SafeLS: an Open Source Implementation of a Lockstep NOEL-V RISC-V Core

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

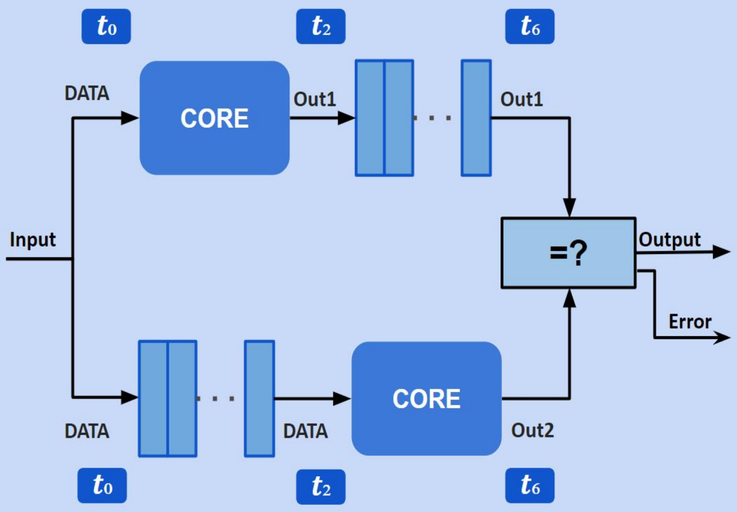
Marcel Sarraseca
marcel.sarraseca@bsc.es

Sergi Alcaide, Francisco Fuentes, Juan Carlos Rodriguez, Feng Chang,
Ilham Lasfar, Ramon Canal, Francisco J. Cazorla, Jaume Abella

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Link to the Implementation

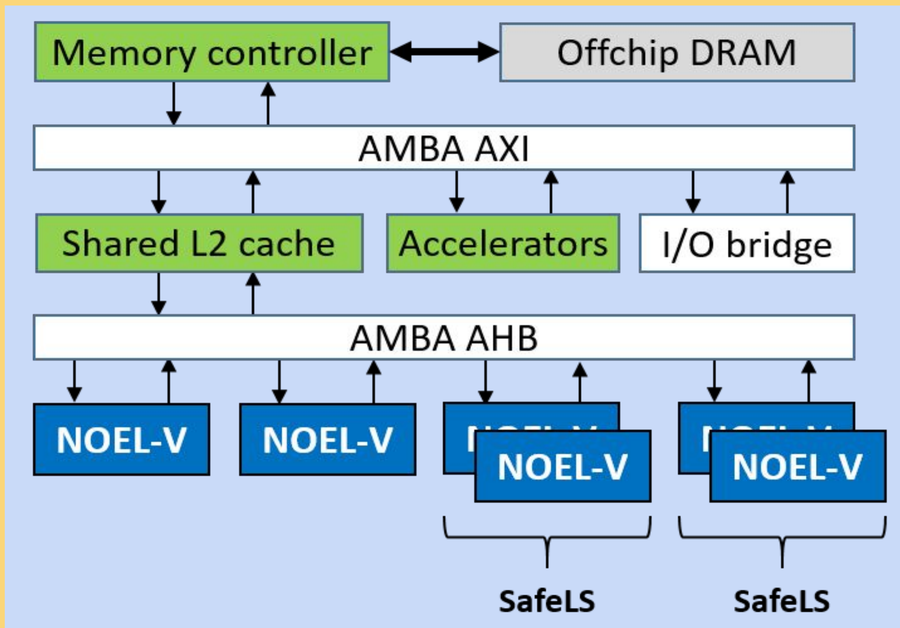
1. Introduction

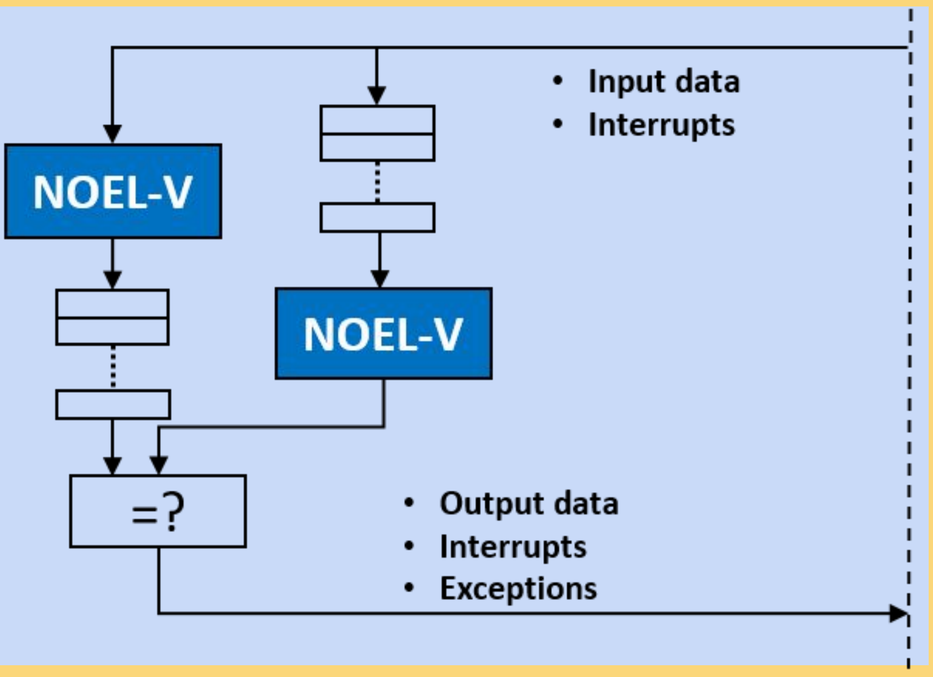


- Safety-critical automotive, avionics, and space systems require safety measures to prevent failures due to random hardware errors like radiation and electromagnetic interference.
- Common cause failures (CCFs) occur when a fault produces **identical errors** in redundant elements, making **error detection with only** redundancy **impossible**.
- **Lockstep cores**, where two cores execute the same instructions with a time offset, are commonly used to **avoid CCFs** in cores. Thanks to the **time-diversity,** faults will affect differently the two executions and **enable** the **fault-detection** at the output comparison.
- Commercial lockstep core solutions exist from chip vendors like Infineon and STMicroelectronics, but open-source implementations for safety-relevant SoCs are unavailable.
- **THE CHALLENGE**: Cover the gap by developing an open-source lockstep version of the RISC-V-based NOEL-V core by Frontgrade Gaisler.
- **THE GOAL:** The developed lockstep core is integrated into the open-source SELENE SoC, providing an open-source solution for safety-critical systems.

2. SafeLS: a Lockstep NOEL-V Core

- The sphere of replication refers to the level at which redundancy is implemented in a system.
- Pipeline stage level, as seen in recent implementations for RISC-V cores.
  - \+ Immediate error detection.
  - \- Intrusive and requires additional verification and validation.
- In **safety-critical systems** for automotive, space, avionics, and robotics, errors can often be managed at a coarser grain than pipeline stages.
- **Immediate detection** is **not necessary** as long as errors are detected when a safety-critical task completes its execution, preserving safety requirements.
- The chosen approach is to set the **sphere of replication** at the **core level**.





- **All input signals** for the NOEL-V core **are replicated** for both cores.
- One core receives the inputs **immediately.** The other core receives them with a **programmable delay** of 2 or 3 cycles.
- Outputs from one core are **delayed** by the same number of cycles.
- The **Outcomes** of both cores are **compared** before sending.
- If **no discrepancy** is detected, **outcomes** are **delivered** back to the rest of the system-on-chip.
- **Discrepancy** means that at least one of the outcomes is erroneous. If dual modular redundancy (DMR) is employed, it is unknown which outcome is correct.
- An appropriate **interrupt** is **raised** at the system level to manage the error (e.g., resetting the SafeLS and re-executing the task).

3. Future Plans

- Release an **open-source component** for SELENE SoC as a standalone module and part of the system (check the **QR**).
- Aim to enhance SELENE SoC with additional features for safety-critical systems in various domains (e.g., automotive, space, railway, robotics).
- First-level caches of the NOEL-V core are protected against single bit-flips.
- The read-only instruction cache is parity protected, and single bit-flips can be corrected by invalidating erroneous cache lines and fetching them from upper memory levels.
- Analyze a **smaller sphere of replication** that will exclude first-level caches in the cores to prevent cache duplication.
  - This approach may be more intrusive but offers advantages in terms of power and area.

4. Summary

- Safety-critical systems impose the use of lockstep cores to avoid **CCFs**.
- Our work delivered **SafeLS**, the first **open-source RISC-V-based lockstep** core based on the commercial Gaisler's NOEL-V and integrated into a fully-functional SoC (the SELENE SoC).
- The lockstep is validated, and the implementation will be released open-source by the time of the summit.

5. Acknowledgements

This work is part of the project PCI2020-112010, funded by MCIN/AEI/10.13039/501100011033 and the European Union "NextGenerationEU"/PRTR, and the European Union's Horizon 2020 Programme under project ECSEL Joint Undertaking (JU) under grant agreement No 877056. This work has also been partially supported by the Spanish Ministry of Science and Innovation under grant PID2019-107255GB-C21 funded by MCIN/AEI/10.13039/501100011033.