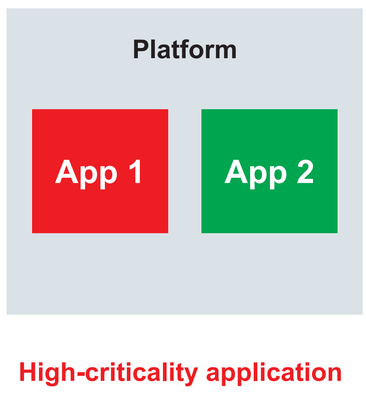
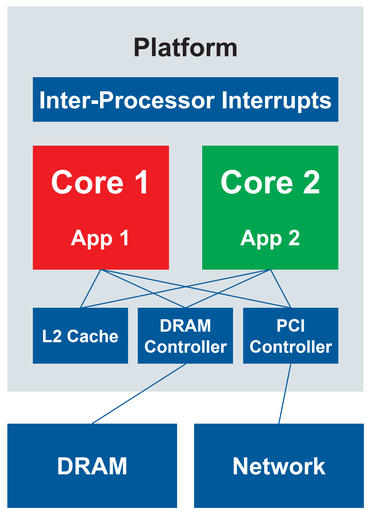
Explorative Surveying RISC-V Open Hardware and Specifications for Mixed-Critial Systems

Samuel Ardaya-Lieb[1], Holger Blasum[2], Enkhtuvshin Janchivnyambuu[2], Florian Krebs[2], Jan Reinhard[2], Darshak Sheladiya[2], and George Violettas[2]
[1]Consolinno Energy GmbH, [2]SYSGO GmbH
Presenting authors (present at this RISC-V summit): jan.reinhard@sysgo.com, darshak.sheladiya@sysgo.com

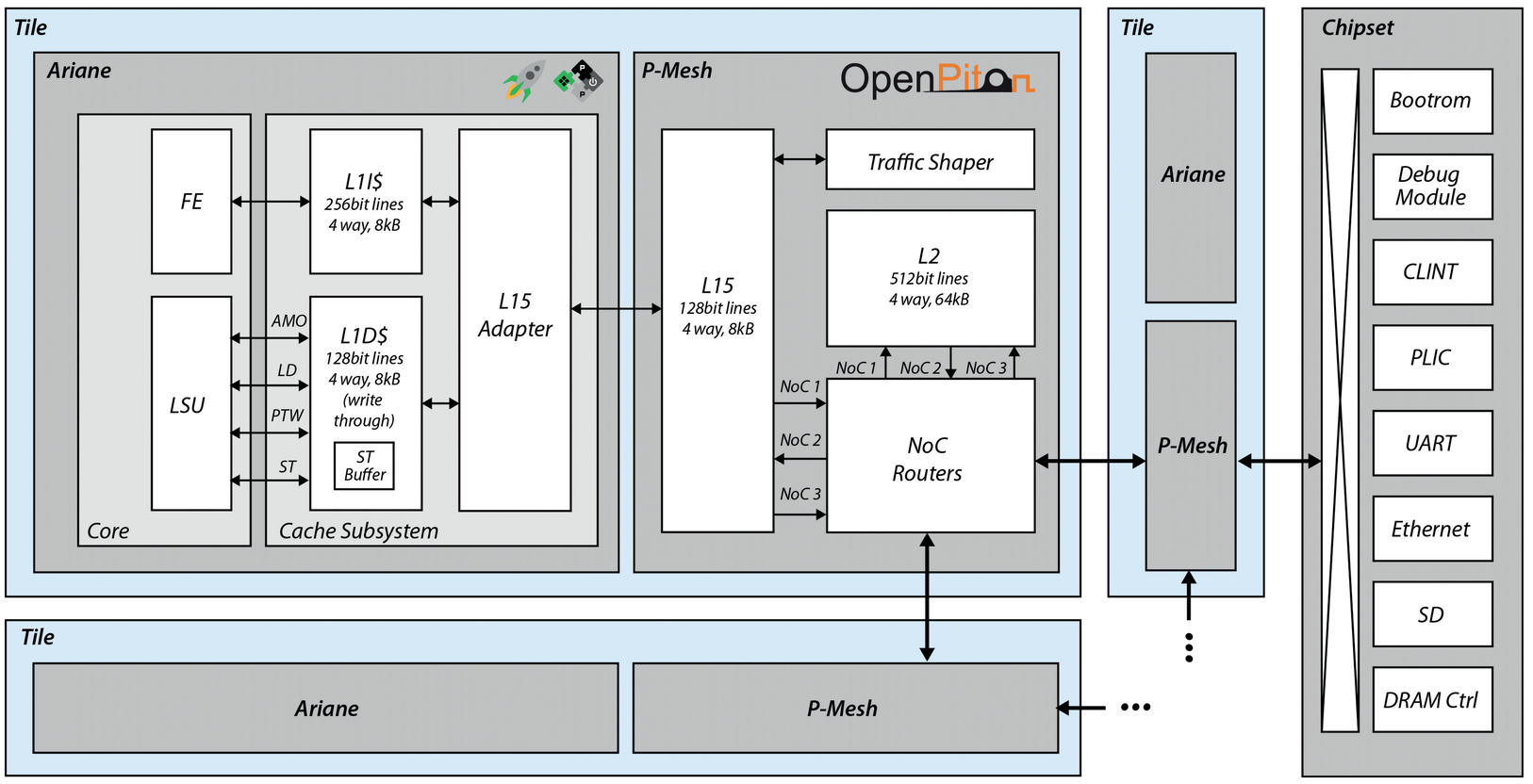
Mixed-critical systems are essential in modern computing, where applications of different criticality levels share the same hardware platform(s) and/or resources. This paper explores the robustness and implementation of mechanisms for such mixed-critical systems utilizing RISC-V specifications and available open hardware. In particular, the CVA6 processor and OpenPiton System on Chip (SoC) are used. We also research the mixed-criticality suitability of core-to-core communication, resource management, and specific components like performance counters, memory, and caches. Furthermore, we discuss future developments of mixed-critical systems utilizing open hardware.



- **Mixed-criticality systems:** Run applications with different criticality levels (often safety-focused) on the same HW platform.
- **Hardware separation:** Physically separate HW for critical applications (during design/planning).
- **Benefits of mixed-criticality systems:**
  - More flexible than physical separation.
  - Many applications in modern computerized systems.
- **Simplest case:** One critical and one less critical application on the same platform.



- **Traditional time-sharing systems:** Processes run concurrently on the same processor.
- **Modern approach (multi-core processors):** Cores are assigned to different applications.
- **Mixed critical systems:** Cores share resources (L2 caches, DRAM, PCI controller).
- **Configuration** ensures high-criticality applications aren‘t blocked by lower-criticality ones.



www.github.com/PrincetonUniversity/openpiton

- **RISC-V for mixed-critical systems:** Malleability of ecosystem easies development of dedicated mixed-criticality support. Also open HW components allow independent verification of safety / security properties.
- **Resource management:**
  - Performance counters help allocate resources.
  - Memory management offers isolation (MMU) but shared memory (DRAM) can cause issues. Cache partitioning (not yet standardized) can improve isolation.
- **Communication and synchronization:**
  - Mechanisms for strict isolation between domains (like multiple OSes) are under development.
  - Deterministic communication (essential for safety) remains a challenge.

- **Security:** Speculative execution poses security risks. „fence.t“ instruction (concept) could mitigate these risks.
- **OpenPiton SoC example:** HW / SW monitoring for systems with shared resources (common technique: partition some resources with hardware and manage others with OS-based on performance counters).
- **Future directions:** Specifying a more mixed-criticality-oriented SoC for future hardware development. Exploring reliability assessment techniques.

Acknowledgment
This work was supported by the European Union projects TRISTAN (RIA Chips-JU, GA 101095947), and ISOLDE (RIA Chips-JU, GA 101112274). Insights were drawn from Jérôme Quévremont and Rudolf Fuchsen, and from discussions at the RISC-V functional safety special interest group.

Paper Download
www.sysgo.com/wp-riscvoh

TRISTAN Project has received funding from the Chips Joint Undertaking (Chips-JU) under the grant agreement nr. 101095947. ISOLDE Project has received funding from the Chips Joint Undertaking (Chips-JU) under the grant agreement nr. 101112274. Chips-JU receives support from the European Union’s Horizon Europe’s research and innovation programme and Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Germany, Denmark, Estonia, Greece, Spain, Finland, France, Hungary, Ireland, Israel, Iceland, Italy, Lithuania, Luxembourg, Latvia, Malta, Netherlands, Norway, Poland, Portugal, Romania, Sweden, Slovenia, Slovakia and Turkey.