Enhancing Safety with RISC-V based SPIDER Autonomous Robot

A Use-Case from ECSEL FRACTAL Project

Joaquim Maria Castella Triginer

Markus Postl, Mikel Fernandez, Feng Chang, Sergi Alcaide, Ramon Canal, Jaume Abella

1Virtual Vehicle Research GmbH
2Barcelona Supercomputing Center
3Universitat Politècnica de Catalunya
1. FRACTAL Project
2. SPIDER Autonomous Robot Use-Case
3. Safety and Security in Automotive
4. Safety Services
The OBJECTIVE of FRACTAL project is to create a COMPUTING NODE as the building block of scalable Internet of Things.

The two main general characteristics of our node would be: COGNITIVE + FRACTALITY
1. To design and implement an open-safe-reliable hardware platform. It will be used for building the cognitive edge nodes of variable complexity.

2. To guarantee extra-functional properties of FRACTAL nodes (dependability, security, timeliness and energy-efficiency).

3. To evaluate and validate data analytics with AI. To identify the largest set of working conditions, while preserving safe and secure operations.

4. To integrate fractal communication and remote management features into the nodes.
SPIDER AUTONOMOUS ROBOT USE-CASE
Objective 1
Co-execution of safety-relevant, security-relevant, as well as AI based tasks

Objective 2
Guarantee extra functionality of fail-operational capabilities

www.v2c2.at/spider
Path Tracking Node
- Redundant, and accelerated AI model execution

Collision Avoidance Node
- Redundant Execution
- Monitoring of RISC-V cores

Use-Case Architecture

Perception
- Point Cloud Fusion
- Point Cloud Filtering
- Cost Map Generation

Collision Avoidance
- Safe Stop
SAFETY AND SECURITY IN AUTOMOTIVE
Safety and Security in Automotive

- **Safety in automotive** is driven by ISO 26262 (2018)
- In automotive, the *safety-critical system requires* the highest Automotive Safety Integrity Level (ASIL) risk classification -> ASIL-D
- **Automated driving** functionalities require systems that can meet ASIL-D requirements
- These systems need to accomplish Automotive fail-operational capabilities
  - Controlling failures, such as common-cause failures
  - Maintaining system operation under any circumstances
Safety and Security in Automotive

- Common-cause failures: **failure of two or more elements of an item** resulting directly from a single specific event or root cause

- Mitigation strategies (Safety measures):
  - **Redundancy** helps in improving the reliability and availability of a system.
  - **Diversity** aims to achieve independence

- Fault Tolerant Time Interval
  - **Safety Mechanism**
  - **Emergency Operation**

(*)Figures from ISO 26262 (2018)
SAFETY SERVICES
Prevention of common cause failures.

- All cores can be used by less critical apps
- SafeSoftDR creates independent copies of input and output data
- Function is executed in a diverse (time-staggered) redundant execution
- Results are compared
- Upon a mismatch, an appropriate safety measure should be triggered

Released open-source: [https://gitlab.bsc.es/caos_hw/software-diverse-redundancy-library](https://gitlab.bsc.es/caos_hw/software-diverse-redundancy-library)
Multicore timing interference monitoring

- Non-intrusive interference monitoring
  - Per core interference quota allocation
  - Measure total execution time
  - Measure interference of each core or accelerator
  - Per core Interrupt signalling

Released open-source: https://gitlab.bsc.es/caos_hw/hdl_ip/bsc_pmu
THANK YOU

Joaquim Castella Triginer
Joaquim.CastellaTriginer@v2c2.at

Markus Postl, Mikel Fernandez, Feng Chang, Sergi Alcaide, Ramon Canal, Jaume Abella

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 877056. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Spain, Italy, Austria, Germany, France, Finland, Switzerland.