



Introduction to
RISC-V Functional Safety
special interest group

Spring 2022 RISC-V Week, Paris
Jérôme Quévremont, Thales Research & Technology

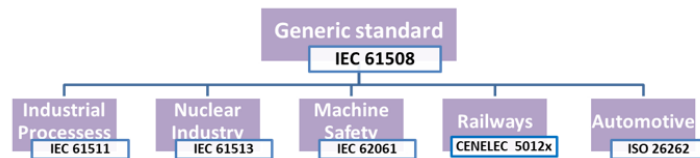
“Functional Safety” in a nutshell (1/2)

- **Definition:** Absence of unreasonable risk due to hazards caused by malfunctioning behavior
- **Goal:** Actively protect people from injuries and health damages (directly or through the environment) thanks to the correct behavior of safety features
- **Domains:** automotive, aerospace, medical, energy, railways, defense, industry...

“Functional Safety” in a nutshell (2/2)

- Often relates to domain-specific **certification** standards:

- “Generic”: IEC-61508
- Automotive: ISO-26262
- Aerospace: DO-178C, DO-254...



- Not to mistake with *information security*
 - Common properties, such as availability, system integrity...
 - Very diverse intent:
 - Functional Safety: protect humans from systems (failures)
 - Security: protect systems from humans (hackers)

Main Properties for Safety-Critical Systems

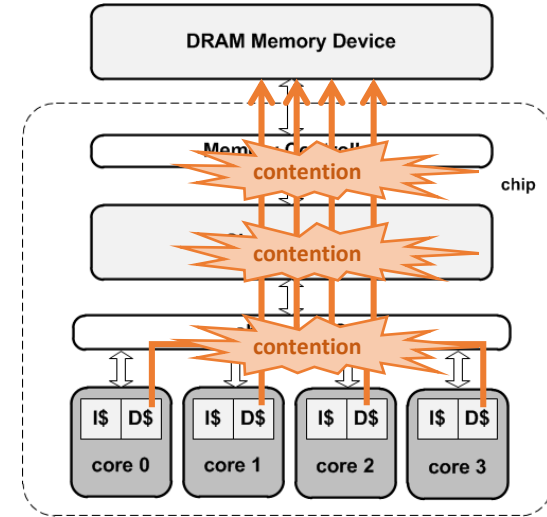
- **Availability**: readiness of the system when needed
- **Predictability**: ability to predict how a system will behave with given inputs
- **Reliability**: ability to resist to harsh environmental conditions
- **Integrity**: ability to retain data uncorrupted
- **Explainability**: capability to explain why a system is behaving as it is (required to reach predictability)
- **Observability**: ability to observe the detailed system state
- **Simplicity** (limited complexity): ability of a system to be understood end-to-end in a concise manner
- ...

What is Functional Safety SIG

- A forum to discuss functional safety in a RISC-V context
- Primary goals
 - Identify gaps and technical needs for functional safety
 - Advocate recommendations and/or solutions for various application domains
 - Identify specific problems to be addressed by current or spun off task groups
- Not a specification TG:
 - We do not develop RISC-V extensions
- Participants
 - OEM, silicon manufacturers, software and CAD vendors, IP providers, research labs, etc.
- Leadership
 - Chair: Jérôme Quévremont, Thales
 - Vice-Chair: Amit Pabalkar, Nvidia → Jaume Abella, BSC

Example #1 - Time interference in Multi-Core

- Minimize contention points between independent initiators (cores, DMA masters, etc.)
 - Minimizing shared single paths to endpoint resources
 - Distributing the memory architecture
 - Minimizing implicit data sharing, cache coherency traffic
- Hardware control features
 - Bound the worst case execution time at the cost of average execution time, e.g. cache partitioning, locking, or even cache deactivation
- Spatial and temporal isolation in multi-core SoC
 - Timers, scheduling, OS...
 - Interconnect, memory protection...
- Reduce the impact of interrupts that introduce non-determinism

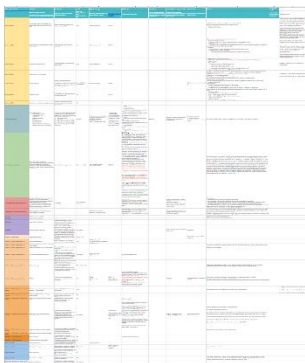


Example #2 - Hardware Safety Mechanisms

- Safe Interconnects
 - Guarantee execution of safety-critical transactions between CPUs and connected devices
 - Dynamic/configurable interconnects
- Built-in self tests
- ECC/Parity protection
- Lock-step
- Clocks and Voltage monitors
- Hardware watchdog
- Hardware monitors to measure jitter and take corrective actions

Activity

- Past work:
 - Wiki pages to capture expectations from different perspectives
 - “Blueprint of a safety processor”
 - Spreadsheet broken down in several “attributes”



- White paper preparation
 - Elaborate on the blueprint
 - Chapters:
 - Partitioning (spatial/temporal)
 - Performance counters
 - Error detection and reporting
 - QoS and priority management
 - Redundancy
 - Caches and TCM
 - Support and tooling
 - Contents:
 - Needs and desired features
 - RISC-V solutions to deploy these features
 - Gaps and recommendations

Engagement

- Joining:
 - <https://lists.riscv.org/> then
 - <https://lists.riscv.org/g/sig-safety>
- Meetings: Wednesdays, alternating:
 - 12pm EST, 18:00 CET
 - 8 am EST, 14:00 CET
 - <https://calendar.google.com/calendar/u/0/embed?src=tech.meetings@riscv.org>
- Regular participants (2+ meetings / 6 months)



Thank you!

