Safe, Secure and Reliable Computing with NOEL-V Processor: from De-RISC H2020 project onward

Jimmy Le Rhun, Sylvain Girbal – Thales Research & Technology
Johan Klockars, Nils-Johan Wessman, Fabio Malatesta, Jan Andersson – Frontgrade Gaisler

RISC-V Summit Europe, Barcelona - 5-7/06/2023

This project has received funding from the European Union's Horizon 2020
Research and Innovation Programme under Grant Agreement EIC-FTI 869945

THALES

Thales Research & Technology

THALES

- Corporate research center
  - Applied research, technology transfer to Business Units
  - HPC and Critical Systems labs involved in RISC-V
- Contributions to RISC-V ecosystem
  - Chair of Functional Safety SIG at RISC-V International
  - OpenHW Group:
    - Co-Chair technical WG
    - Leader of the CVA6 project
  - Involved in IOMMU specification
- In addition, specific research activities for critical systems
  - Improvement of safety and security properties
  - Collaboration with Thales Alenia Space for specification and evaluation of Space-grade System-on-Chip

Thales keynote
by Thierry Collette
Thursday morning

GROUP OPENHW
PROVEN PROCESSOR IP

ThalesAlenia Space
a Thales / Leonardo company

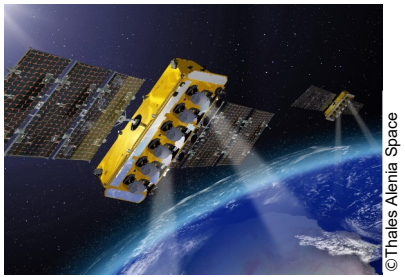

Context and Challenges

Context of safety-critical & space systems

- Strict requirements for dependability
  - Robustness in harsh environments
  - Fault tolerance, fail-operational
  - Deterministic real-time behaviour, esp. in a multi-core system
    - Timing interference due to concurrent access to shared hardware resources
- Increasing need for performance
  - Algorithms get more complex, with larger datasets
  - Adaptive or multi-mode applications, multiple applications
  - Not only average-case performance, but also guaranteed worst-case
- New requirements
  - Increased connectivity
  - Cybersecurity
  - Free from export control restrictions


©Nadezda Murmakova


©RTA


©Thales Alenia Space

Openness advantage

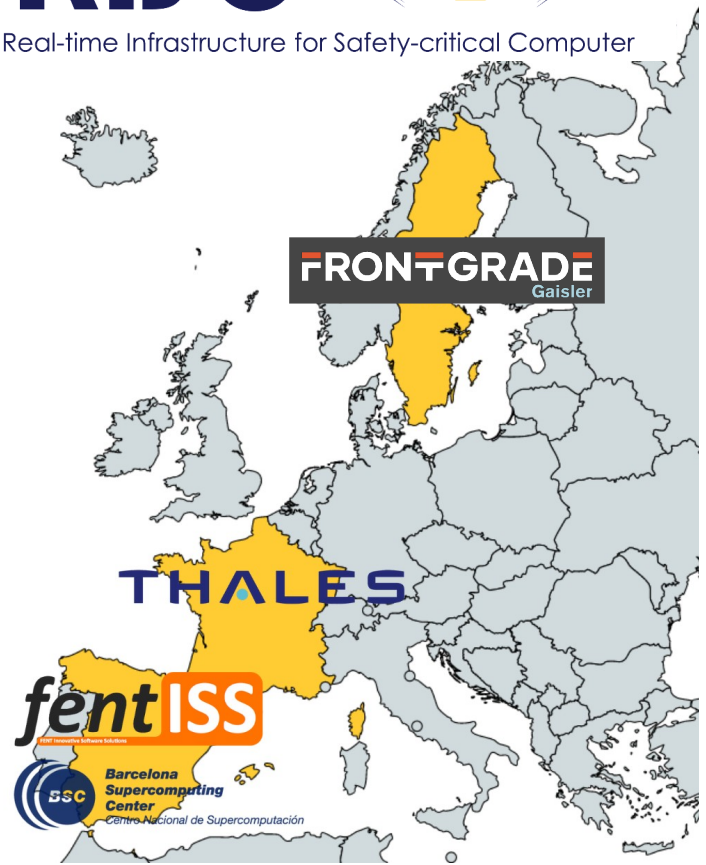
- Safety-critical systems are a collection of small markets
  - Previously not cost-effective to design dedicated hardware
    - Except for radiation-tolerance constraints in space
    - But New Space constellations need cheaper solutions
  - It's also increasingly costly to use multicore COTS
- Open-source advantages
  - Openness: observability, ability to document, cybersecurity audit
  - Respect of standards, interoperability
  - Better test coverage by a broader userbase
- Open-source Hardware
  - LEON Sparc is a European success story in Space
  - Great momentum with RISC-V ecosystem
  - Opportunity to introduce safety constraints in the community


De-RISC approach

De-RISC project overview

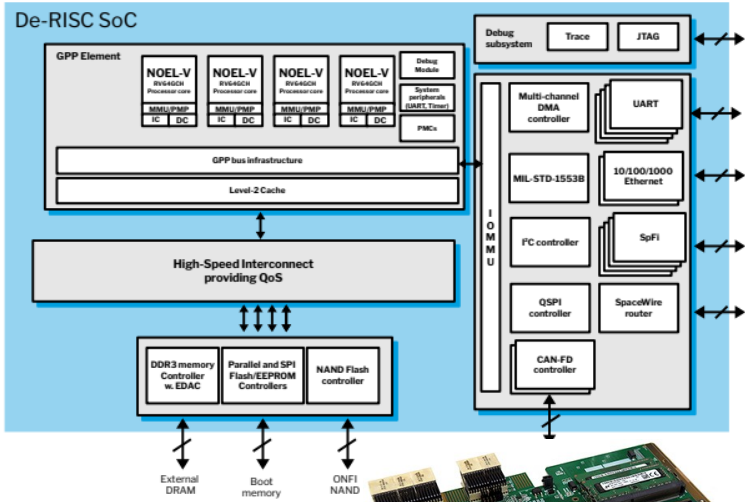
De-RISC
Dependable Real-time Infrastructure for Safety-critical Computer

- Dependable realtime infrastructure for Safety-critical Computers
  - H2020 Fast Track to Innovation project
  - 4 partners: fentISS, Barcelona Supercomputing Center, Frontgrade Gaisler, Thales Research & Technology
  - Started in October 2019 for 36 months
- Goal: to develop a full computing platform for space
  - Fault-tolerant multicore NOEL-V architecture on FPGA
  - XtratuM NG space-qualified hypervisor
  - Advanced monitoring and interference mitigation
  - Validation with space applications
- Made in Europe
- ESA-supported program for SoC ASIC implementation



NOEL-V core and De-RISC Platform architecture

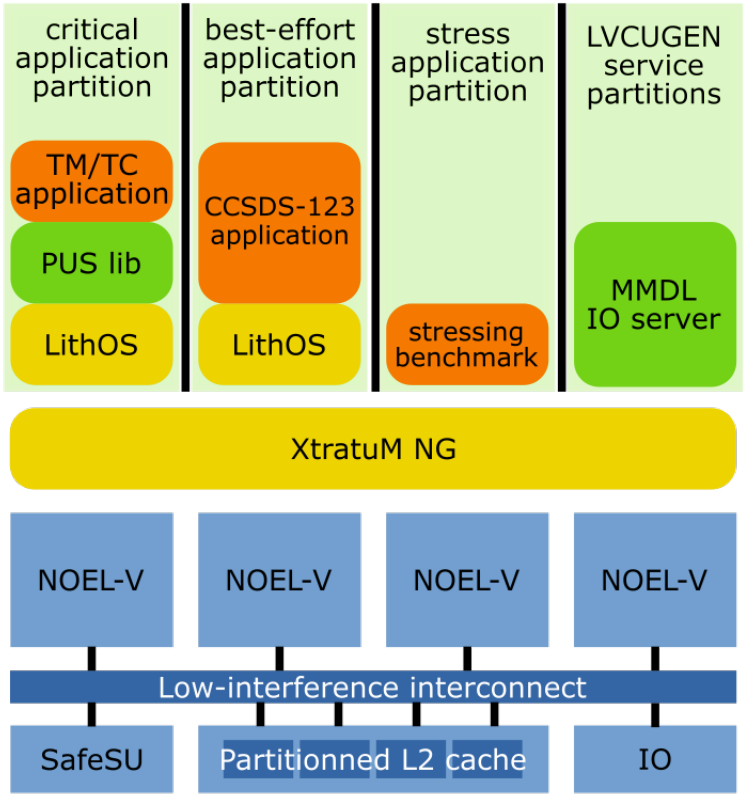
- NOEL-V processor core
  - Conform to the OS A (Embedded) RISC-V Platform Specification
  - RV64GCH – 64-bit processor
    - In-order, dual-issue, 7-stage pipeline
    - NanoFPU or pipeline FPU (Zfhmin, FD)
    - MMU - 39 bit virtual addressing, separate I and D, fully associative, TLB
  - Cache control extensions
  - RISC-V Advanced Interrupt Architecture (AIA)
  - GPL and commercial licences
- De-RISC computing platform
  - Quad-core SoC
  - Dedicated IO for space systems (SpaceWire, SpaceFibre, etc.)
  - Space-grade hypervisor: XtratuM NG (FentISS)
  - Advanced monitoring with SafeSU (BSC)
- Implemented on FPGA
  - Demo Bitstreams available for Xilinx and Microchip eval boards
  - DeRISC embedded board



©Frontgrade

Isolation and partitioning

- Hypervisor support
  - Implementation of H extension
  - Support by XtratuM NG hypervisor
    - Guest OS: LithOS, RTEMS, Linux
  - Validation with CNES's LVCUGEN space payload framework
- Physical Memory Protection (PMP)
- IOMMU
- Low-interference interconnect
  - Address-striped Multi-bus
  - Partitionned L2 cache
  - Multi-channel DDR controller

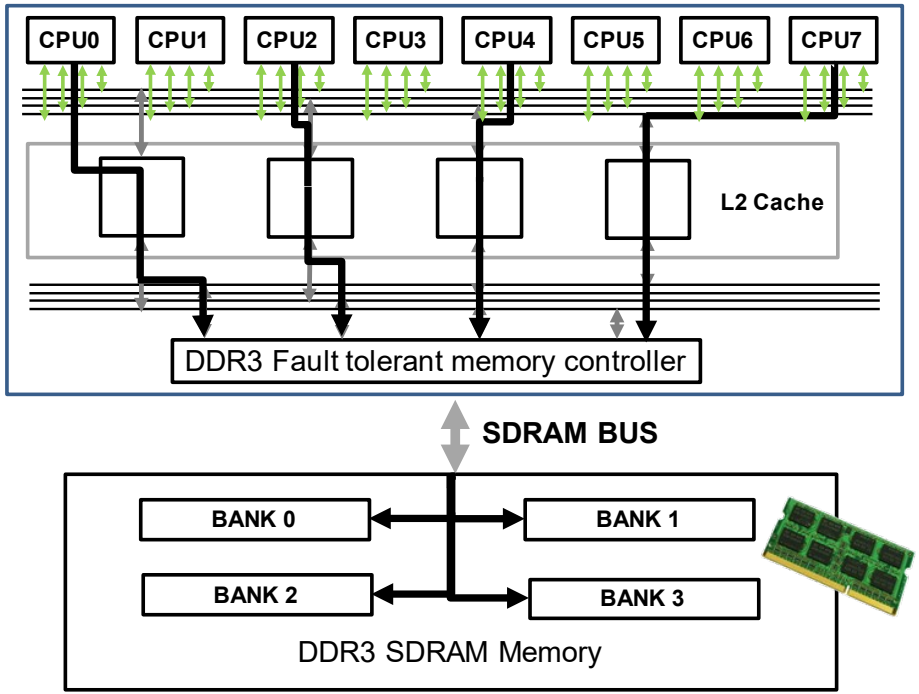


Isolation : address-striped multi-bus interconnect

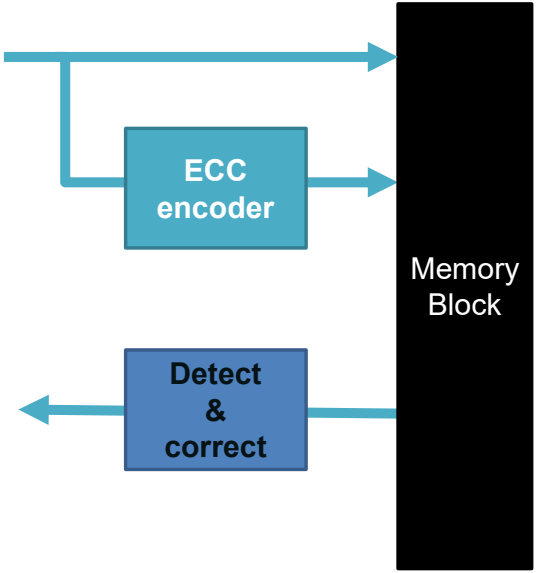
- 4x AHB 2.0 buses
  - **All cores connected to all stripes**
  - Support for larger physical address space, up to 48-bits
  - **Encoding to stripe based on (configurable) bits in physical address**
    - Default setting: map stripes to cache lines
    - Encoding to stripe address space in L1 cache backend
    - Achieve isolation by changing a stripe selection bit to a higher logical address bit
  - Consistent addressing from L1 backend to DDR controller
- Fully isolated L2 cache pipelines dedicated to each stripe
- The striped interconnect allows for concurrent accesses to different memory banks
  - Minimizing interference
  - Improving performance
  - Maintaining L1 cache coherency

An L2 cache hit causes no interference

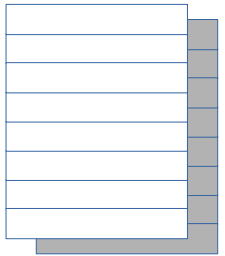
- Also time-slotted mode (under development):
  - Accesses to each memory bank are only allowed 1/4 of the time
  - Zero interference between the stripes
  - Performance cost



Reliability and Integrity for space



- Protection of memory blocks (in caches & register file) using error correcting codes
  - Protected with a full SECDED code with custom scheme:
    - Deliver correct data locally without causing memory access
    - Guaranteed detection also of 3-bit and 4-bit adjacent bit errors
  - Hardware scrubber built into processor to avoid error build-up
    - Removes need for manual scrubbing routines
  - Error counters and diagnostic interfaces to monitor and inject errors
- Radiations tests performed during the project
  - cf. RADECS'22 paper
- Control flow integrity (standardization ongoing)
  - Shadow stack - stack overwrites must not cause return to the wrong place
  - Landing pad - memory overwrites must not cause jumps/calls to the wrong place



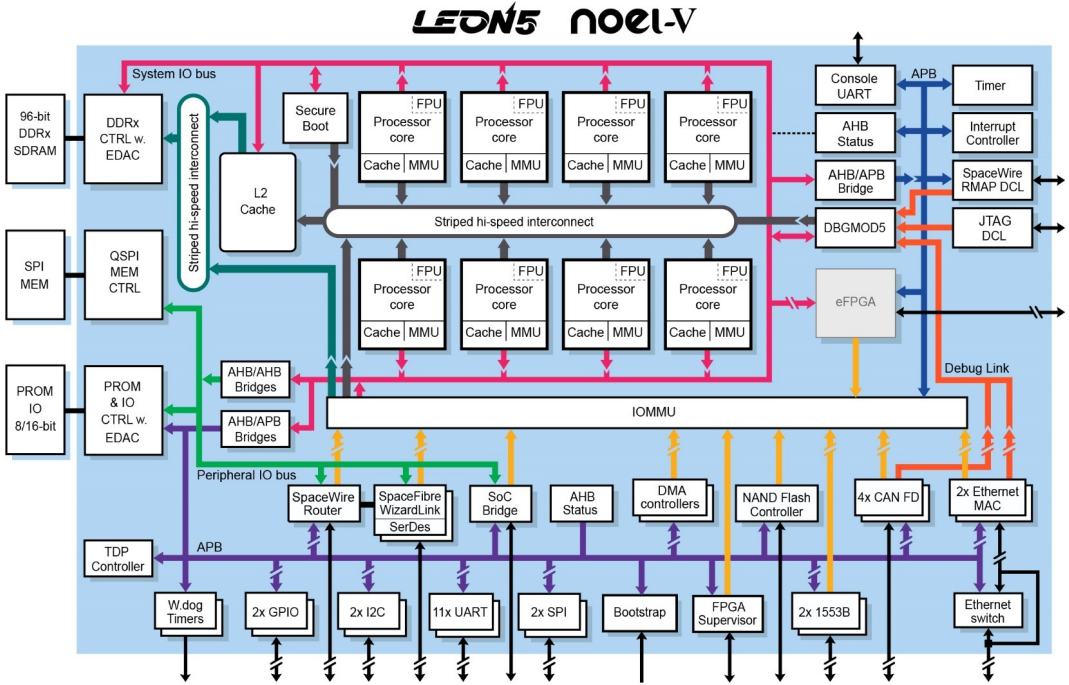

GR765

ESA project – GR765 octa-core processor

Baseline Features

- Fault-tolerant **octa-core** architecture
  - **LEON5FT SPARC V8** or **NOEL-V RV64GCH**
  - Dedicated FPU and MMU, 64 KiB per core L1 cache, connected via multi-port interconnect
- **1 GHz processor frequency - 26k DMIPS**
- 2+ MiB L2 cache, **512-bit** cache line, 4-ways
- **DMA controllers**
- **DDR2/3 interface with dual x8 device correction capability**
- 8/16-bit PROM/IO interface
- **(Q)SPI and NAND memory controller interfaces**
- **Secure Element**, providing Secure (authenticated) boot (TBD)
- **eFPGA** ~30k LUT (TBD)
- **High-pin count – LGA1752 package** allows reduction of pin sharing
- Target technology: **STM 28nm FDSOI**

In development
No guarantee of product launch



Conclusion

- RISC-V is a great opportunity for critical systems
  - To regain control on fine-grain hardware features
  - To implement solutions for safety and reliability
  - To jointly tailor HW and SW
  - To team-up across application domains
- De-RISC solution
  - Open, safety- and determinism-oriented multicore SoC
  - Complete and certifiable software stack
  - Validation using a space-grade software stack
  - ASIC coming soon

© Lunar Gateway ©Thales Alenia Space/Briot

De-RISC
Dependable Real-time Infrastructure for Safety-critical Computer

www.derisc-project.eu

@DeRISC_H2020_EU

De-RISC

info@derisc-project.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement EIC-FTI 869945