Vulnerability Analysis of Embedded Digital Systems: from Physics to Microarchitecture

Olivier Sentieys
Univ. Rennes, Inria, IRISA
olivier.sentieys@inria.fr

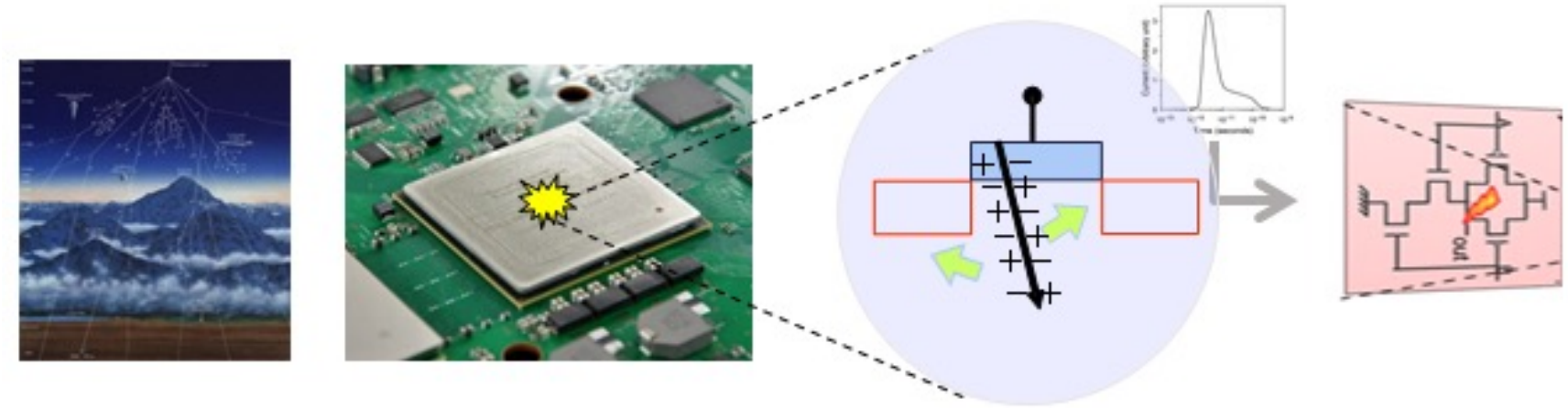
collaboration with Joseph Paturel, Angeliki Kritikakou, IRISA,
and Guillaume Hubert, ONERA, Toulouse

Why care about Fault Tolerance?

- Modern technologies
  - Lower node capacitances
  - Denser layouts, larger circuits
  - Increased frequencies
- Energy efficiency
  - Lower supply and threshold voltages

High SET[1] sensitivity

[1]Single-Event Transient



Vulnerability Analysis of Complex Designs

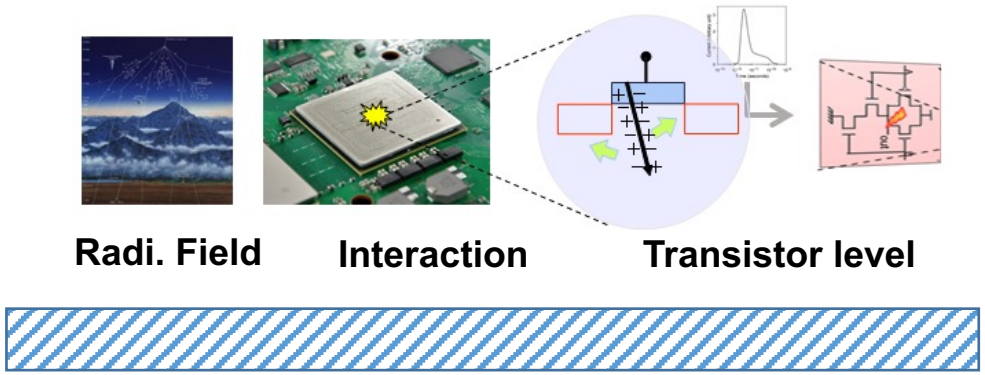
- Fault injection, simulation or emulation most often:
  - Only inject single-bit faults [1, 2]
  - Do not model the microarchitecture or ignores combinational logic [3, 4]
  - Do not take account of the physical effects
- Memory/register fault injection is not enough
  - Need to model microarchitecture
  - Need to consider combinational logic [5]
- New technologies exhibit multi-bit error behaviors
  - Need to model MBUs[1] as well as SEUs[2]

[1] Multi-Bit Upsets
[2] Single-Event Upsets

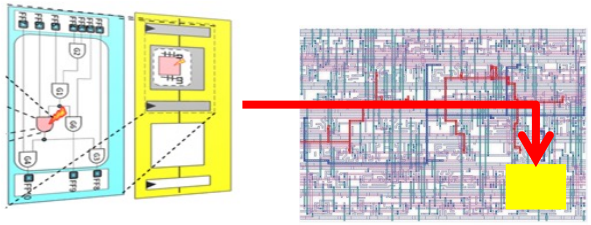
Single Event Effect: from the particle to the effect on circuits

- SEE analyses based on simulation:
  - Two disconnected approaches

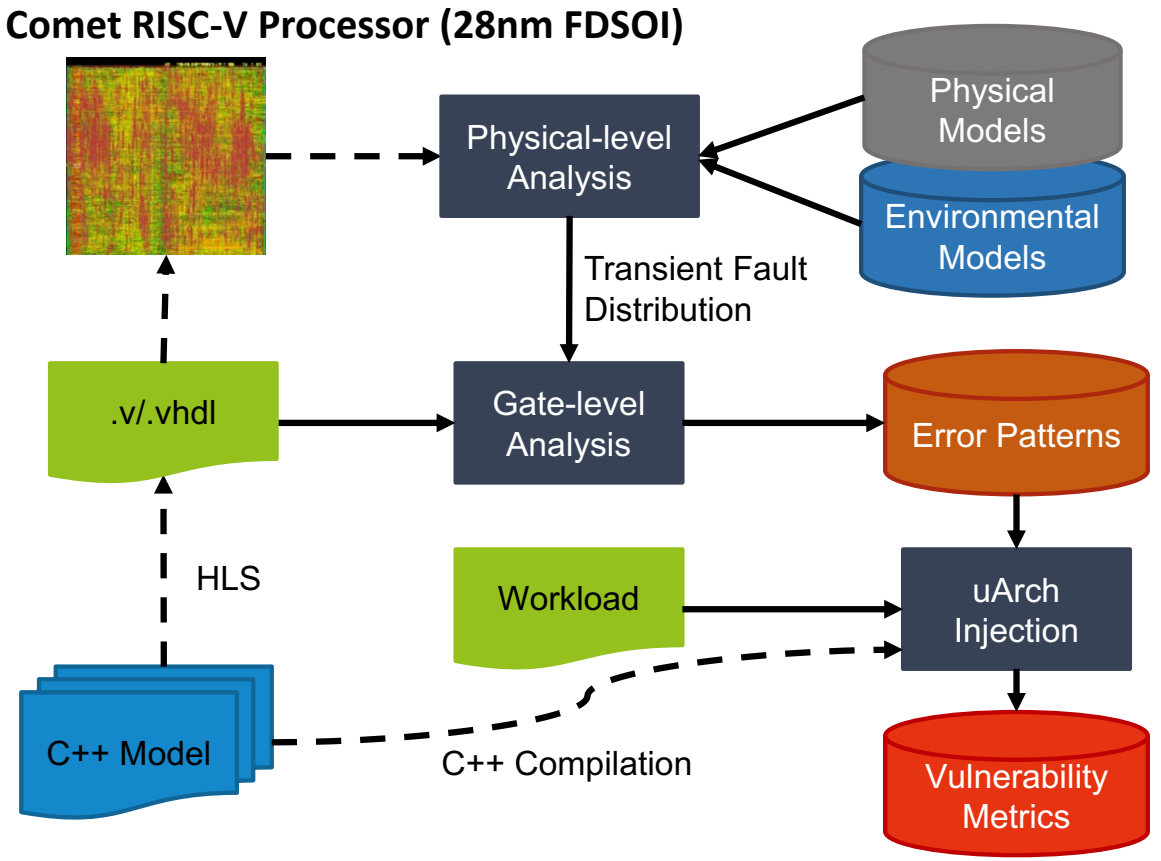
Multi-physic modelling: until cell level



Fault injection: no-physical contraints



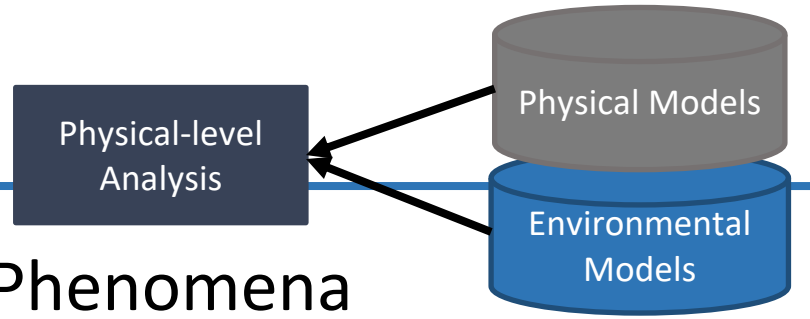
- Proposed Vulnerability Analysis Flow
  - From Physical to Architectural Level



Main Contributions

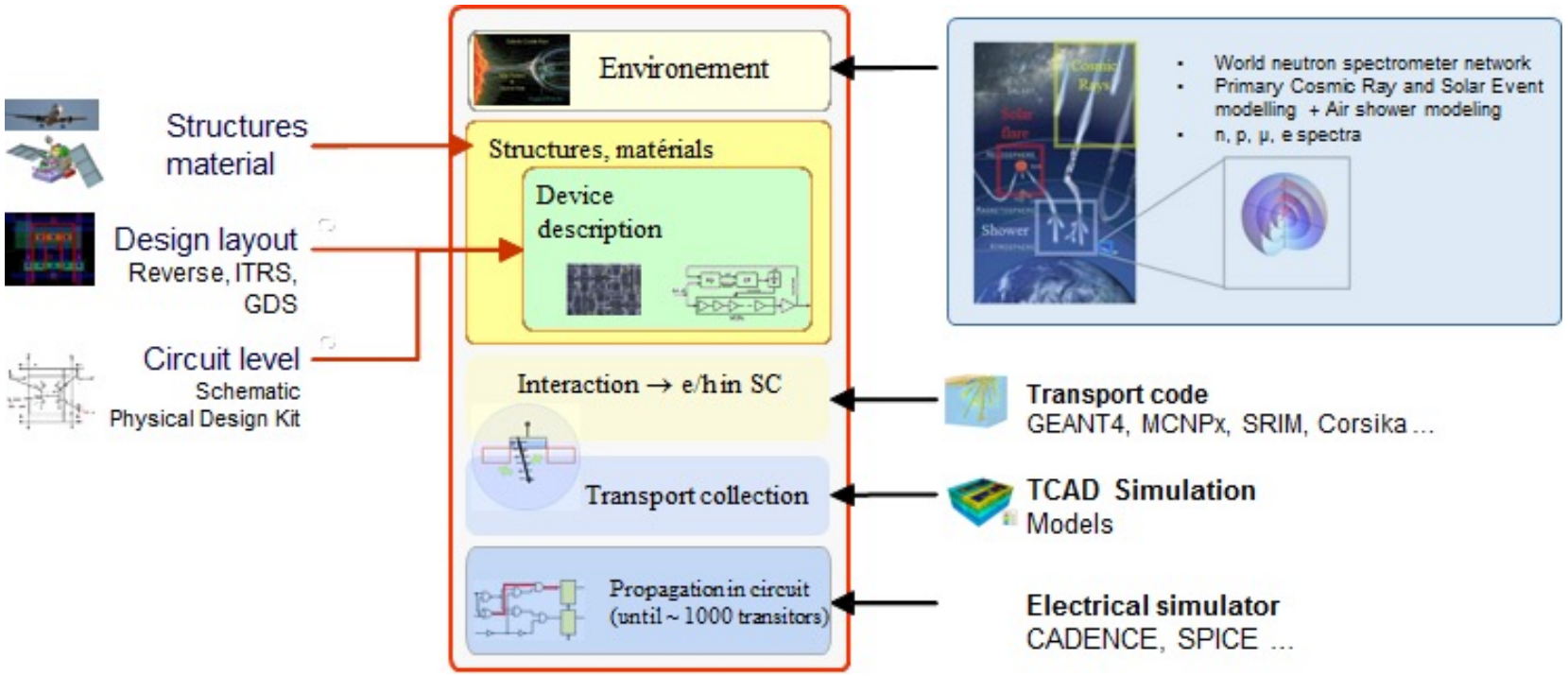
- Physical description of particle interactions on nanoscale transistors
  - Operational conditions: mission profile, space weather, temperature, power supply …
- Fault injection methodology and flow for complex designs
  - From physics to gate to microarchitecture
  - Account for SEUs and MBUs coming from combinational logic
  - But remains fast
- MBUs are present and are here to stay
  - Impact vulnerability
- Use case: in-house RISC-V processor core

ONERA Multi-Physics Platform

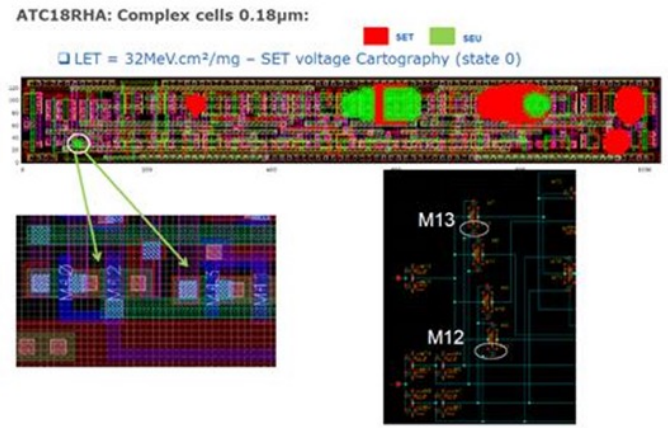


- MUSCA SEP3: Multi SCAles Single Event Predictive Phenomena Platform
  - SEE modelling → hardening by design, risk assessment and anticipation

Design & description | **MUSCA SEP3 Flow** | **Research activities**



Analyses
ex: hardening by design

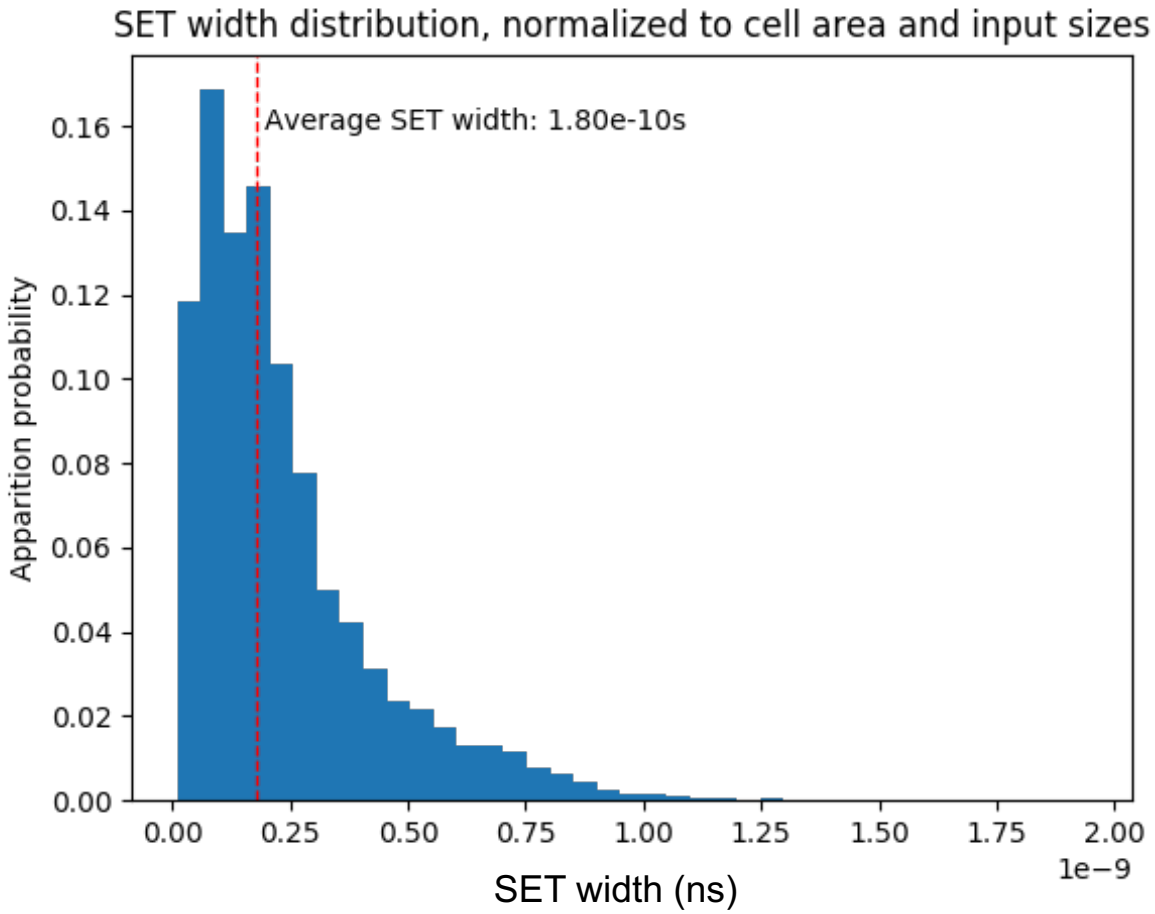


Results: Physical-level Analysis with MUSCA SEP3

- Distribution of transient delay profiles
  - Worst-case radiation scenario
    - LET = 58 MeV.cm2.µm-1
    - FDSOI 28nm, 25°C
    - Incidence Angle = 90°
  - 212K injections on 91 logic gates

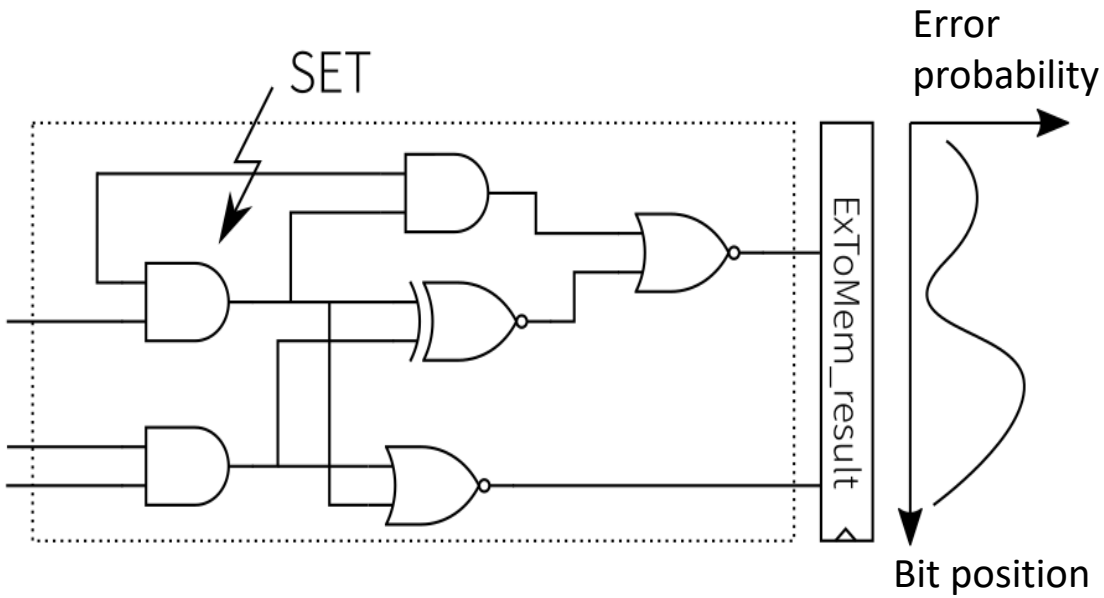
SET width	Proportion(%)
>500ps	10.543%
>1ns	0.651%
>1.5ns	0.13%

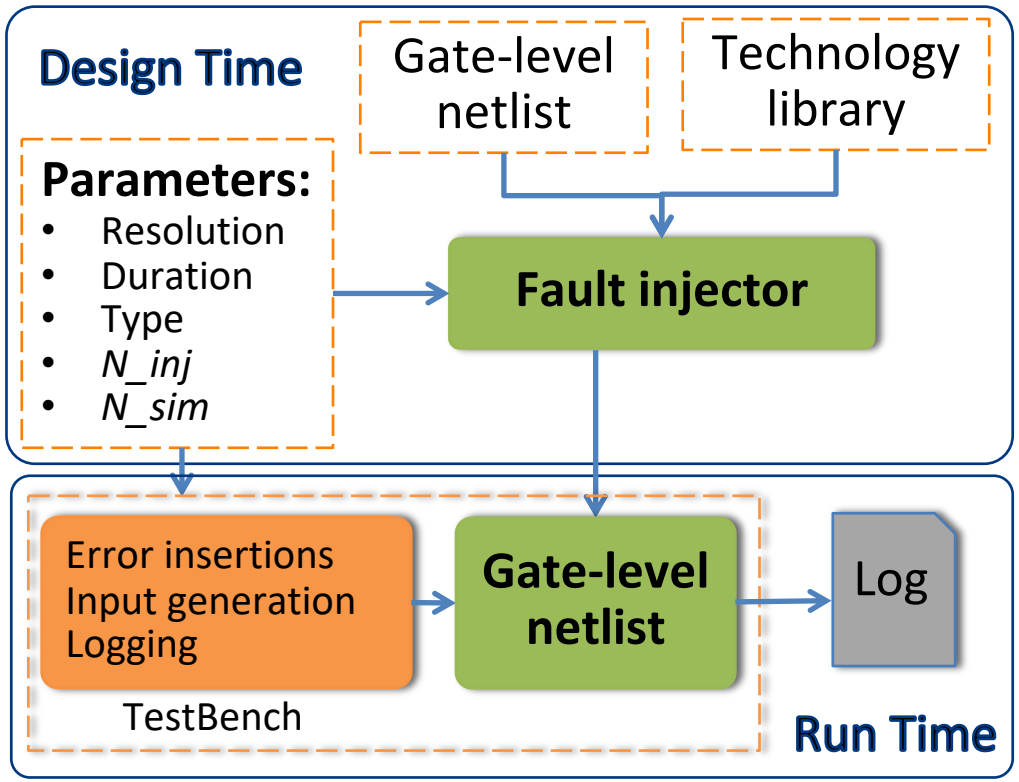
- Delay profiles are used during gate-level fault injection



Gate-level Fault Injection

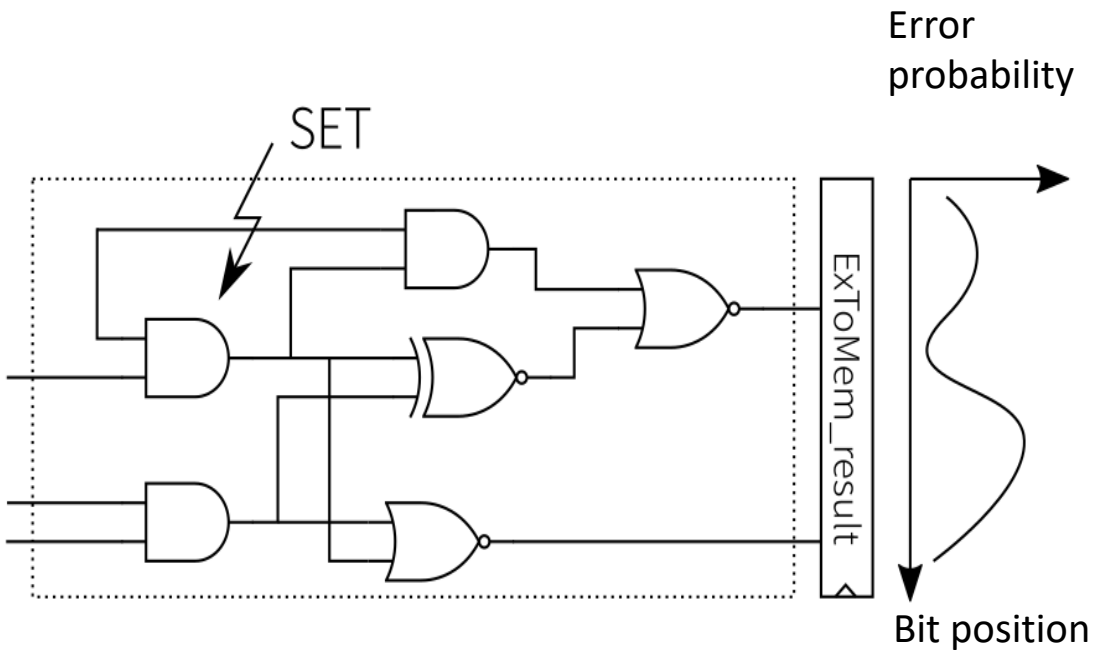
- Inject SETs in the gate-level netlist
- Aim is to capture profile and probability of error

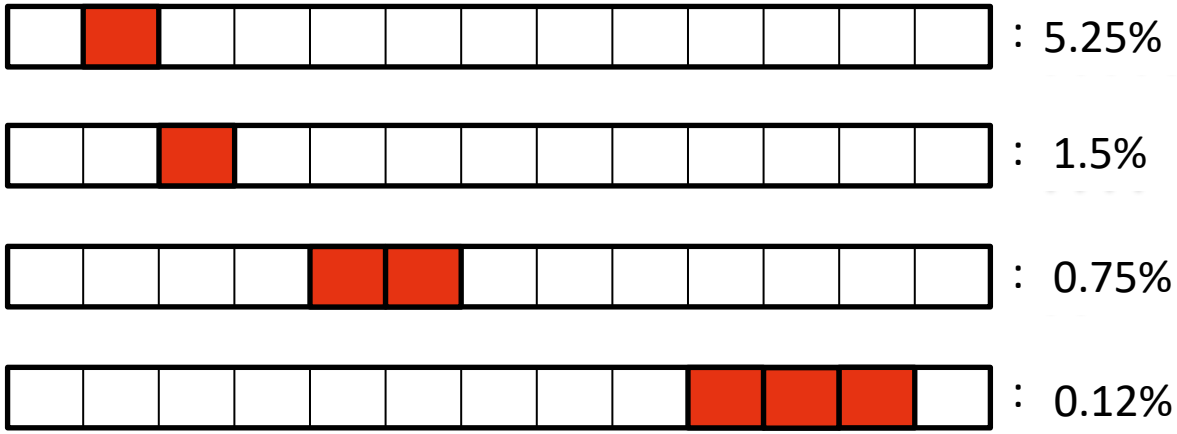




Gate-level Fault Injection

- Logging patterns and error probability (SEUs + MBUs)



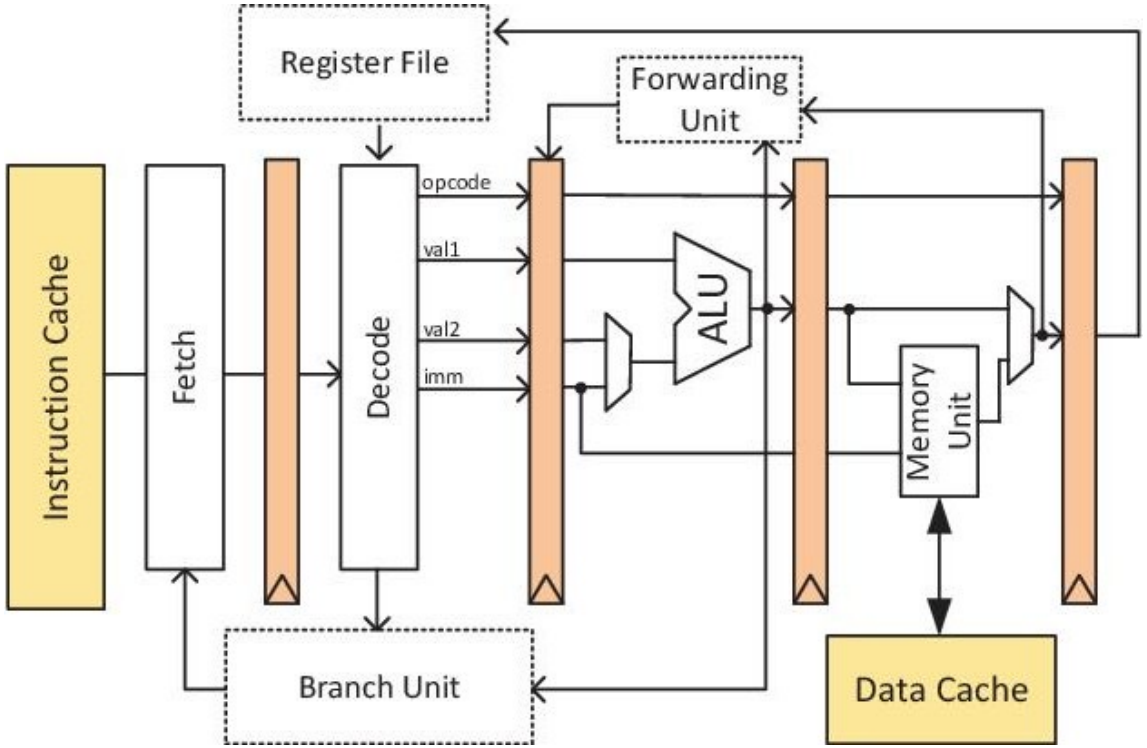


Probabilities of Error Patterns

[IEEE ISVLSI'20]

Comet Processor (RISC-V Instruction Set Architecture)

- 32-bit RISC-V instruction set RV32IMF
- In-order 5-stage pipeline micro-architecture
- Designed from a single C++ specification using High-Level Synthesis (HLS)
  - The simulator IS the hardware
- https://gitlab.inria.fr/srokicki/Comet

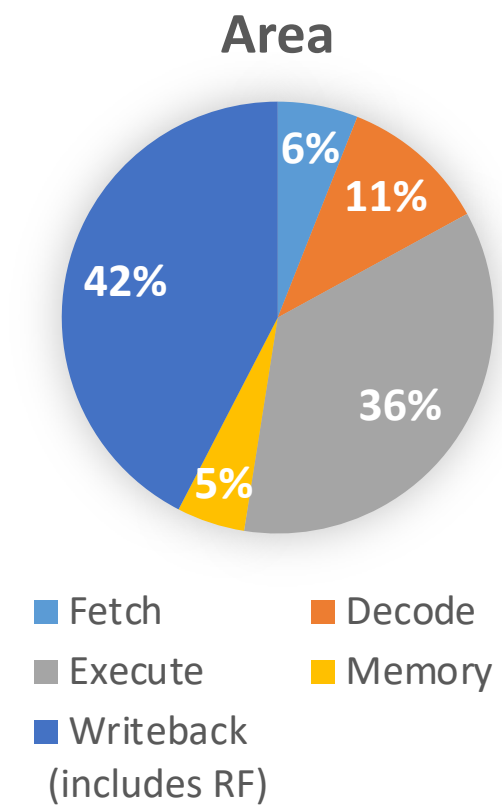


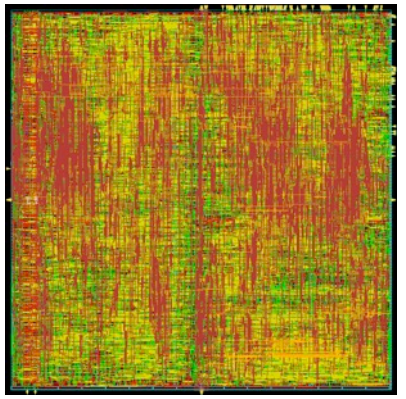
[IEEE/ACM ICCAD'19]

Comet Processor (RISC-V Instruction Set Architecture)

- Logic Synthesis + Place&Route Results
  - FDSOI 28nm
  - rv32i including memory: 0.02mm²
  - 700MHz

Core	ISA	freq. (MHz)	Area (μm^2)	Lang.
Comet [14]	rv32i		8 168	C++
	rv32im		11 099	
	rv32imf		26 760	
Rocket [12]	rv32i	700	11 114	Chisel
	rv32im		12 606	
	rv32imf		26 550	
PicoRV [15]	rv32i		7 747	Verilog
	rv32im		11 176	



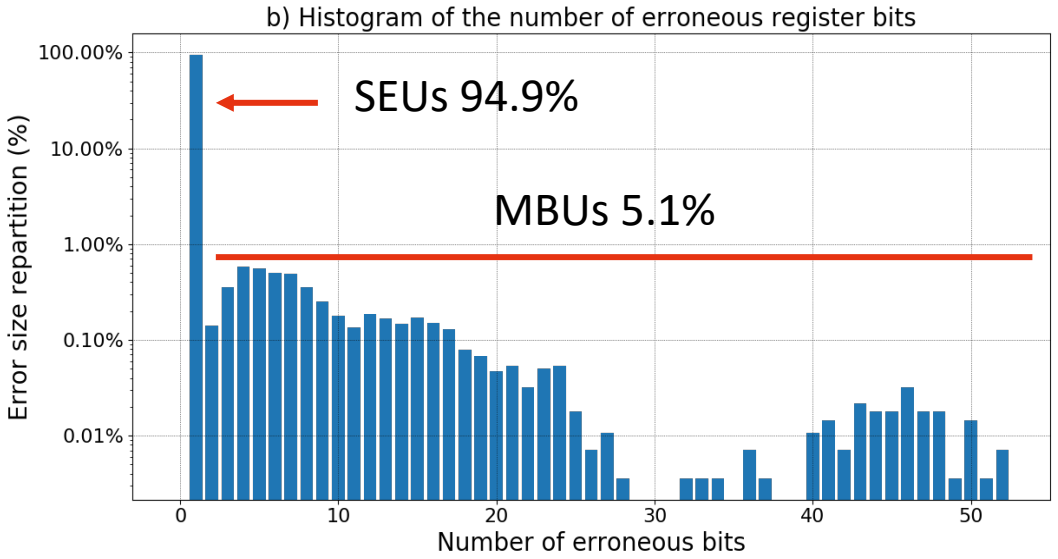


Results: Comet Execution Stage

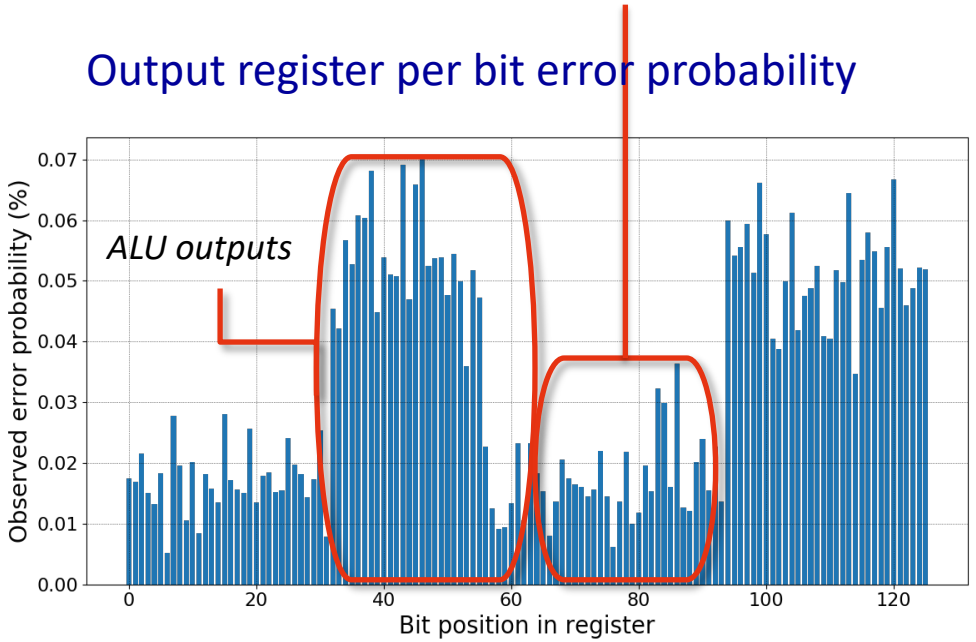
- Logging patterns and error probability (SEUs + MBUs)

Dest. Register, Opcode Forwarding, etc.

Number of erroneous bits in output register



Output register per bit error probability



- Patterns used during Microarchitectural-Level Fault Injection

Results: Comet Execution Stage

- Influence of SET Width and Frequency on MBUs
  - Fixed width (400ps)

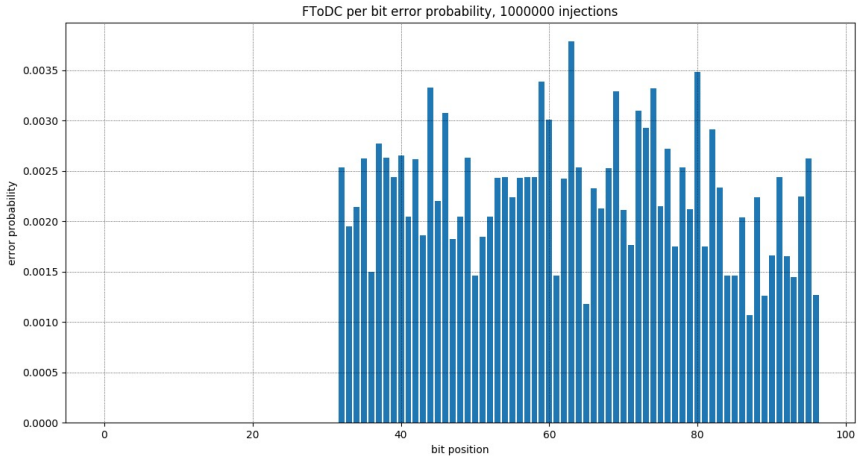
Freq.	200 MHz	300 MHz	400 MHz	500 MHz	600 MHz
SEU	9,308 93%	15,592 96.3%	23,613 94.1%	26,489 94.9%	30,919 95.5%
MBU	699 7%	599 3.7%	1,473 5.9%	1429 5.1%	1,447 4.5%

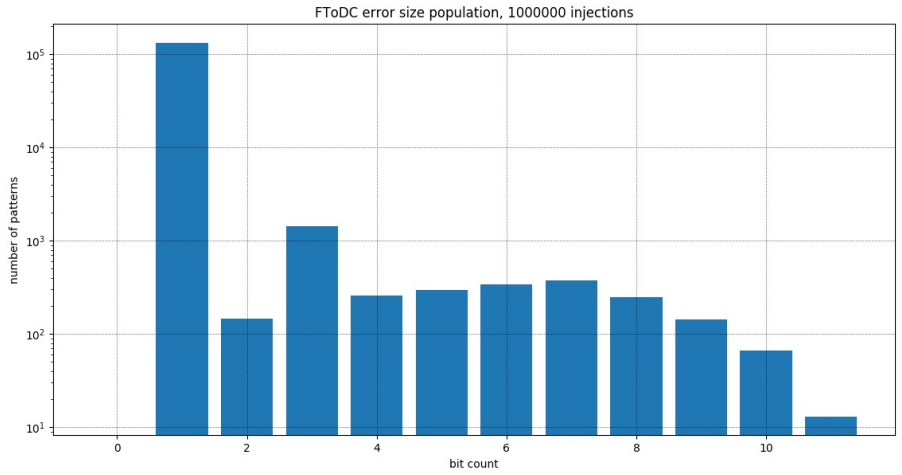
  - Fixed frequency (500MHz)

SET	100 ps	200 ps	400 ps	500 ps
SEU	5,144 97.6%	10,529 95.3%	26,489 94.9%	33,449 95.9%
MBU	127 2.4%	755 4.7%	1429 5.1%	1,432 4.1%

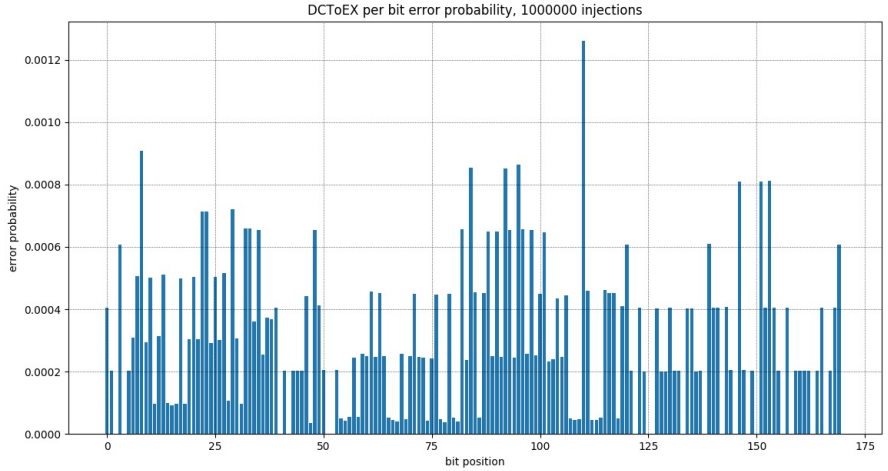
Results: Other Comet Stages

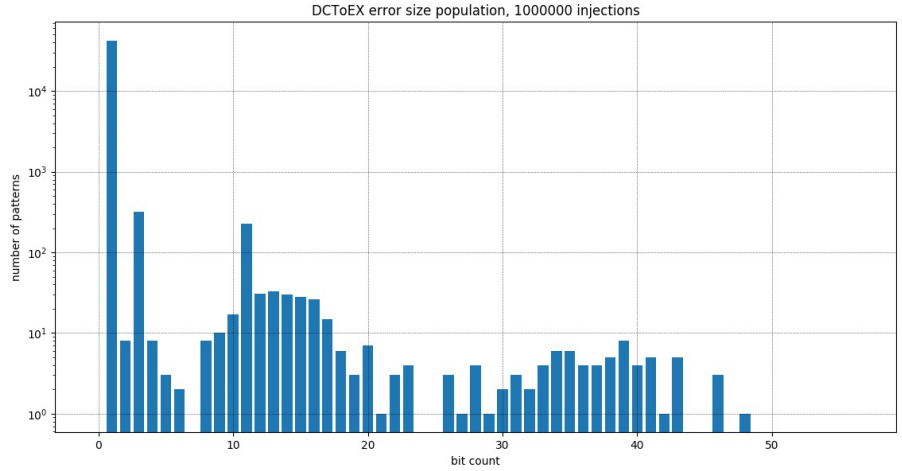
- FtoDC





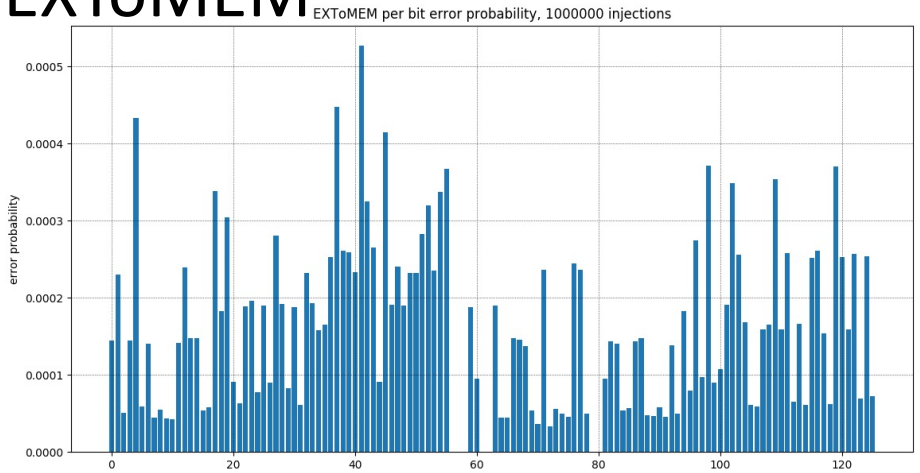
- DCToEX

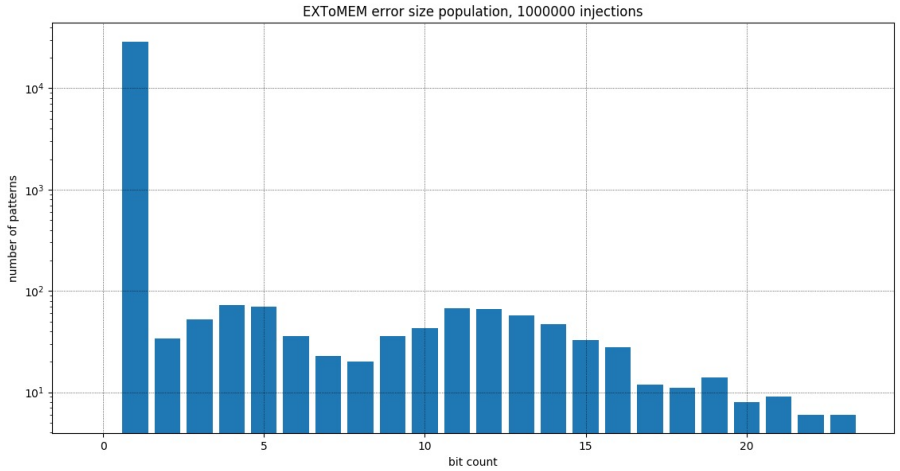




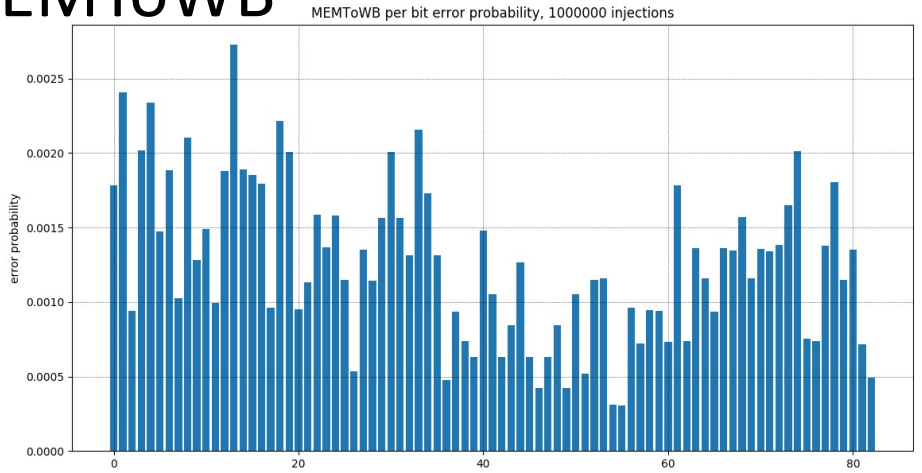
Results: Other Comet Stages

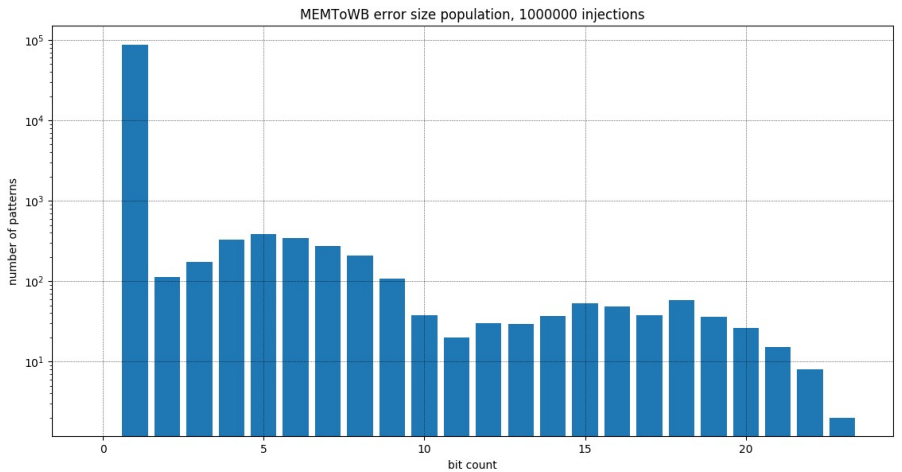
- EXToMEM



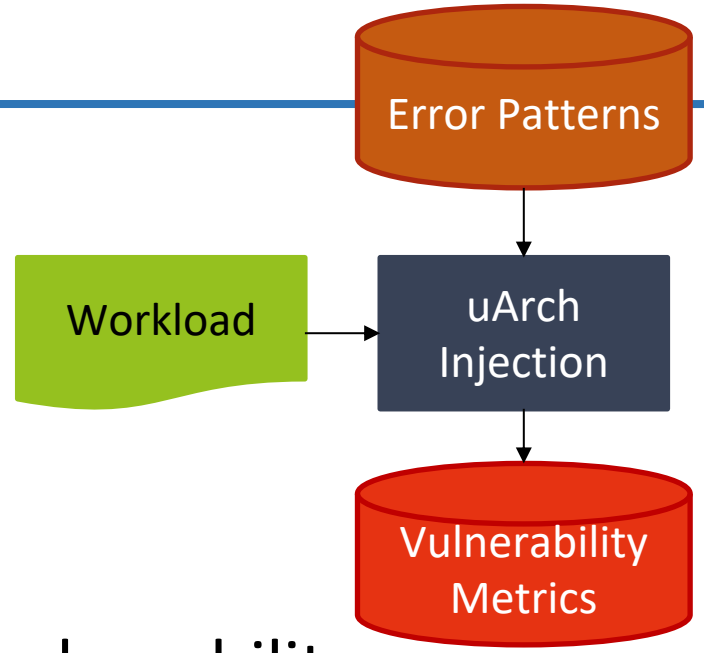


- MEMToWB





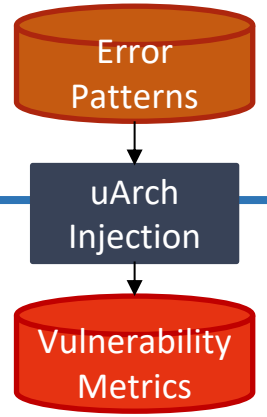
Microarchitectural-Level Fault Injection: Vulnerability Analysis



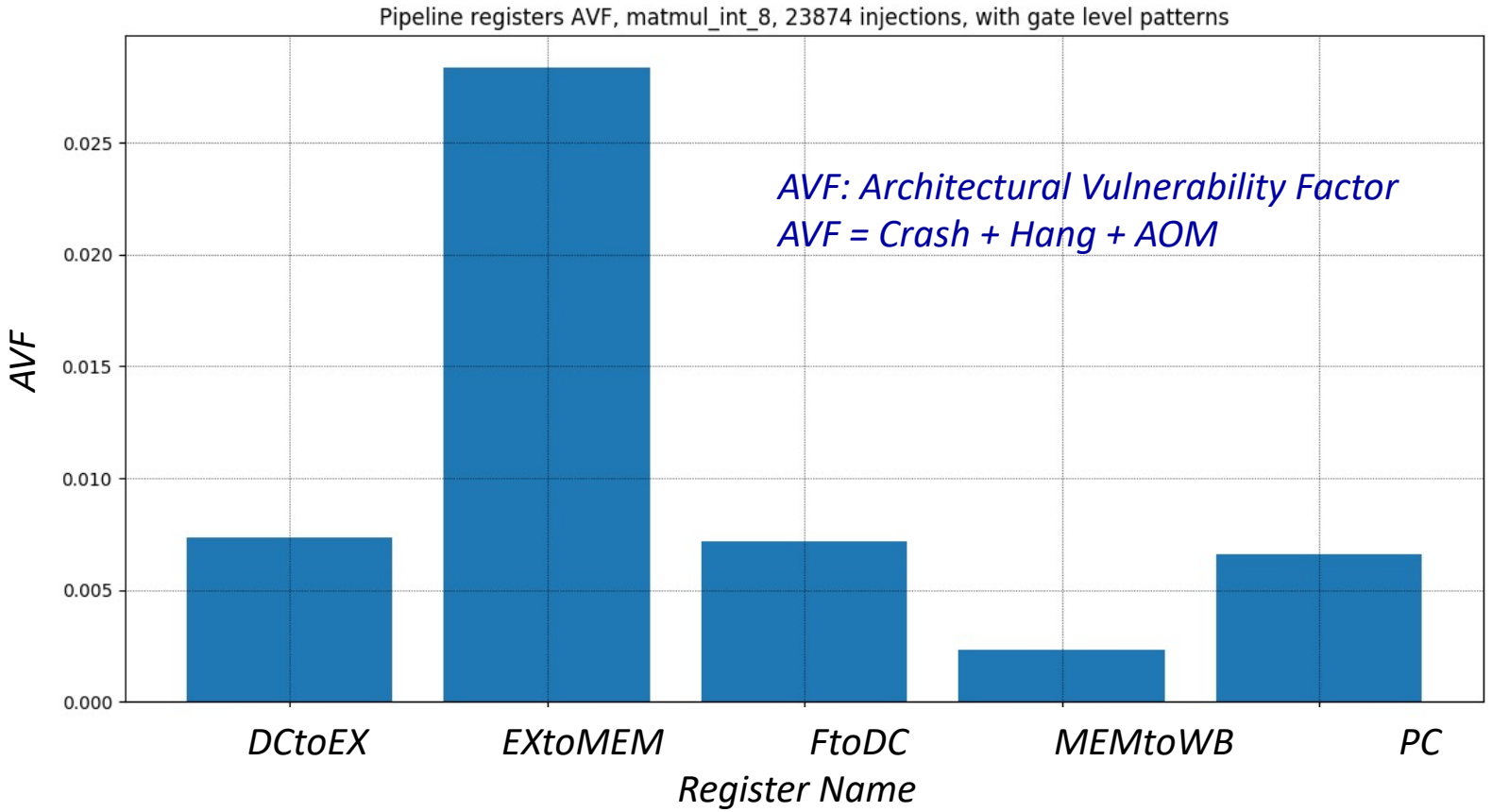
- Augmented Comet simulator used for fault injection
- Injection is guided by:
  - i) area of the different pipeline stages
  - ii) gate-level fault patterns
- Architectural Vulnerability Factor (AVF) analyzes the vulnerability of a processor through the probability of fault classes appearing during the execution of a given workload
- Fault classes considered:
  - Crashes and Hangs
  - ISM, AOM, ISM & AOM

ISM: Internal State Mismatch
AOM: Application Output Mismatch

Results: Microarchitectural-Level Fault Injection

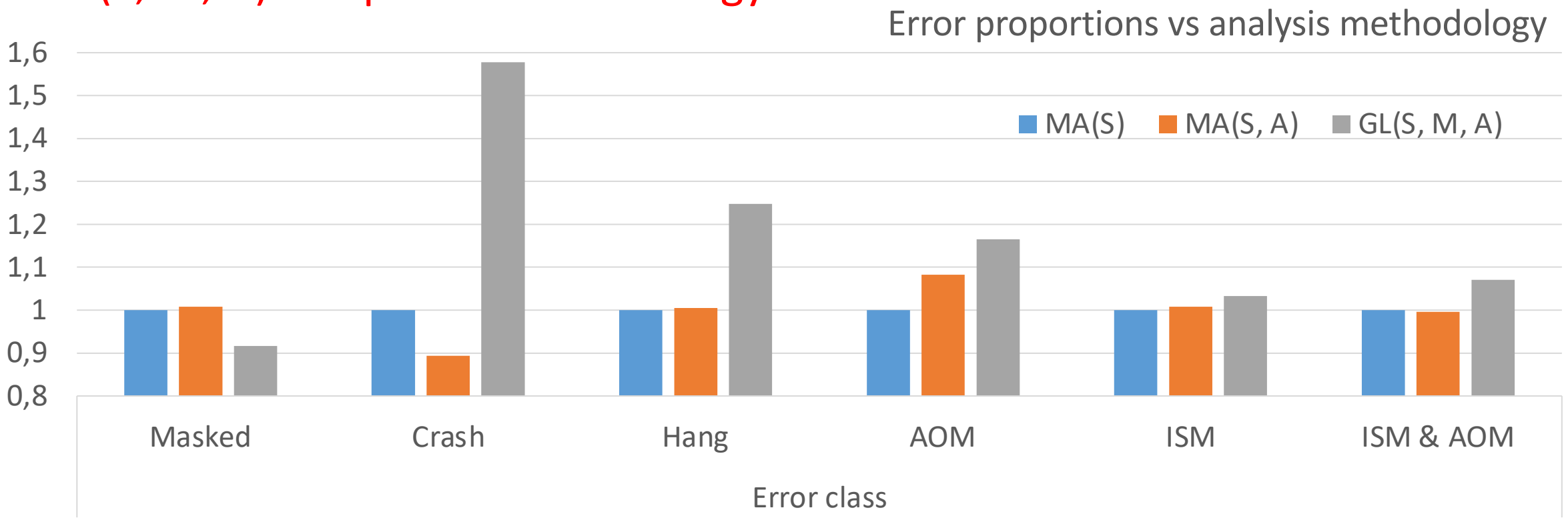


- AVF of microarchitecture registers
  - with gate-level patterns (SEU+MBU)



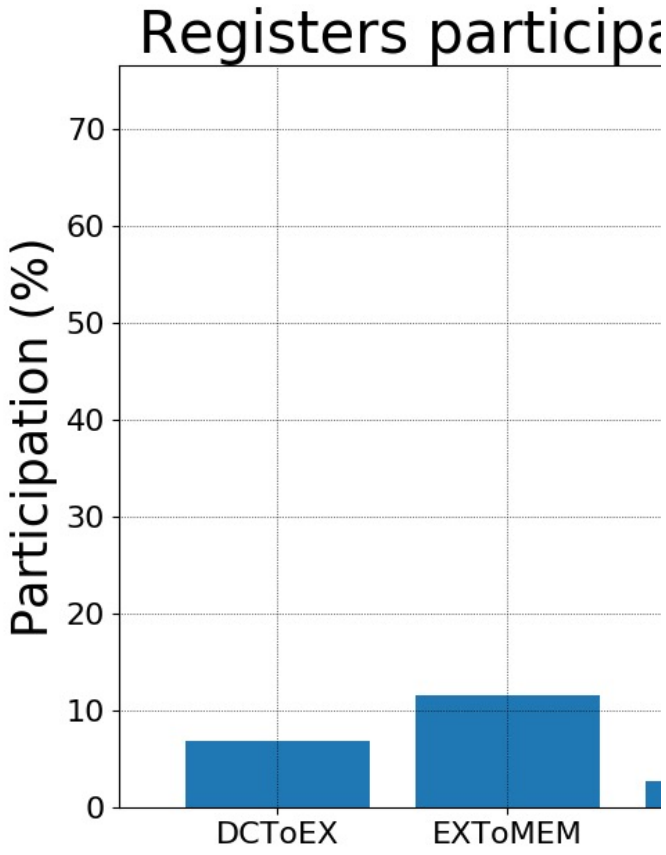
Comet Vulnerability Analysis Results

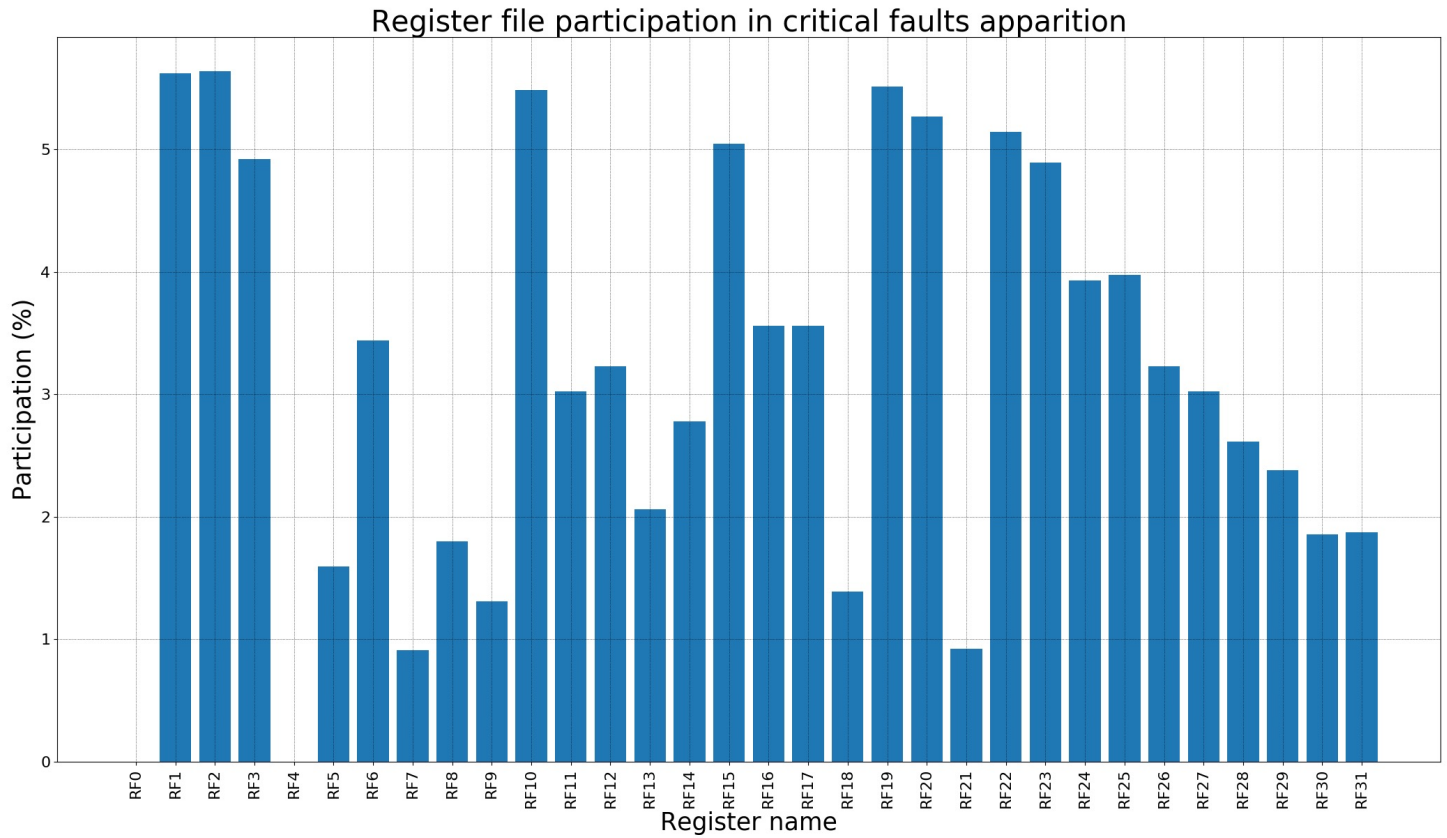
- MA(S): SEUs only, uniform error probability
- MA(S, A): SEUs only, error probabilities based on pipeline area
- GL(S, M, A): Proposed methodology



Fine-Grain Vulnerability Analysis

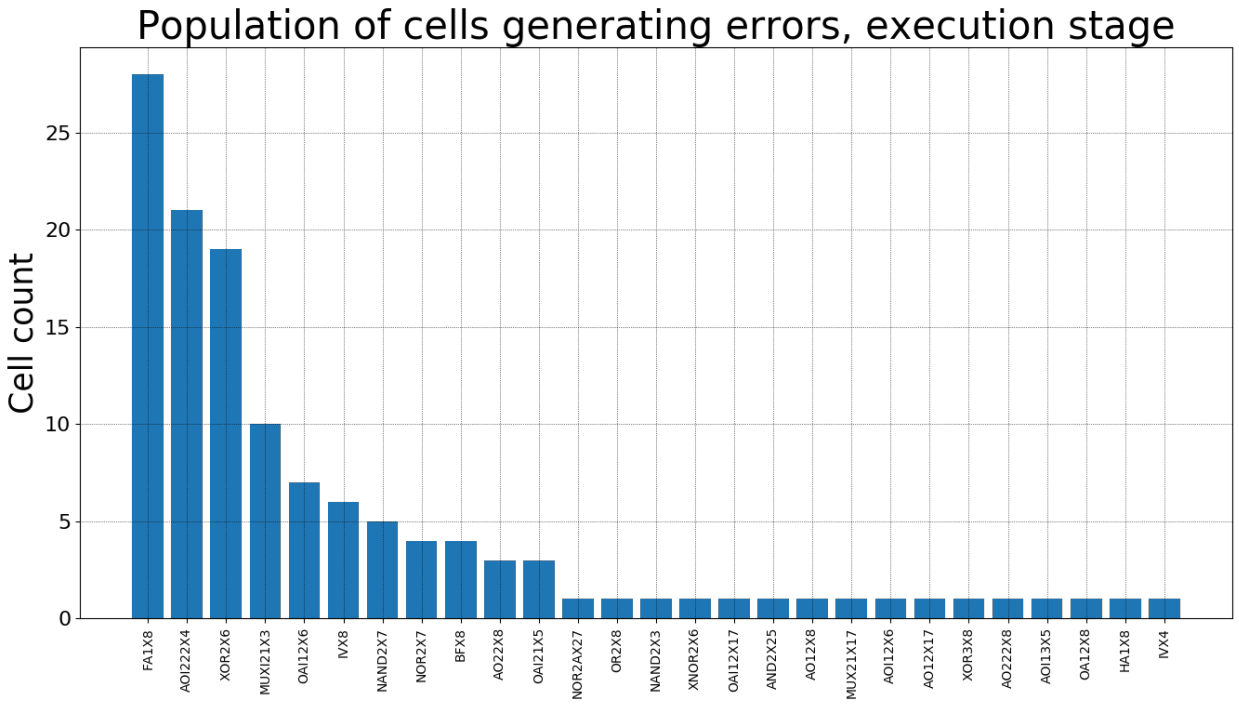
- Impact on registers



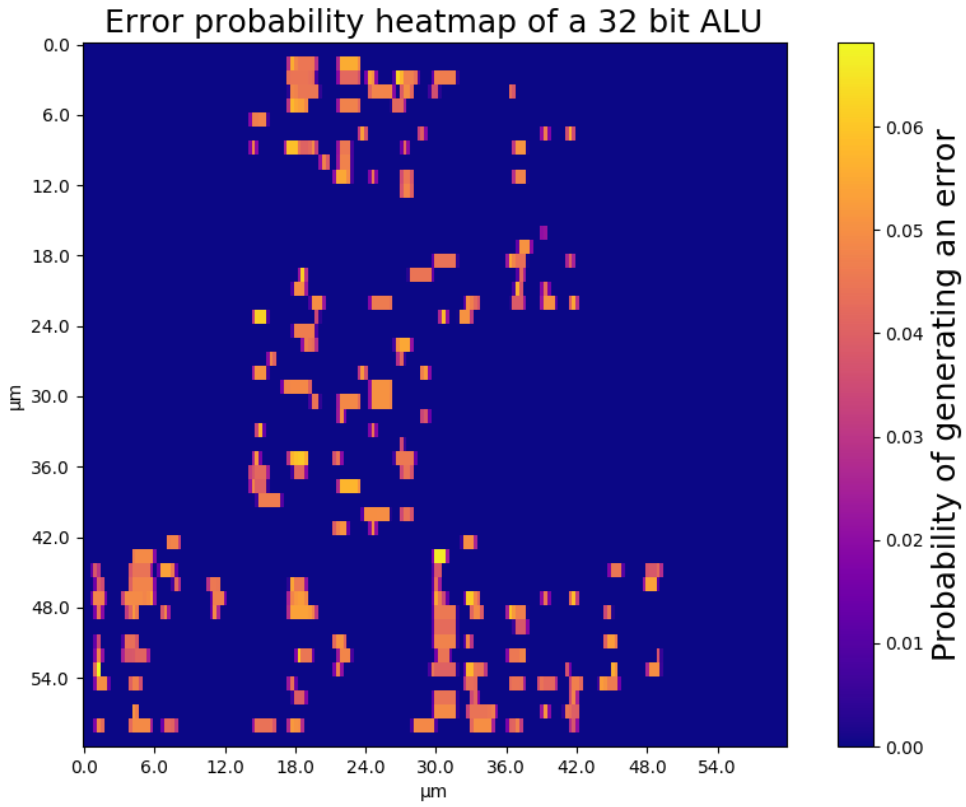


Fine-Grain Vulnerability Analysis

- Trace-back information of AVF down to gate-level
  - Identification of critical area
  - Guiding exploration of design space when adding fault-tolerance techniques

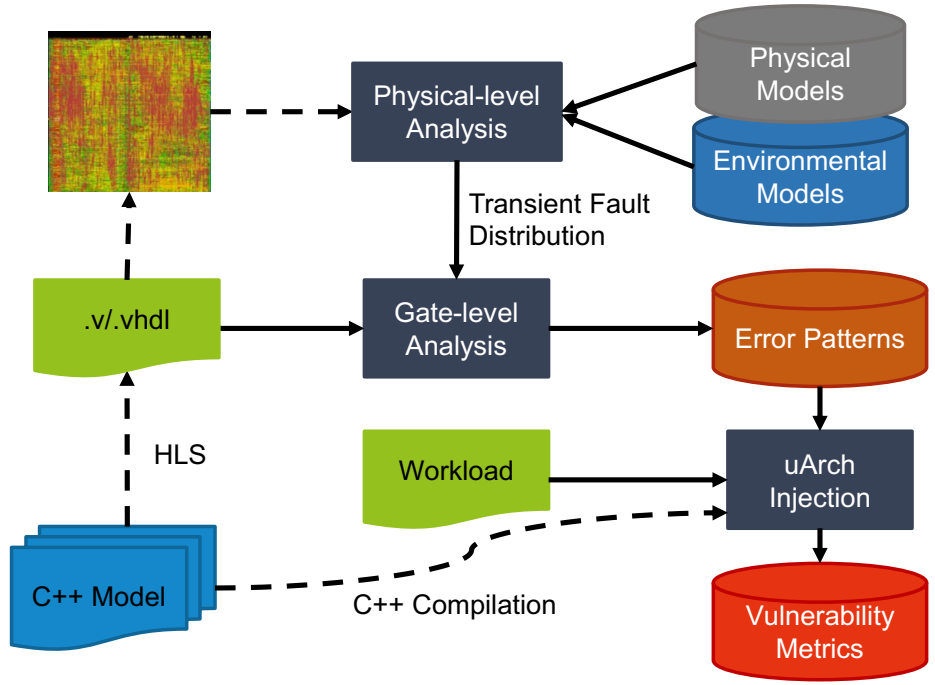


heatmap of vulnerability



Conclusion

- More refined physics for nanoscale technologies
  - Physical fault injection at transistor and gate levels
- MBUs are present and are here to stay
- MBUs significantly impact AVF
  - More than 50% of critical errors (crashes & hangs)
- Fault injection methodology and flow
  - From Physics to gates to microarchitecture
  - Conscious of MBU patterns and error probability
- More complex processor designs
- Guiding Design Space Exploration
  - of architecture-level fault-tolerant techniques
- Physical fault injection on FPGA cell models



Vulnerability Analysis of Embedded Digital Systems: from Physics to Microarchitecture

Olivier Sentieys
Univ. Rennes, Inria, IRISA
olivier.sentieys@inria.fr

collaboration with Joseph Paturel, Angeliki Kritikakou, IRISA,
and Guillaume Hubert, ONERA, Toulouse

References

[1] N. J. Wang et al., “Examining ace analysis reliability estimates using fault-injection,” SIGARCH Comput. Archit. News, vol. 35, p. 460–469, June 2007.

[2] Y. Xie et al., “An Automated FPGA-Based Fault Injection Platform for Granularly-Pipelined Fault Tolerant CORDIC,” in Int. Conf. on Field-Programmable Technology (FPT), pp. 370–373, Dec. 2018.

[3] B. Mutlu et al., “Characterization of the Impact of Soft Errors on Iterative Methods,” in IEEE Int. Conf. on High Performance Computing (HiPC), pp. 203–214, Dec. 2018.

[4] C. Mao et al., “An Automated Fault Injection Platform for Fault Tolerant FFT Implemented in SRAM-Based FPGA,” in IEEE Int. System-on-Chip Conf. (SOCC), pp. 192–196, Sept. 2018.

[5] N. N. Mahatme et al., “Comparison of Combinational and Sequential Error Rates for a Deep Submicron Process,” IEEE Trans. on Nuclear Science, vol. 58, pp. 2719–2725, Dec. 2011.