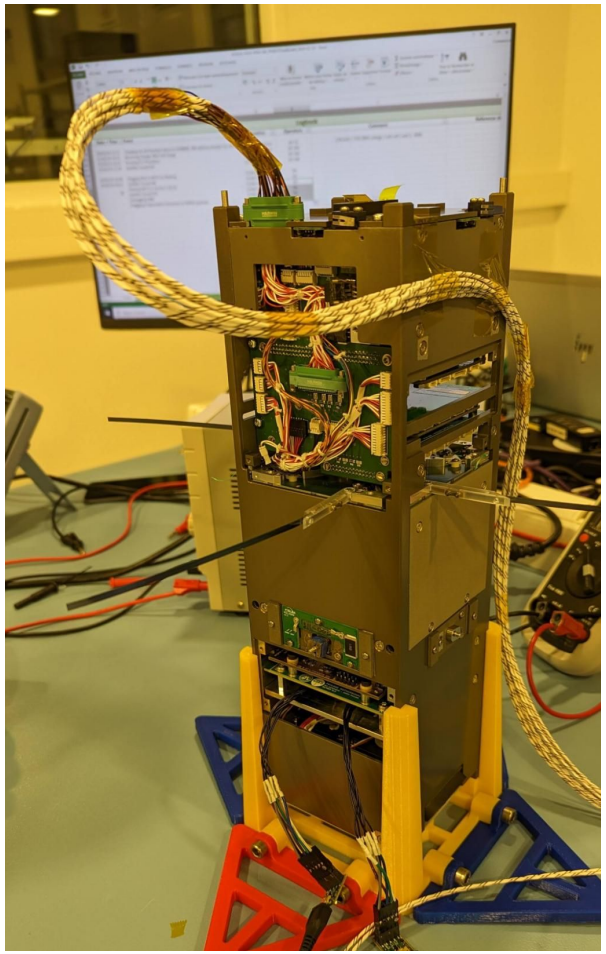
Table 4.13 – Error propagation per HFTEs for each HARV-SoC configuration.

Configuration	HFTE Type	#HFTE[1]	#Prop. HFTEs[1]	HFTE Prop. XS[1] [cm²/device]
Baseline	Memory single-bit upset	21	0	-
	Register file single-bit upset	6	1	6.99×10^{-13}
	Timeout load access fault	6	4	2.80×10^{-12}
Hardened	Memory single-bit upset	23	0	-
	Register file single-bit upset	11	0	-
	Timeout load access fault	3	1	6.28×10^{-13}
	Memory double-bit upset	2	0	-
	Program counter single-bit upset	1	0	-
	Instruction register double-bit upset	1	0	-
	Program counter double-bit upset	1	0	-
	Load access fault	1	0	-

[1] Analysis considering before device failure at 25 *krad*

4.5x reduction

ROBUSTA-3A - HARV payload



ROBUSTA-3A - CSUM - Centre spatial de l'Université de Montpellier

- 3U cubesat
- Launched in July 9th, 2024
- LEO orbit at 600km
- Expected to last at least 2 years

HARV payload

- Developed for characterizing the HARV-SoC
- 588 hours of experiment so far

Summary and Conclusion

Summary and Conclusion

HARV-SoC

- Fault tolerance at the microarchitecture level
- Error detecting and reporting

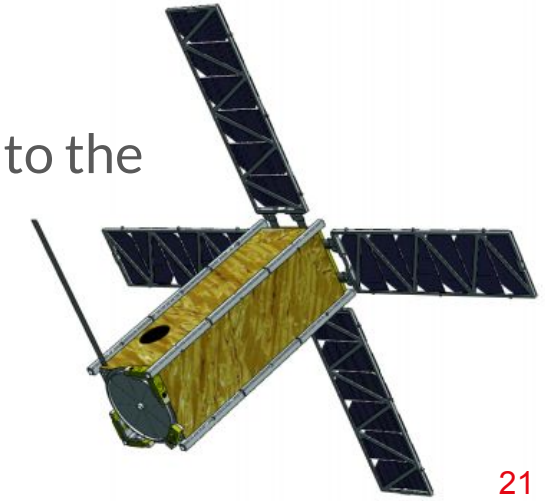
Enhanced Observability

- Temporarily storing the information about the detected errors in the processor core and SoC structures
- Report radiation-induced errors through RISC-V exceptions

Presented characterization results of fault-injection experiments

- SoC has been characterized with **neutrons**, **mixed-field**, and **protons**
- Identifies radiation-induced events and provides information that points to the compromised structure

Flight Mission ongoing in the ROBUSTA-3A Méditerranée



Summary and Conclusion

Future Work

- Development of a development platform for engineers with an integrated fault injection simulation tool
- Improvement of the processor performance by using different strategies but maintaining its observability requirements
- Extension of the SoC
- Open-source version envisioned

HARV-SoC

Hardened RISC-V System-on-Chip

Université de Montpellier

Douglas A. Santos, Carolina Imianosky, and Luigi Dilillo

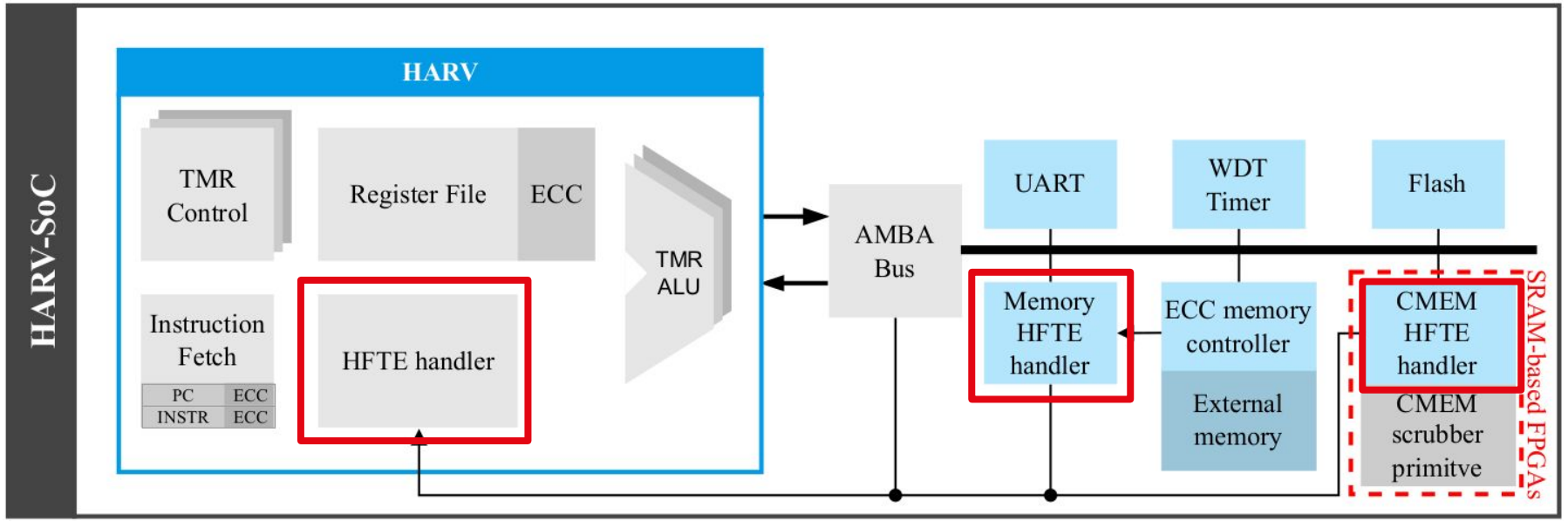
EXTRA SLIDES

HARV-SoC

Separated error handlers for the processor and SoC

- Error handler
- SoC error handler

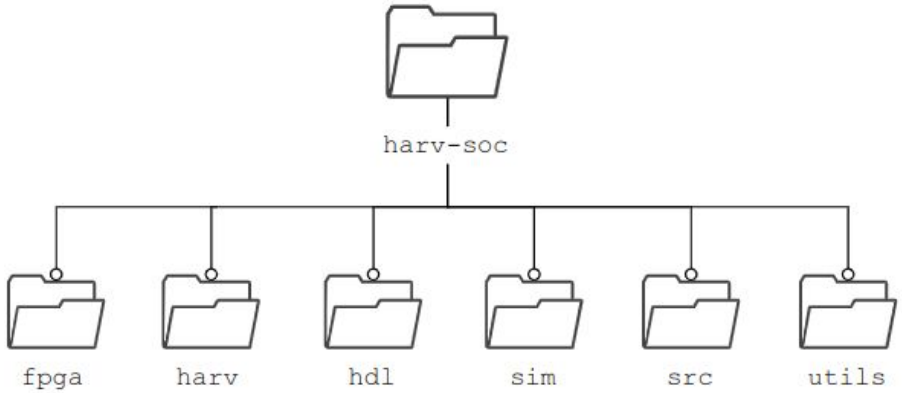
Simplifies error handler for processor



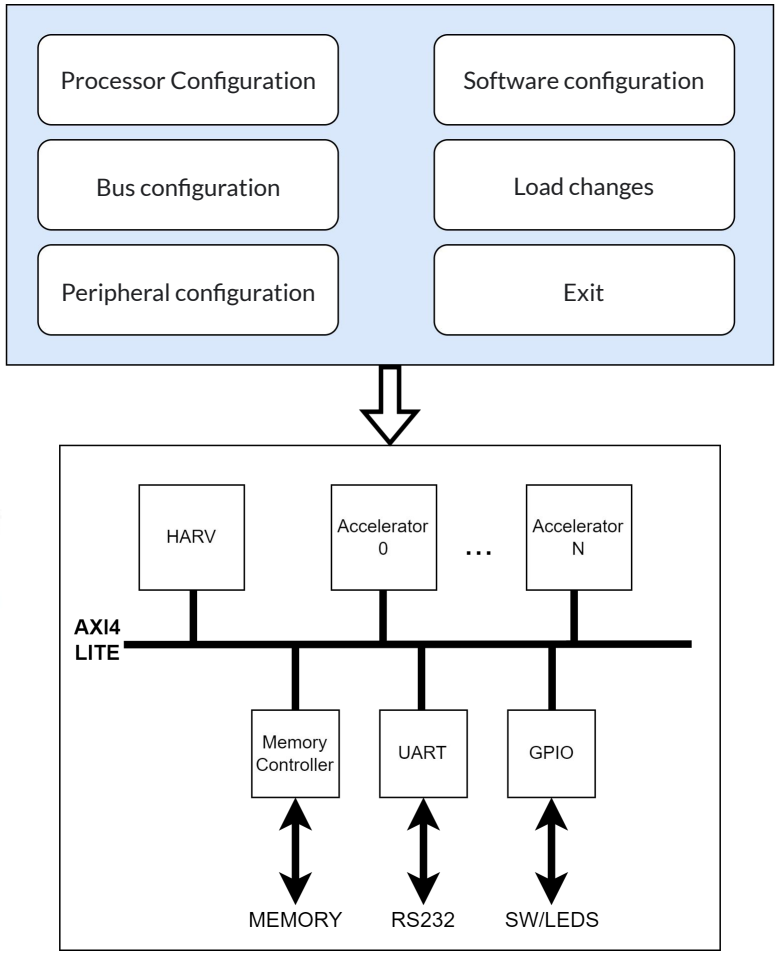
Development Platform

Platform for easy software development through simulations and FPGA prototyping

- Bare-metal
- FreeRTOS



Command	Description
`$ make app`	Compile the application.
`$ make ahx`	Generate the files for simulation.
`$ make axh-sim`	Compile and generate the files for simulation.
`$ make ghdl-sim`	Execute the simulation
`$ make vivado-sim`	Execute the simulation by Vivado.
`$ make DUMP_ALL=1 vivado-sim`	Execute the simulation by Vivado and dump all the signals to a file.
`$ make vivado-open-sim`	Open the waveform of the dumped signals on Vivado. This command can only be executed after the `$ make DUMP_ALL=1 vivado-sim`.
`$ make modelsim-sim`	Execute the simulation by Modelsim
`$ make modelsim-sim-fault`	Execute the simulation by Modelsim with fault injection. The execution simulates the radiation environment of ChipIR accelerated by 10x.
`$ make clean`	Cleans the folder `out`.



HARV Hardening

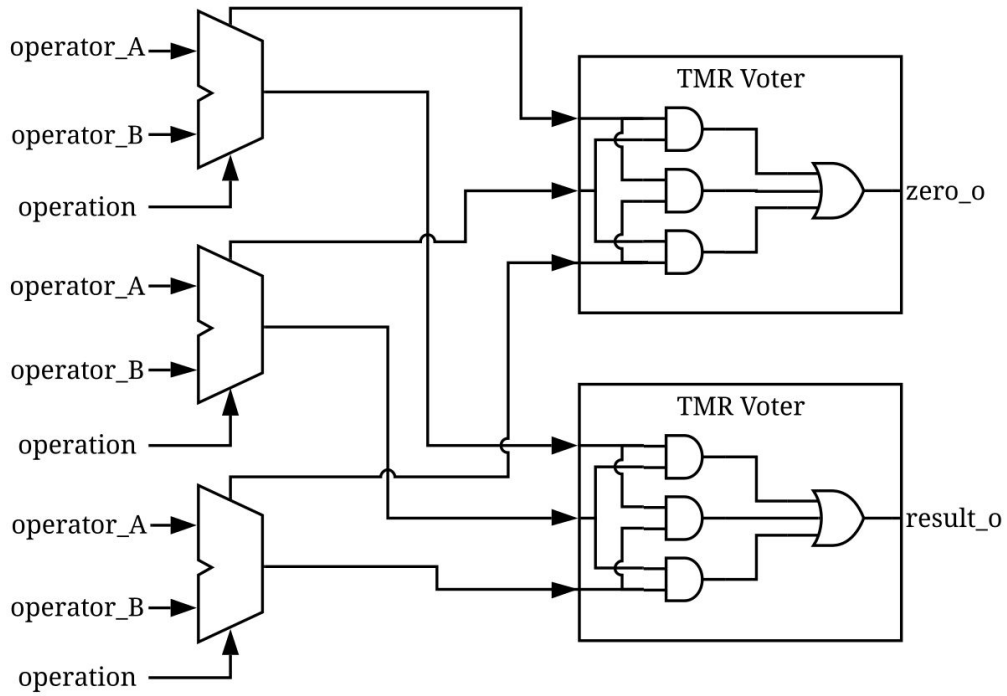
TMR: Triplication of the module

↓

Bitwise voting of the most common result

Implemented in combinational structures

- Control
- Arithmetic-Logic Unit (ALU)



HARV Hardening

Hamming code-based Error Correcting Code (ECC)

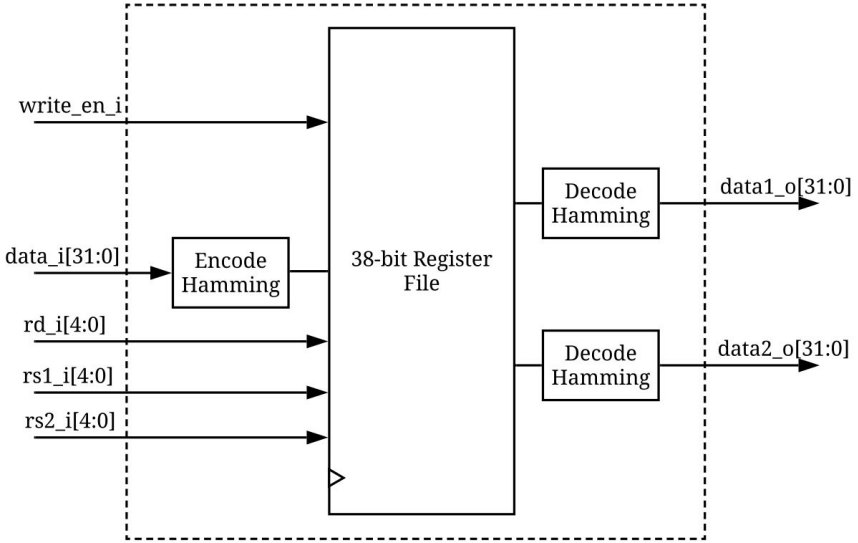
- Add 7 redundant bits to correct 1-bit upset and detect a double-bit upset

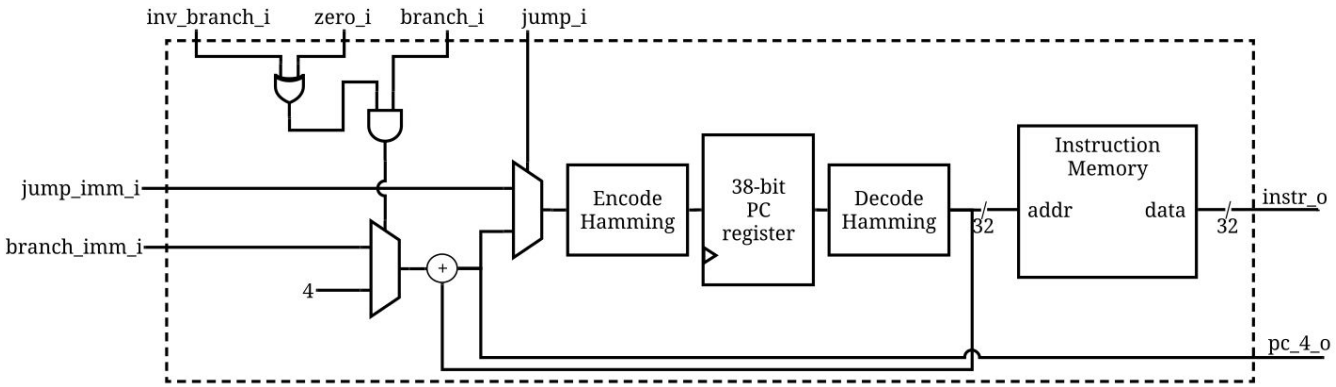
Require the implementation of two blocks

- ECC encoder → generates ECC data
- ECC decoder → corrects upset

Implemented in critical registers

- Program Counter (PC)
- Register file





Registers Hardened with TMR

- **mtvec**

  Stores the function address that will handle the traps. Bit upsets in this register will cause the program to jump to an incorrect address, which affects the execution flow of the program.

- **mie**

  Stores the enabled interrupt flags. Bit upsets may cause applications that rely on interrupts for their execution, such as operating systems, in which an interrupt disabling will result in an application failure.

- **hardening**

  It is a read-write-enabled custom CSR that stores the enabled hardening of the HARV. It stores the correction-enable flags for each hardening component. Therefore, bit upsets in this register affect the correction of errors, which may result in unwanted execution experiments.

HARV-SoC: Detailed Error Information

Several information are reported through memory-mapped registers

- Type of error
- Loaded instruction
- Encoded data (upset included)
- ALU output
- Detection cycle
- Application context

Table 6.2 – Memory-mapped registers with HARV HFTE information.

Register	Address	Information
EH_EVENT_ID	0x01000000	[0] PC SBU [1] PC DBU [2] IR SBU [3] IR DBU [4] register file SBU [5] register file DBU [6] register file SBU [7] register file DBU [8] control TMR error [9] ALU TMR error [10] external event (SoC) [11] peripheral access timeout
EH_PC	0x01000004	PC when error detected
EH_INSTR	0x01000008	instruction when error detected
EH_ENC_DATA	0x0100000C	encoded data according to error
EH_ENC_DATA_ECC	0x01000010	encoded data's ECC
EH_ALU_RESULT	0x01000014	ALU result
EH_MCYCLE	0x01000018	MCYCLE when error detected
EH_MCYCLEH	0x0100001C	MCYCLEH when error detected
EH_JALLOG_PTR	0x01000020	pointer to next register in jal logger
EH_JALLOG_SIZE	0x01000024	size of jal logger
EH_JALLOG_BASE	0x01000800	jal logger base

HARV-SoC: Detailed Error Information

Abstraction for SoC errors

- Memory errors
- Peripheral errors
- Device errors

Table 6.3 – Memory-mapped registers in bus with HARV-SoC memory HFTE information.

Register	Address	Information
SOC_EH_EVENT_ID	0x70800000	[0] memory SBU [1] memory DBU [2] stuck-at error
MEM_EH_MEM_ADDR	0x70800004	address with error
MEM_EH_MEM_ECC_ADDR	0x70800014	ECC address
MEM_EH_ENC_DATA	0x70800008	encoded data
MEM_EH_ENC_DATA_ECC	0x7080000C	encoded data's ECC
MEM_EH_PREV_MEM_ADDR	0x70800018	previous address with error
MEM_EH_ENABLE	0x70800010	HFTE detection enable

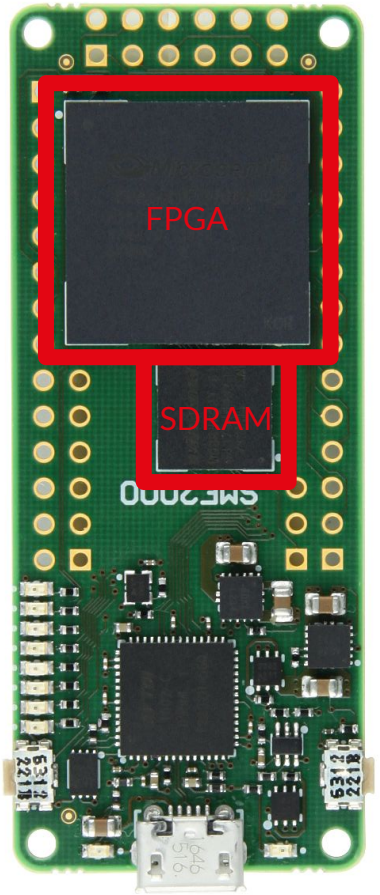
Experiment Setup

Microchip's Flash-based FPGA

- Flash-based Smartfusion2 M2S010
- Resilient against soft errors in the configuration memory
- SRAM-based block RAM
- D-type flip-flops

SMF2000 board

- Compact design → easy utilization in irradiation facilities
- External SDRAM component



Experiment Setup

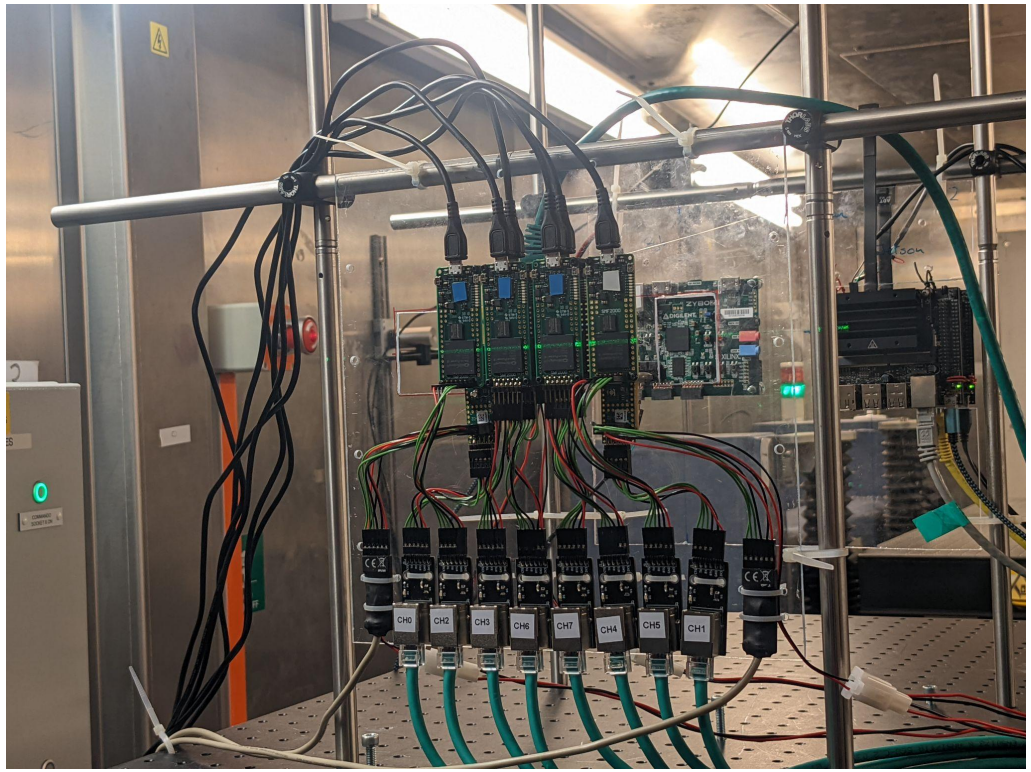
Four SMF2000 boards

Individual power supply with current monitoring

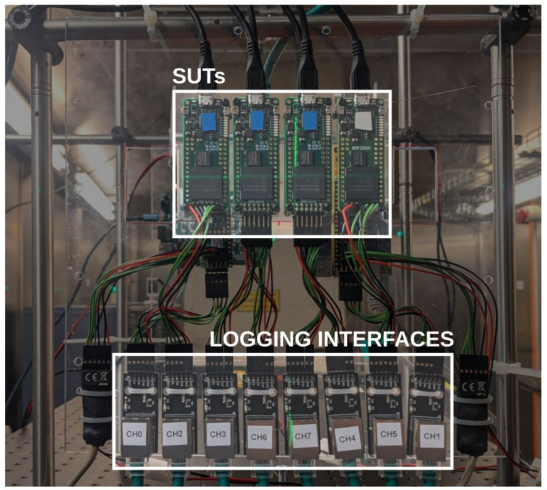
FTDI devices for logging the UART output

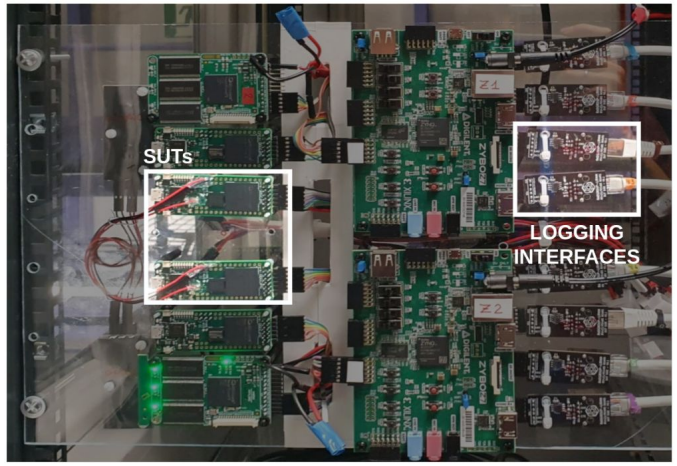
Coremark Benchmark

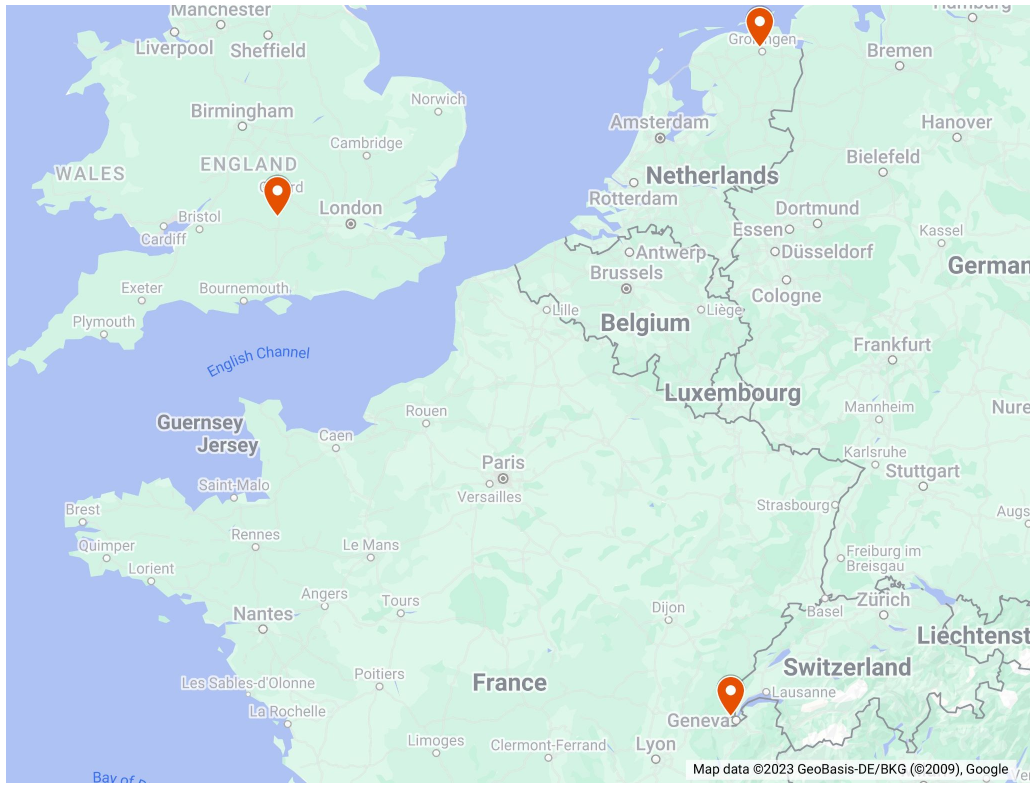
- List processing, matrix multiplication, state machines, and cyclic redundancy check
- Single-thread
- 200 iterations (~12 mins execution)
- Coremark debug flag enabled

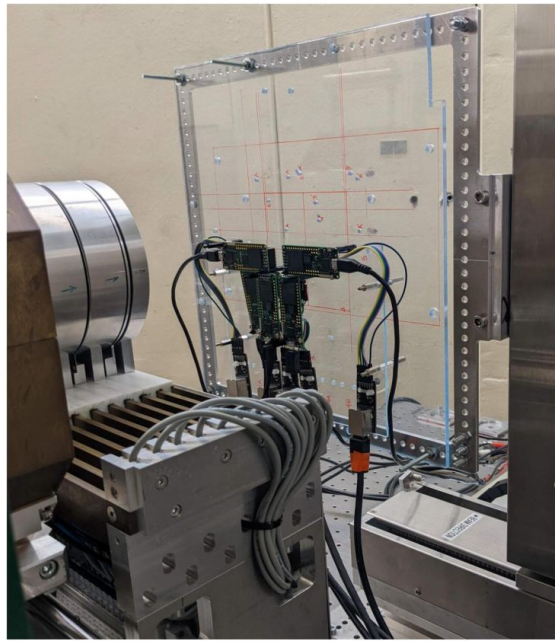


Experiments









Neutron Experiment

Classified errors based on correctability

- 55% of the errors were correctable with the hardened
  - Significant increased compared to 14% in baseline
- Most errors due to failures induced in the SoC

Error Classification	Baseline	Hardened
Correctable error	14.29%	55.56%
Not correctable error	71.42%	11.11%
Non-recognized error	14.29%	33.33%

Results: Neutron Experiment

Calculated device failure mean fluence to failure and cross-section

Similar numbers between boards

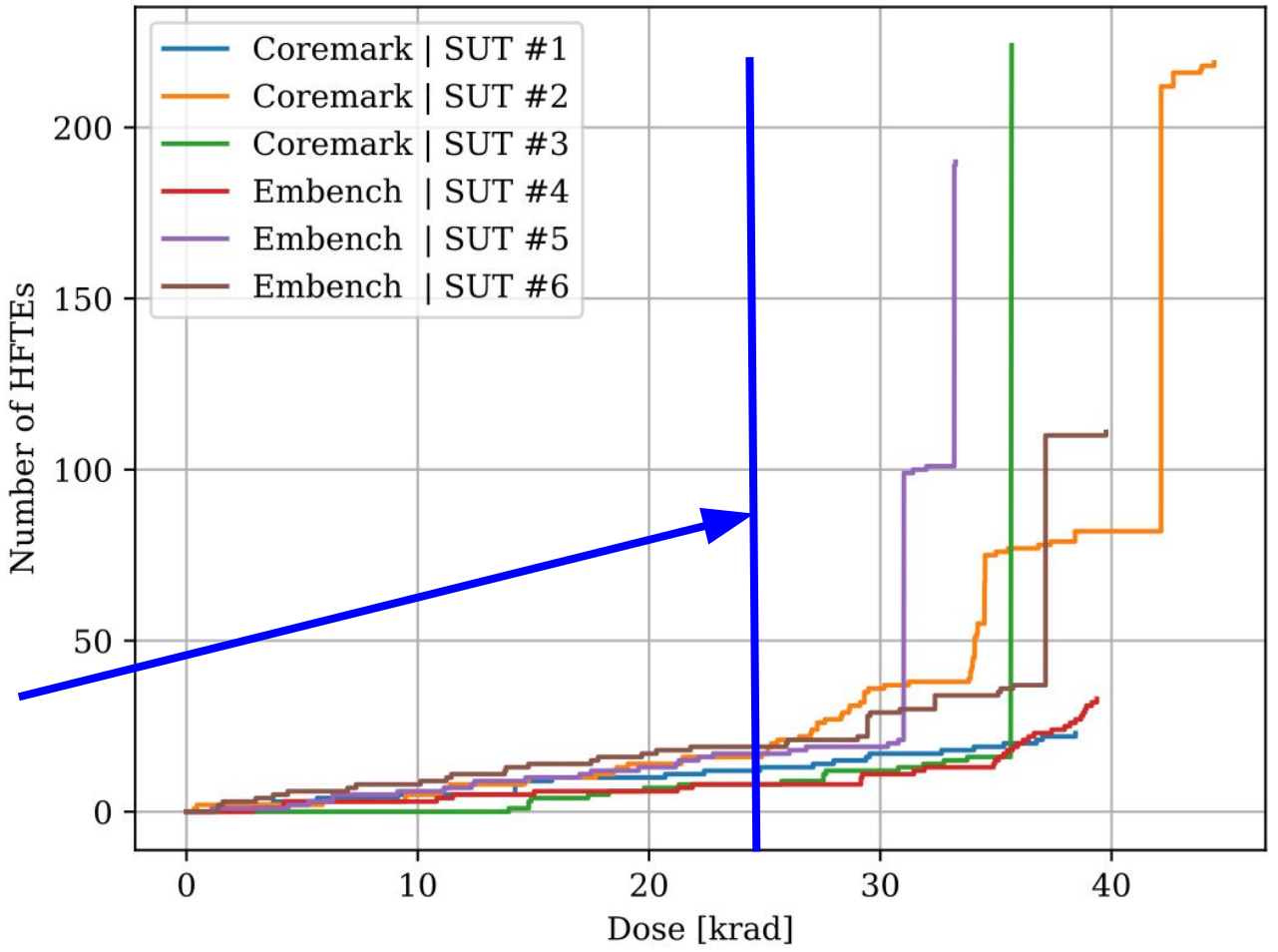
Board	MFTF [n/cm²]	Neutron Failure XS [cm²/device]
#B1	1.66×10^{10}	6.03×10^{-11}
#B2	1.85×10^{10}	5.42×10^{-11}
#B3	2.19×10^{10}	4.56×10^{-11}
#B4	2.15×10^{10}	4.66×10^{-11}
#B5	1.89×10^{10}	5.29×10^{-11}
#B6	2.60×10^{10}	3.84×10^{-11}

MFTF: Mean Fluence to Failure.

Proton Experiment

Number of reported HFTEs increased significantly after 25 kRAD because of dose effect

Threshold for SEE analysis defined as **25 krad**



Proton Experiment

Calculated cross-section for each defined HFTE

- Mostly from the memory, followed by the register file

HFTE Type	#HFTE[1]	HFTE XS[1] [cm²/device]
Memory single-bit upset	44	1.88×10^{-11}
Register file single-bit upset	17	7.25×10^{-12}
Timeout load access fault	9	3.84×10^{-12}
Memory double-bit upset	2	8.53×10^{-13}
Program counter double-bit upset	1	4.27×10^{-13}
Instruction register double-bit upset	1	4.27×10^{-13}
Program counter single-bit upset	1	4.27×10^{-13}
Load access fault	1	4.27×10^{-13}
Total	76	3.24×10^{-11}

[1] Analysis considering before device failure at 25 *krad*.

Results: Mixed-Field Experiment

Hardened is able to correct 60% of the detected errors

- Increased compared to baseline of ~40%

Still have not-correctable errors and non-recognized errors

Error Classification	Baseline	Hardened
Correctable error	39.02%	60.00%
Not-correctable error	43.90%	37.14%
Non-recognized error	17.07%	2.86%

Mixed-Field Experiment

Enhanced enabled analysis of number of errors per instruction

- Mostly memory access due to memory being the most significant source of errors

Class	Instruction	#Occurrences	Percentage	HEH XS [cm²/device]
Memory access	`lbu`	78	57.35%	8.11×10^{-11}
	`sw`	31	22.79%	3.22×10^{-11}
	`lw`	10	7.35%	1.04×10^{-11}
	`sb`	4	2.94%	4.16×10^{-12}
	`lh`	2	1.47%	2.08×10^{-12}
	`lb`	1	0.74%	1.04×10^{-12}
Flow control	`jalr`	4	2.94%	4.16×10^{-12}
Arithmetic	`addi`	3	2.21%	3.12×10^{-12}
	`add`	3	2.21%	3.12×10^{-12}

Mixed-Field Experiment

Used only two boards due to cabling and space restrictions

Almost equal MFTF and cross-section

Board	HEH MFTF [H/cm²]	HEH Failure XS [cm²/device]
#B1	1.31×10^{11}	5.20×10^{-12}
#B2	1.31×10^{11}	5.20×10^{-12}