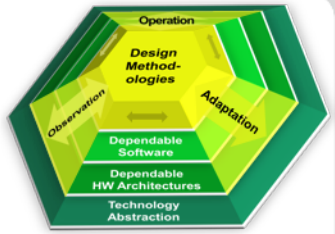
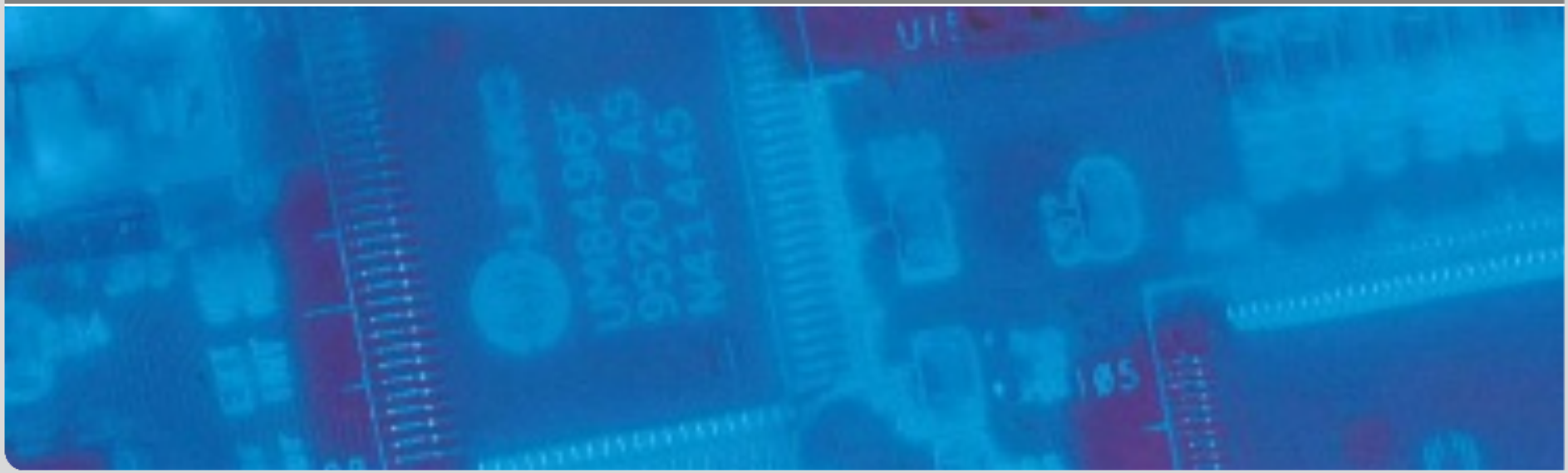


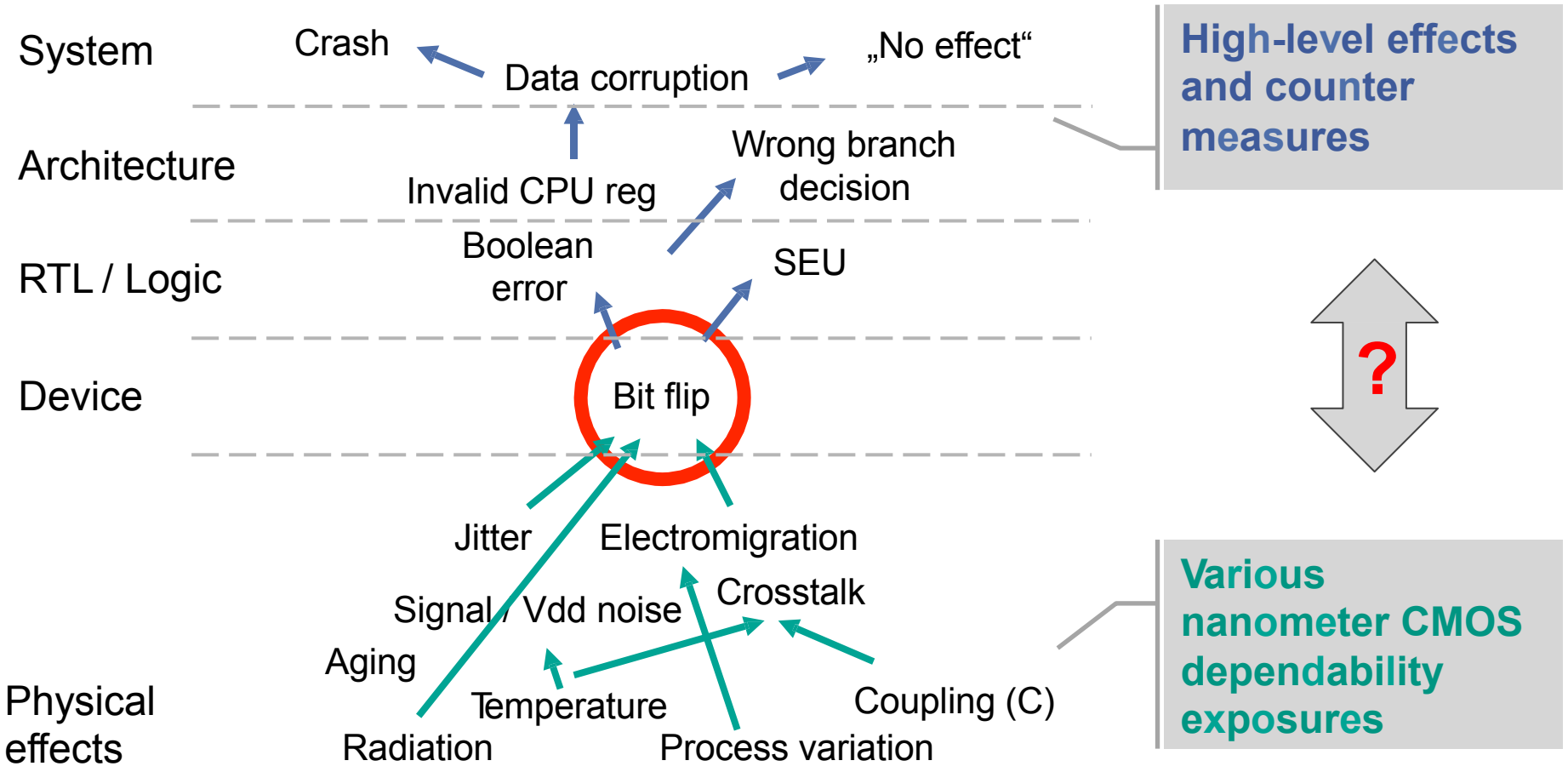
SPP1500: Hardware and Platforms:

- MIMODeS: Christina Gimmler-Dumont, Stefan Weithoffer, Norbert Wehn
- LIFT: Michael Balszun, Veit Kleeberger, Samarjit Chakraborty, Ulf Schlichtmann
- ARES: Johannes Maximilian Kühn, Wolfgang Rosenstiel

SPP1500.itec.kit.edu

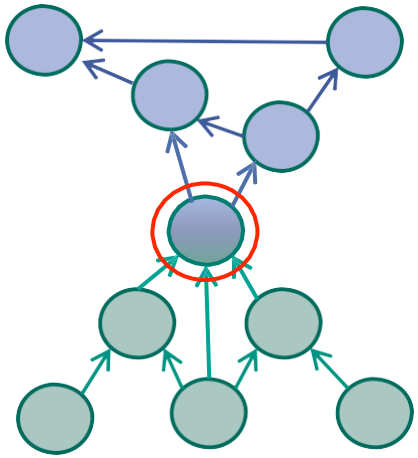


Resilience Articulation Point (RAP) Model



Principal RAP Pillars

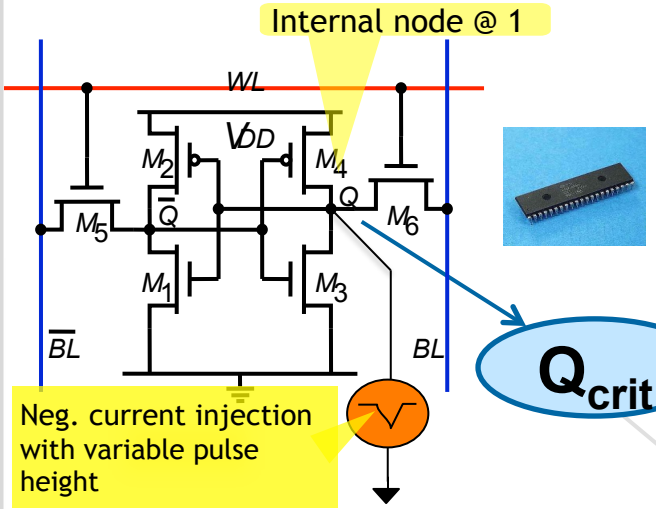
- Fault from various physical effects, if not masked, will manifest as permanent or transient single or multi-**bit invalidations**
- Probabilistic error functions are used to encapsulate and model different physical effects resulting in bit-flips
- Transformation functions convert probabilistic error functions towards higher abstraction levels

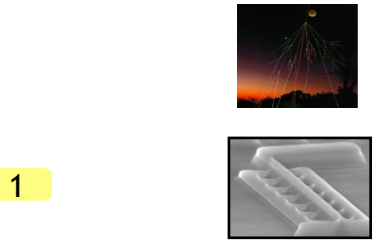


- Error and transformation functions aren‘t integral parts of the RAP model

System Failure Analysis

Technology Level (Fault) Model





Device parameters, Cosmic radiation, NBTI, SEU/SET, thermal stress, …

Induced charge distribution

Q_{crit}

Calculation of **Bit flip** probability (temporal / spatial)

System Level

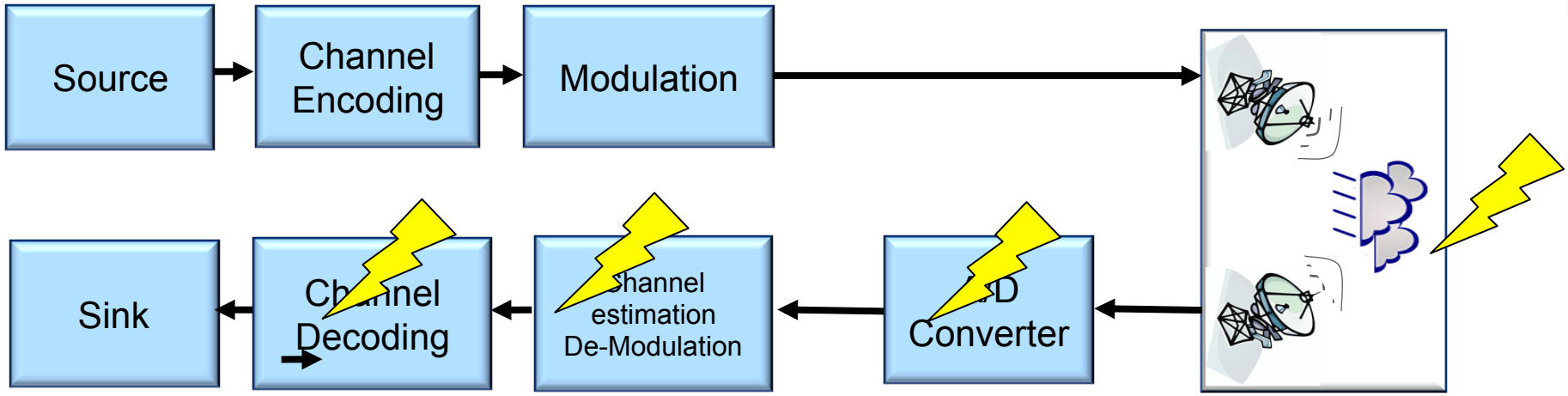
Instruction Level

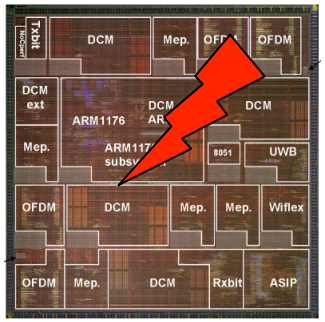
RT Level

Circuit Level

Technology Level

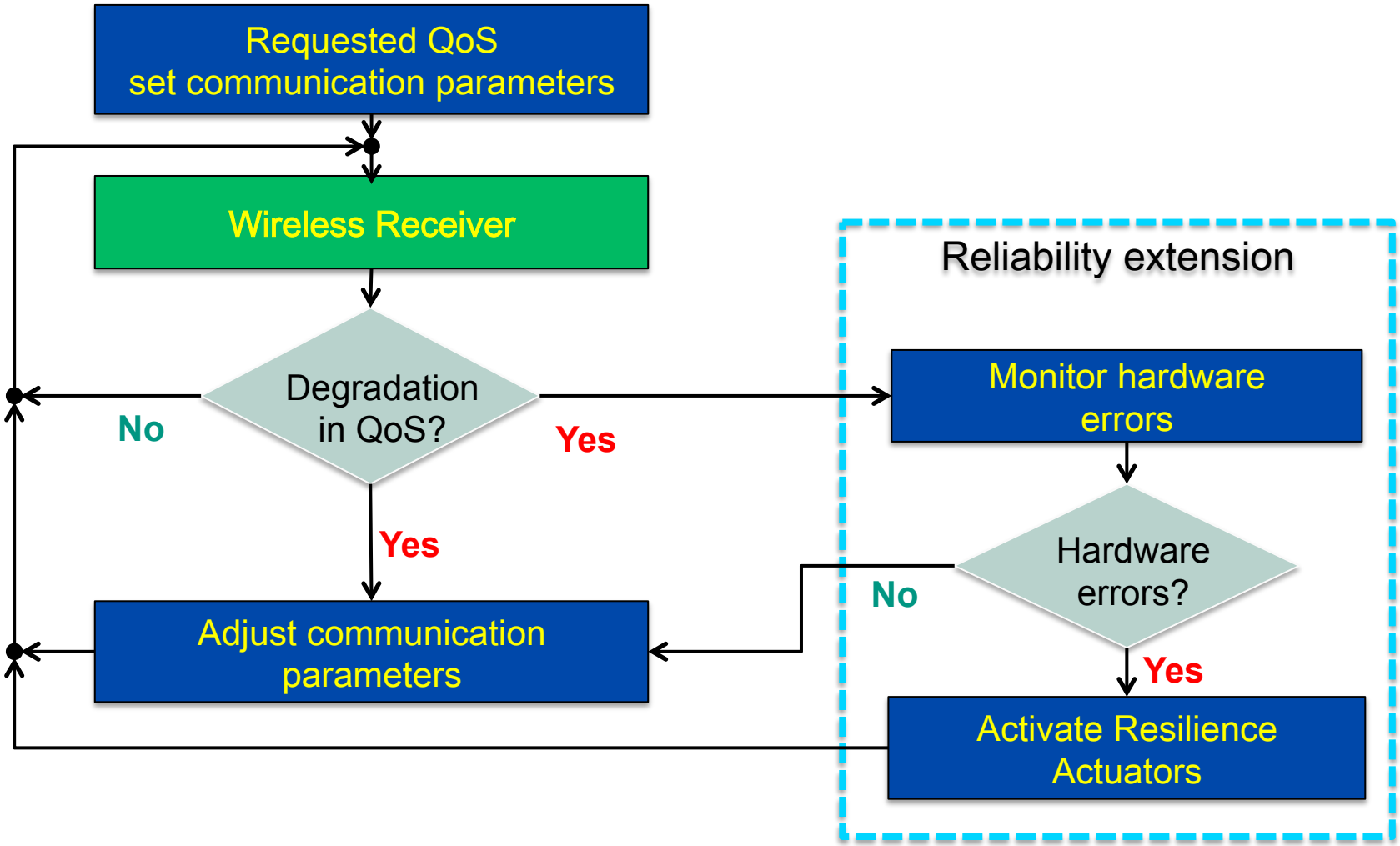
Wireless Communication System



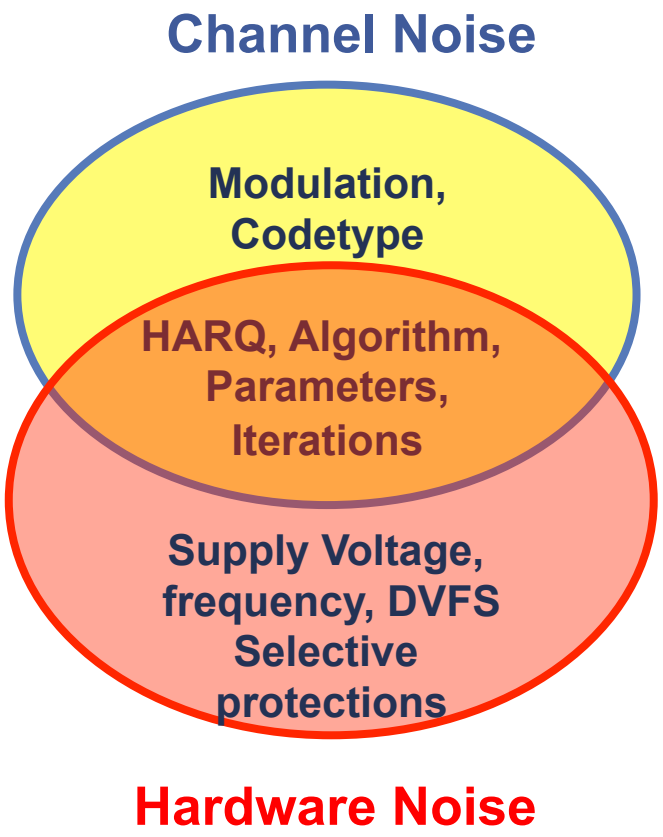


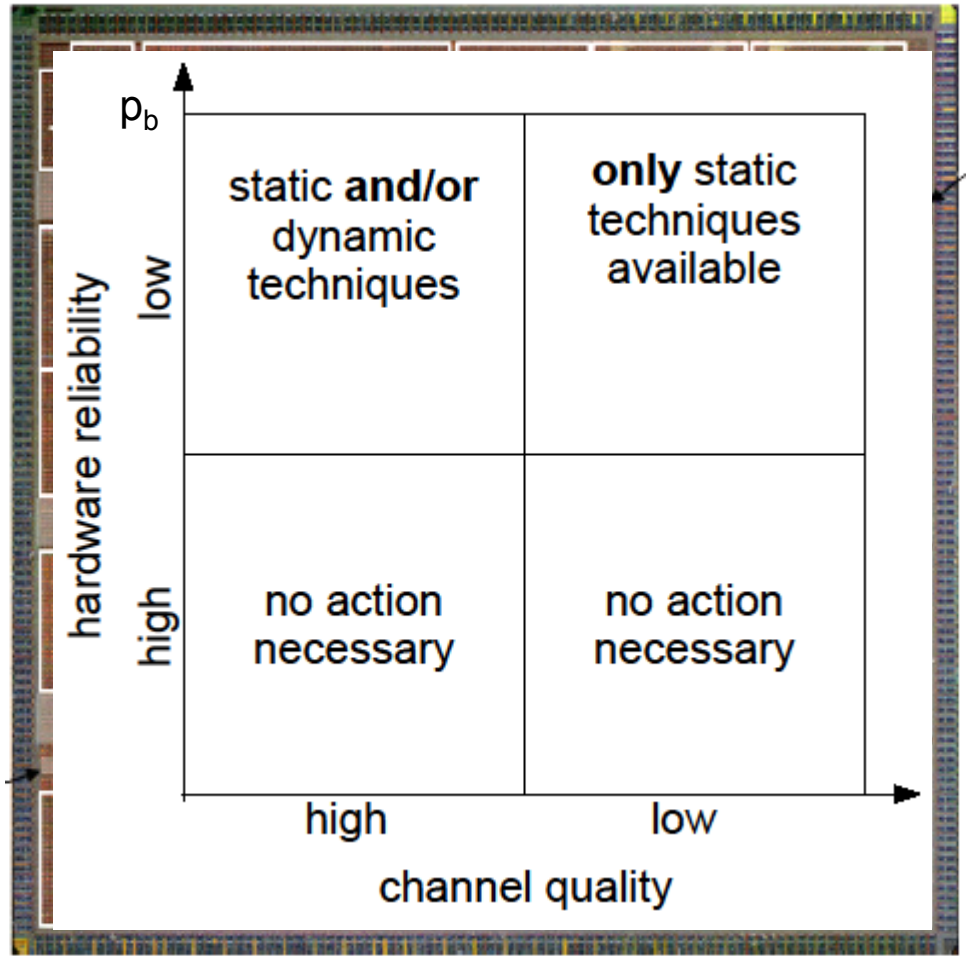
Noise = *noise(communication)*
+ *noise(suboptimal algorithms)*
+ *noise(quantization)*
+ *noise(technology layer)*

Modified QoS Communication Flow

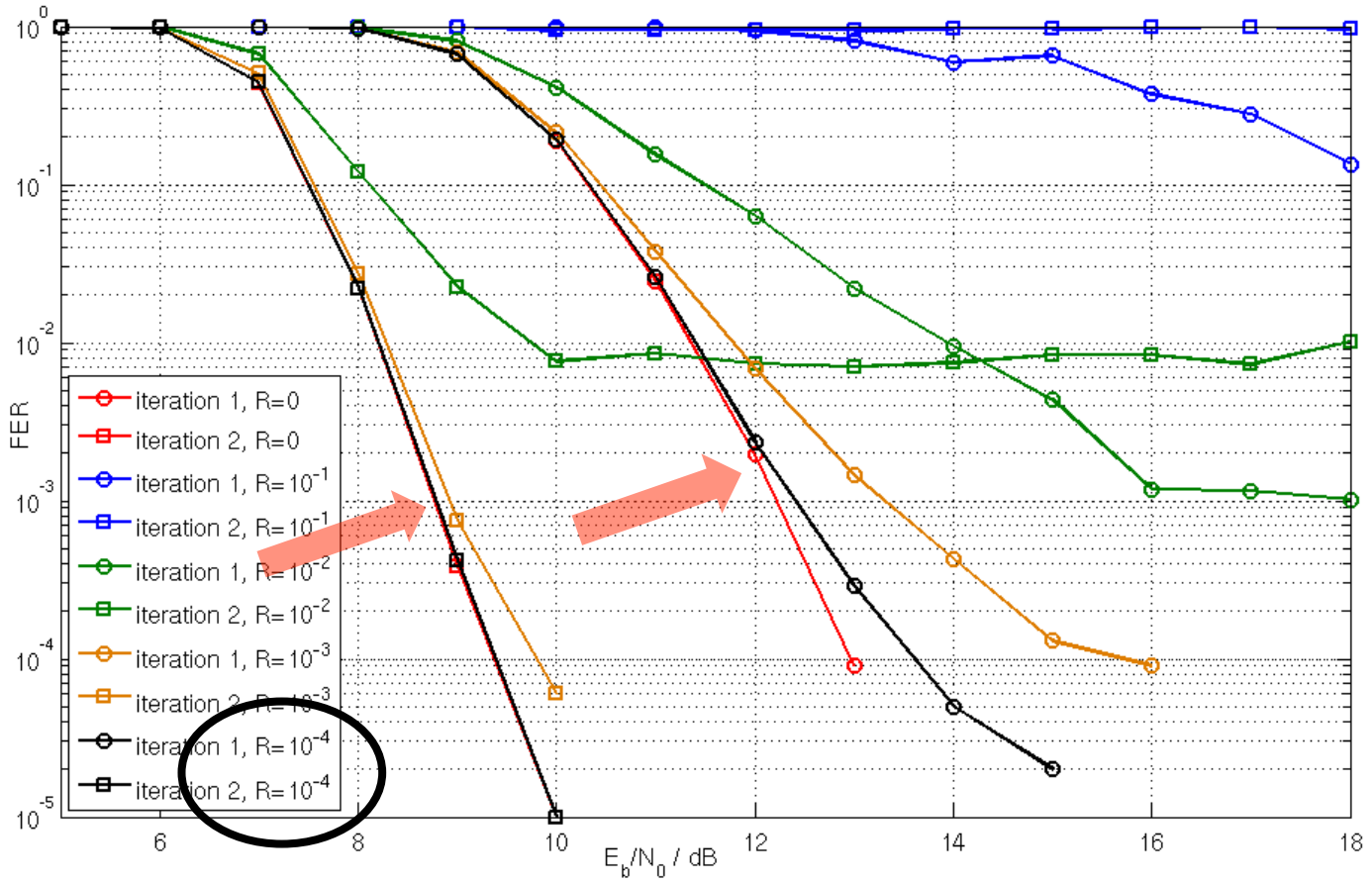


Hardware Error Mitigation Space





Memory Errors MAT_H

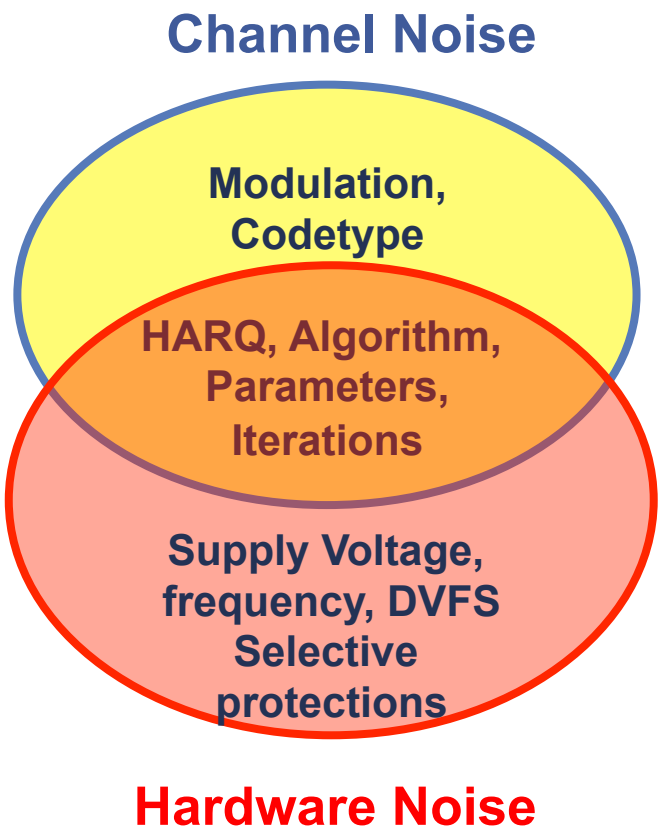


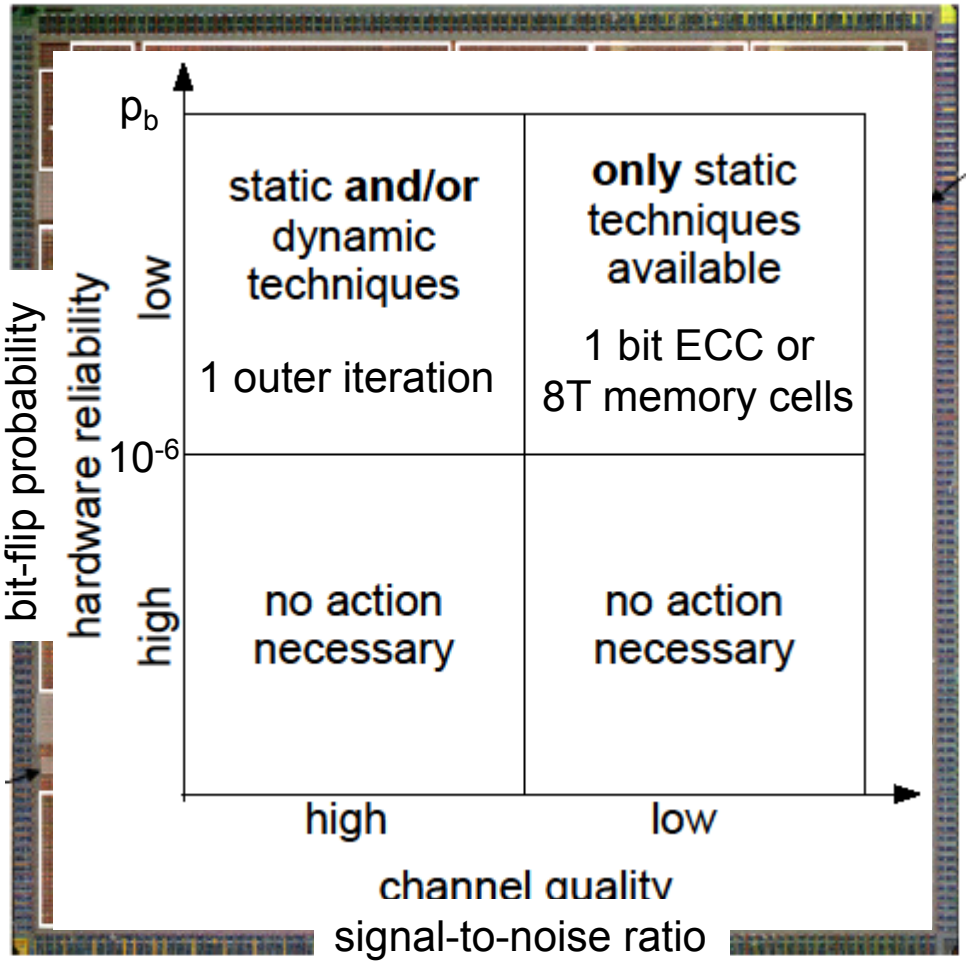
- Inherent system error resilience below memory error rate 10^{-4}

Memory Resilience Actuators MAT_H

resilience actuator	impacts	robustness against supply voltage variations	(dis-)advantages
algorithmic error resilience	area +0% power +0% throughput -0%	-200mV supply voltage	
1 outer iteration	area +0% power +0% throughput -75%	-300mV supply voltage	+ requires no change of existing hardware architecture + dynamic - throughput loss and reduction of energy efficiency
1-bit error correction code	area +30% power +30% throughput -0%	-400mV supply voltage	- static area and power increase + corrects all single bit flips
8T memory cells	area +25% power +0% throughput -0%	-400mV supply voltage	- static area increase + very robust
hybrid 6T/8T memory cells	for DEC_IN area +5% power +0% throughput -0%		+ low area increase - detailed characterization of each memory mandatory

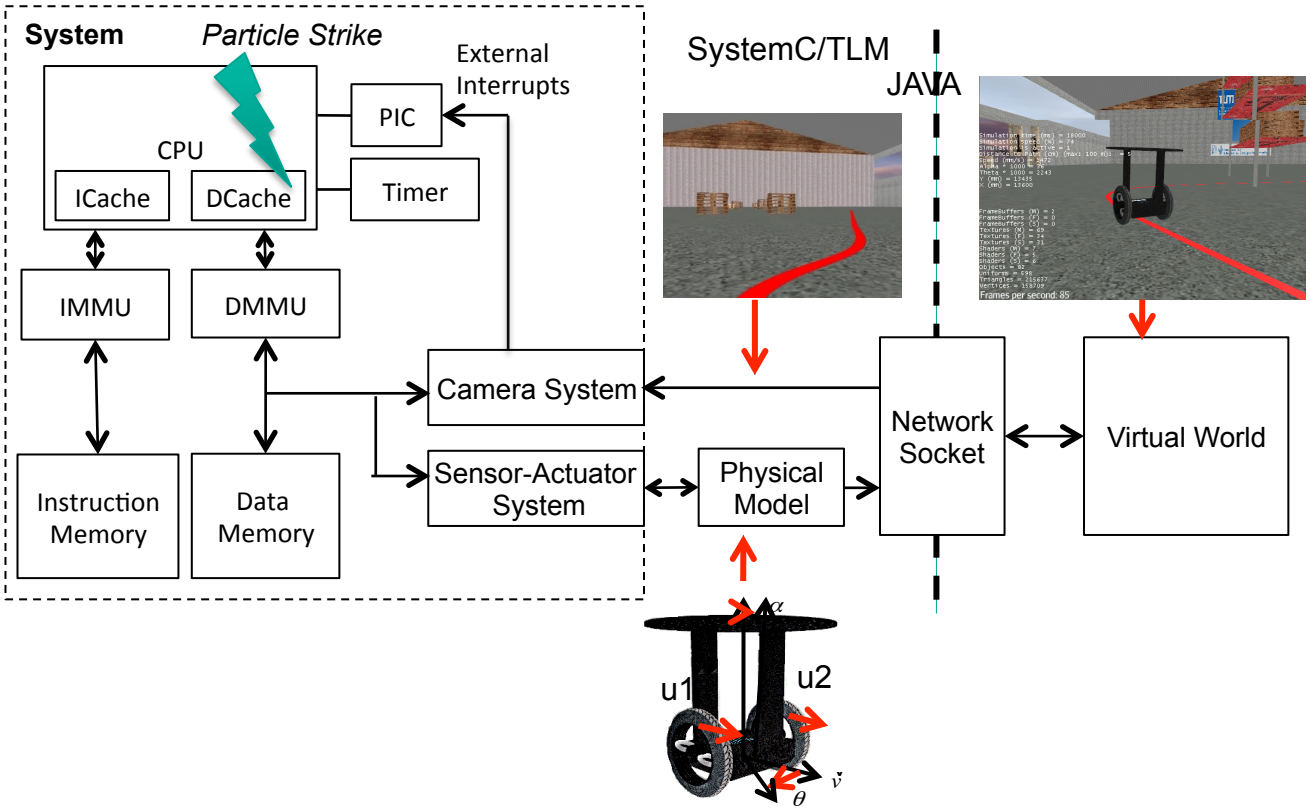
Hardware Error Mitigation Space





System Failure Analysis

Virtual Prototype of a two-wheeled robot



System Level

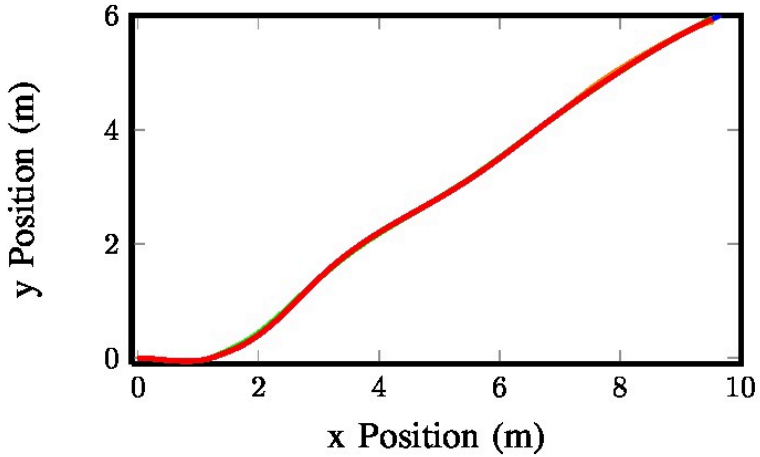
Instruction Level

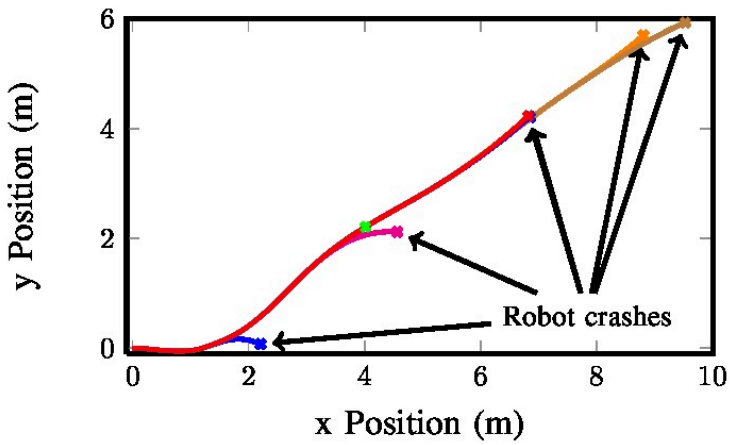
RT Level

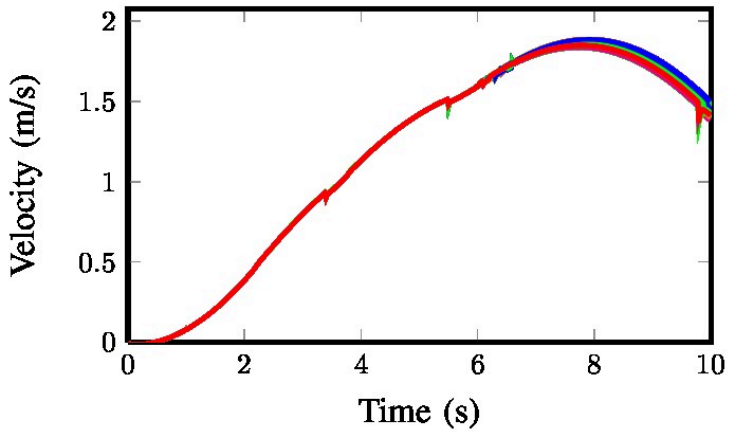
Circuit Level

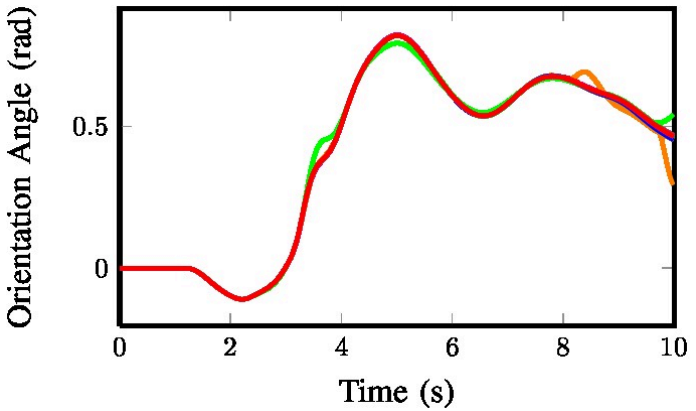
Technology Level

Qualitative Evaluation



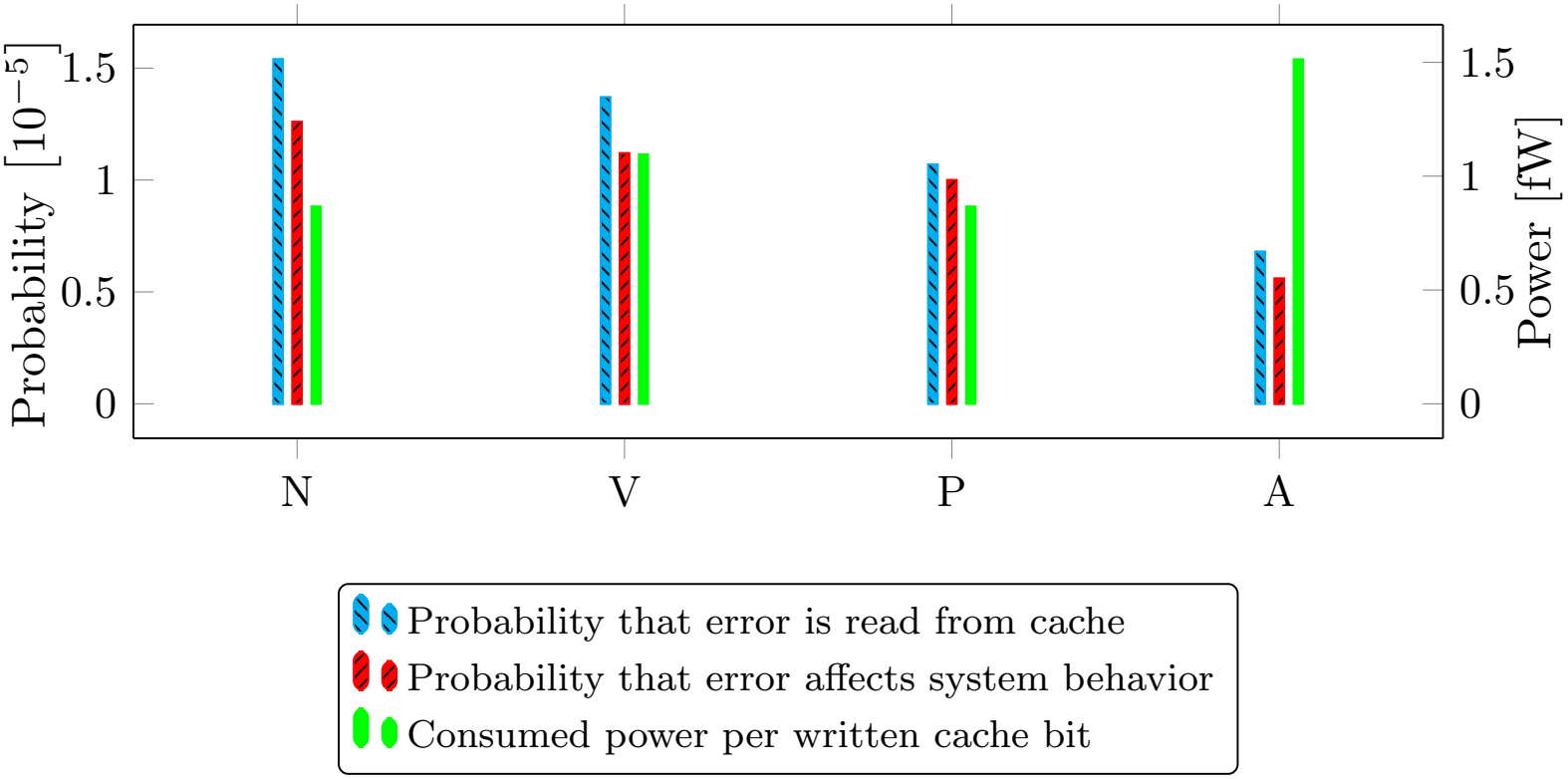






System Failure Analysis

Error Probabilities for 10 seconds simulated real-time



N: Nominal
V: Hardened by +10% VDD
A: Hardened by double area per cell
P: 1-bit parity and write-through mode

ARES Project

Challenge

Increasing reliability costs for SoCs

Proposed Solution

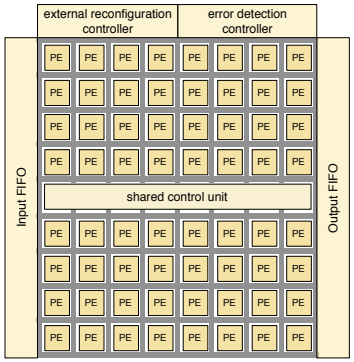
Using coarse grained reconfigurable architectures (CGRAs) as reliability enhancer

Goals

- Avoid inclusion of additional circuits
- Graceful degradation
- Adaptive reliability

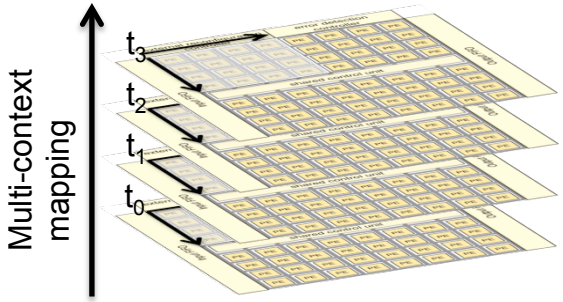
Background

CGRAs



- Array of Processing Elements (PEs)
- Interconnection network
- PE: FUs, register-set, context-memory

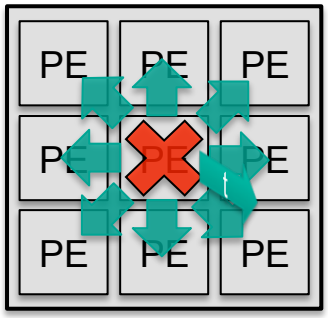
Benefits of CGRAs



- Fast reconfiguration mechanism
- Multi-context mapping
- Inherent redundancy

Contributions (1)

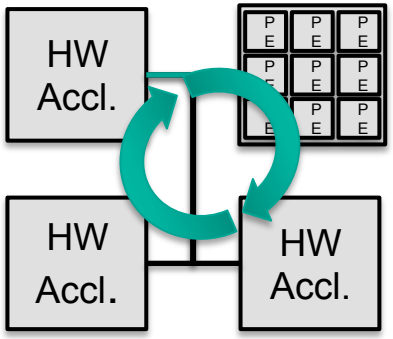
Reliability Method (1)



Hardening of the CGRA

- Low cost TMR method
  - Exploiting inherent redundancy
- Dynamic remapping
  - Adapt routing for defective PEs

Reliability Method (2)

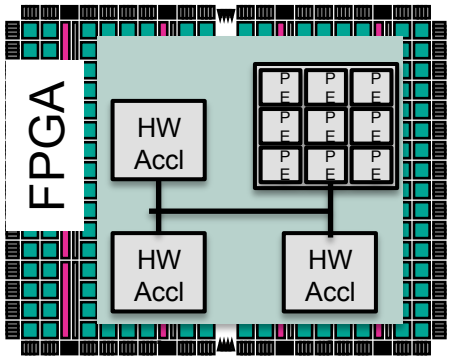


Hardening of the SoC

- Dynamic Functional Verification (DFV) to sample hardware accelerators

Contributions (2)

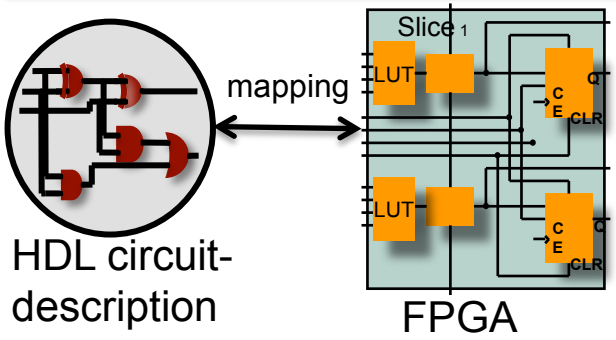
SoC Prototype



Validation of the proposed methods

- Excessive simulation times
- FPGA-based SoC Prototype
- Gaisler Research SoC platform

Fault Analysis Tool



- StML (Static Mapping Library)
- Combines advantages of hardware-based and simulation-based fault injection approaches

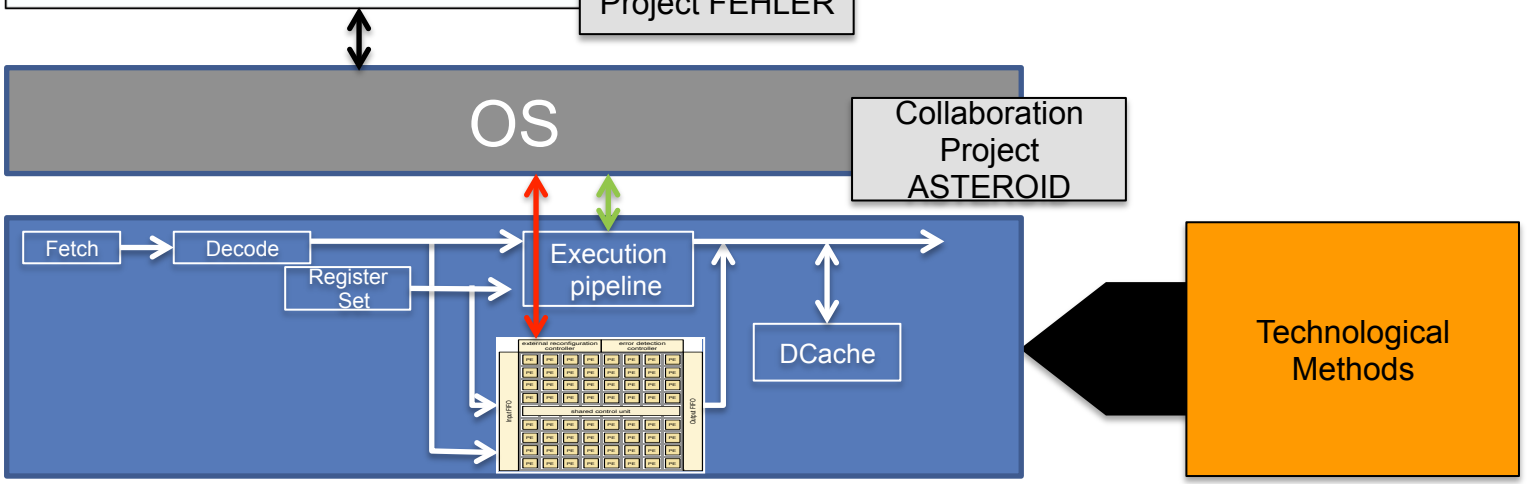
Future Work

Cross-Layer Approach

- Hardening of the processor
- Connecting to OS/Application
- Technological methods

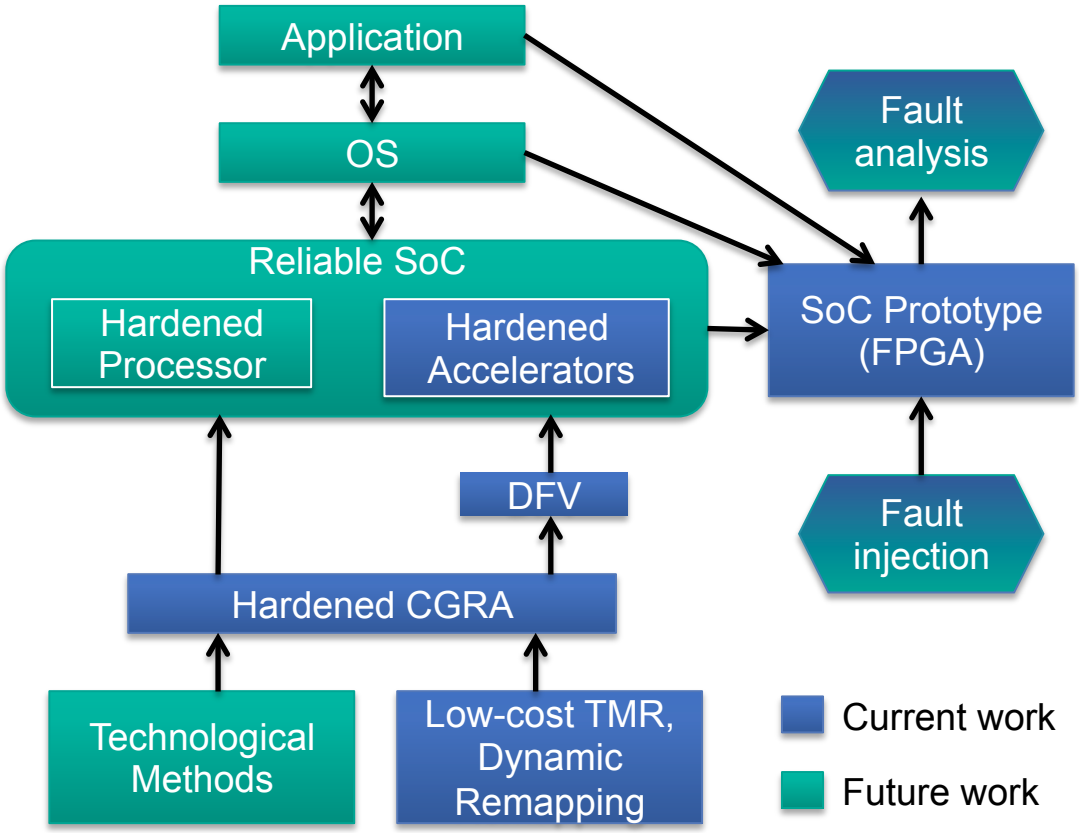
```
/* Piece of software */
reliable int foo = 42;
int bar = 23;

unreliable int compute_unimportant_stuff (…) {
                …
}

reliable int very_important_stuff (…) {
                …
}
…
```

Collaboration Project FEHLER



Conclusion

ARES Project



- Adaptive methods to secure parts of a SoC using CGRAs
- Fault simulation and analysis methods
- We aim to include methods to secure (embedded) CPUs
- We propose a comprehensive cross-layer approach