SafeGantana: A Lockstep In-Order RISC-V Core

Marc Grau Fornt

mgrauifo@bsc.es

Sergi Alcaide[1], Juan Carlos Rodriguez[1], Marcel Sarraseca[1], Francisco Fuentes[1], Omar Alymlahi[1], Feng Chang[1], Ilham Lasfar[1], Francisco J. Cazorla[1], Ramon Canal[1,2], Jaume Abella[1]

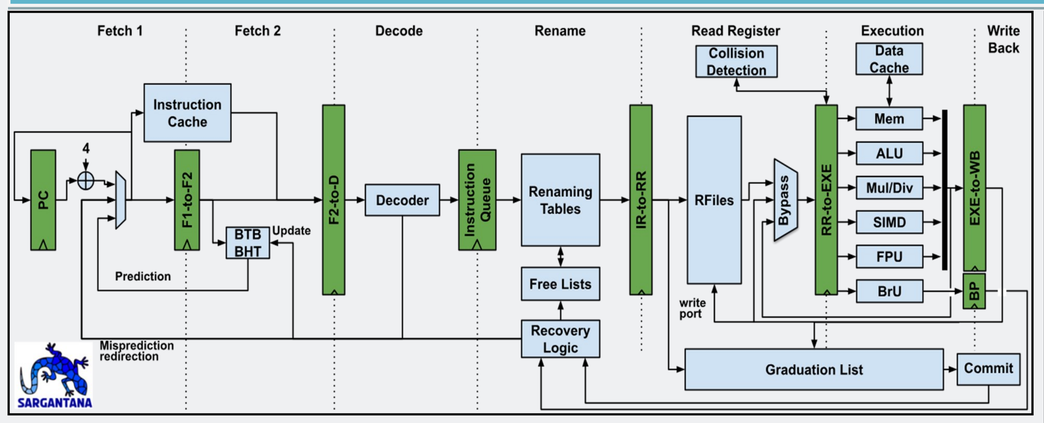
Barcelona Supercomputing Center
Centro Nacional de Supercomputación

[1]Barcelona Supercomputing Center (BSC)
Barcelona, Spain

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

[2]Universitat Politècnica de Catalunya (UPC)
Barcelona, Spain

Introduction



- **SARGANTANA:** An open-source RISC-V core, which we aim at **making the basis** for our safety-relevant SoC.
- A 7-stage in-order 64-bit RISC-V core implementing the RV64G ISA.
- With Single Instruction Multiple Data (SIMD) unit for acceleration purposes.

⇨ 2.44 CoreMark/MHz

- Safety requirements can be found in a lot of domains

- **Safety-critical systems** need to meet specific requirements related to funcional safety and prove them in exhaustive verifcation and validation (V&V) processes

{ Detect faults / Prevent hazardous situations ⇨ System components reach the highest integrity levels (e.g., ASIL-D in automotive)

- Most used fault detection technique is **redundancy**
- **Common Cause Failures (CCFs)** occur when a fault produces identical errors in redundant elements.
- The generation of identical errors by the CCFs make the detection of error impossible with only redundancy.
- Safety mechanisms are required for detecting Common Cause Failures.

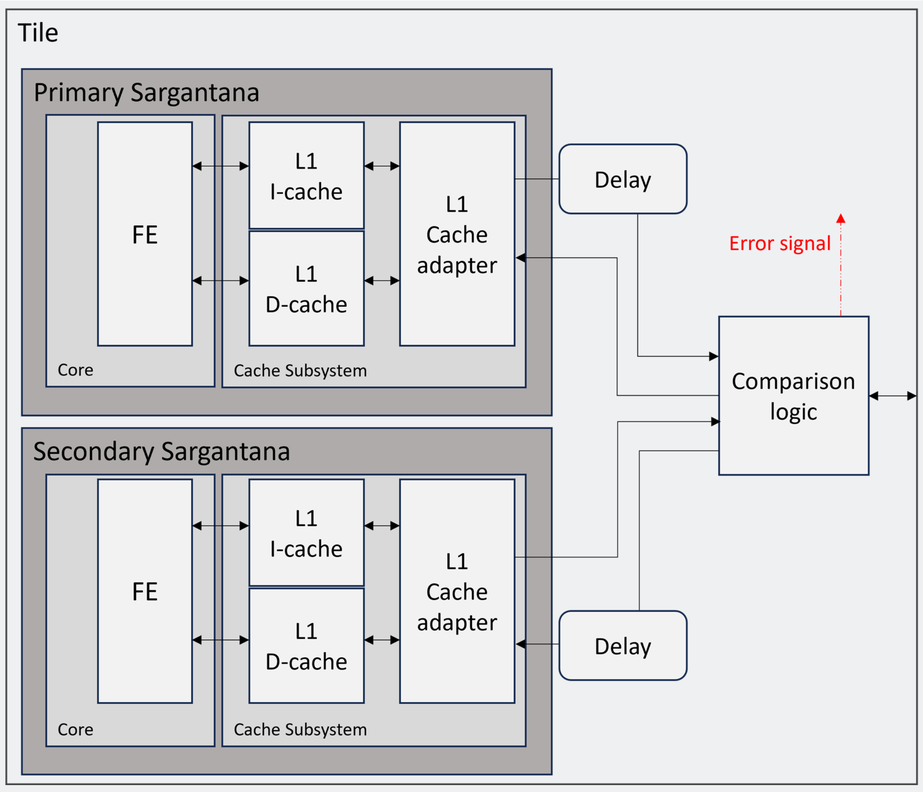
⇨ **Diverse redundancy** is mandatory

- Most common diverse redundancy scheme is to employ a Dual Core Lockstep (DCLS)
  - 2 identical cores executing the same code with some time staggering.

THE CHALLENGE: open-source RISC-V SoC relevant for safety-critical applications.

THE SOLUTION: DCLS version of the Sargantana core.

SafeGantana: a DCLS Version of Sargantana



♦ The **Sphere of Replication** (SoR) is the region where comparison and coalescence occurs (the components replicated)

Small sphere of redundancy		**Big** sphere of redundancy
• **Lower** replication costs	**TRADE-OFF**	• **Higher** replication costs
• **Extra latency** for all cache accesses		• **No penalty** latency for cache hits
• **Shorter** Fault Detection Time Interval (FDTI)		• **Bigger** Fault Detection Time Interval (FDTI)

⇨ SoR selected between L1 caches and the L2 cache

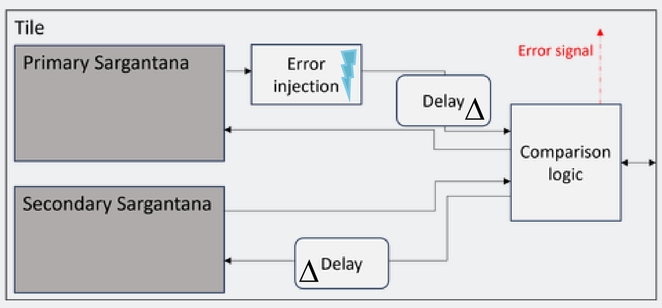
♦ **Programmable delay** logic for staggering purposes, typically 2 or 3 cycles.

♦ **Delayed** inputs to the primary and **delayed** outputs from the secondary.

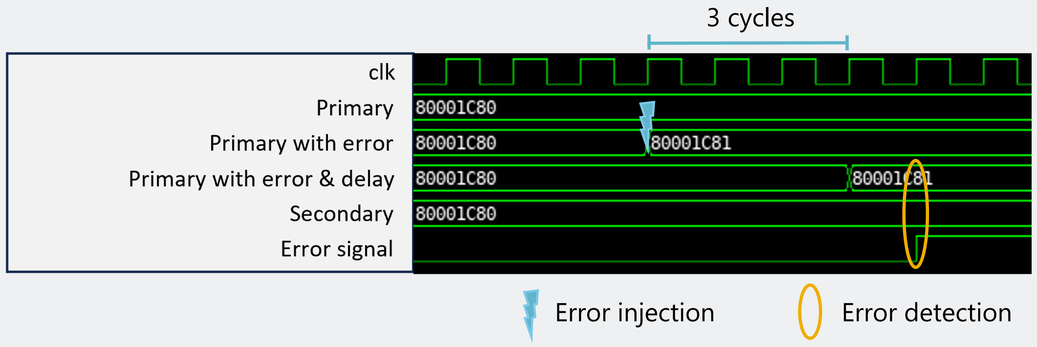
♦ **Error management:** mismatch between the outputs of the primary and secondary cores detected by the comparator. The core operation is stalled not allowing any further output to be propagated beyond the SoR.

Evaluation

- We have evaluated the behavior of the **SafeGantana with 3 cycles staggering**
- Validated the comparison logic with an error injector



- The error injector introduces an error at a specific time.
- We inject the error in an output signal targeting the I-Cache from the **primary** core.
- After delaying the signal, the comparison logic detects the error against the error-free output from the **secondary** core.



- **Hardware costs**

	Number of LUTs	% of LUTs respect to single core	Number of registers	% of registers respect to single core
Single Core	146.400	100%	76.189	100%
Double Core	292.800	200%	152.378	200%
SafGantana	295.756	202,02%	157.455	206,7%

Future plans

- An extra functionality that has been implemented already: Fine-state machine for commanding the initial and finish phases in AXI transactions.
- Boot LINUX on SafeGantana (already booting on Sargantana)
- Integration in BSC Safety Soc (in-house safety platform)
  - ⇨ Report error as a platform interruption
  - ⇨ Evaluate action upon the lockstep interruption
- Integration in OpenPiton platform and extend L2 and L3 with Error Correction Codes (ECC)

Acknowledgments

This work has been partially supported by the Spanish Ministry of Science and Innovation under grant PID2019-107255GB-C21/ AEI/10.13039/501100011033. Authors thank the support given to the Research Group SSAS (Code: 2021 SGR 00637) by the Research and University Department of the Generalitat de Catalunya.