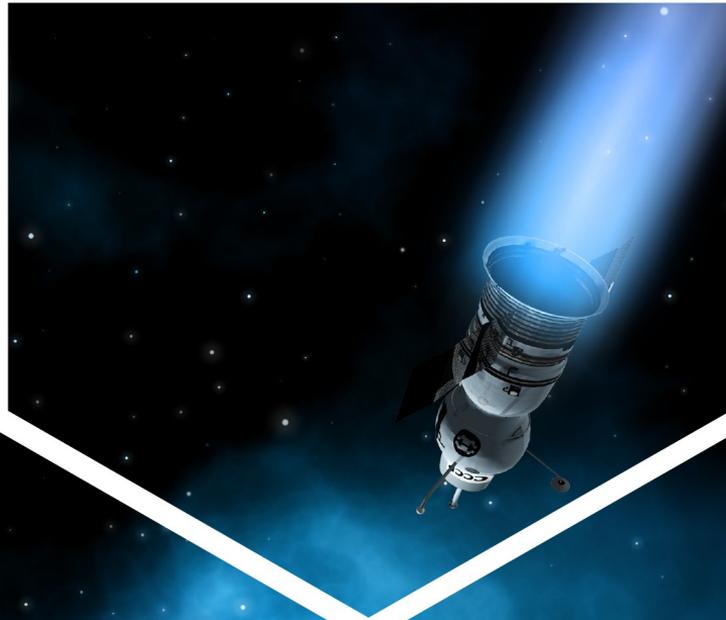# De-RISC

Dependable Real-time Infrastructure for Safety-critical Computer

www.derisc-project.eu

De-RISC: Launching RISC-V into space
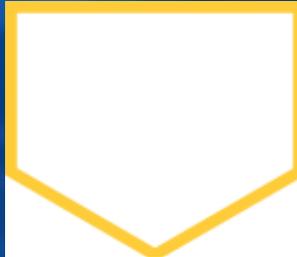
Jimmy Le Rhun – Thales Research & Technology

OBDP'21 - 17/06/2021

**THALES**

Context and Challenges

Context of safety-critical systems

- Strict requirements for dependability
  - Robustness in harsh environments
  - Fault tolerance, fail-operational
  - Deterministic real-time behaviour

- Increasing need for performance
  - Algorithms get more complex, with larger datasets
  - Adaptive or multi-mode applications, multiple applications
  - Autonomous systems

- New requirements
  - Increased connectivity
  - Cybersecurity
 - Free from export control restrictions

www.derisc-project.eu

Context of COTS multicore processors

- To address performance needs, increase the number of processor cores

- Other resources are not duplicated accordingly
  - Memory hierarchy, peripherals, datapaths

- Timing interference
  - Delay due to concurrent access to shared resource
  - Need for interference channels identification and mitigation
    - Required by safety standards (e.g. CAST32A)
  - Often non-documented hardware arbitration policies

- Mitigation of contentions
  - Allocate resource to a single initiator
  - Global scheduling of transactions on shared resources, not just tasks on cores

www.derisc-project.eu
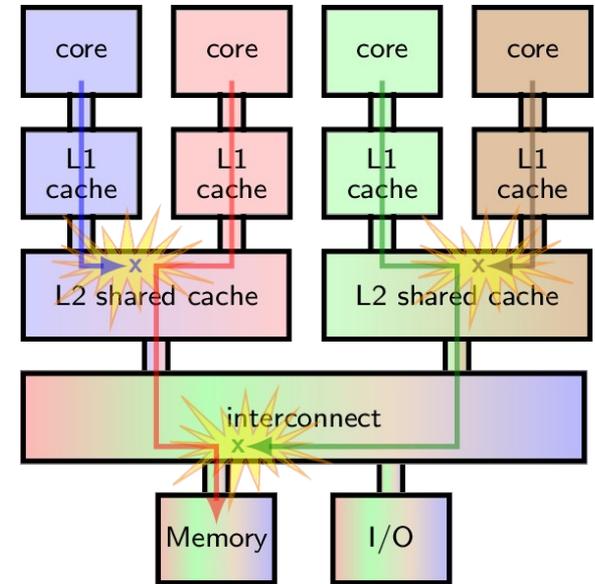
Open-source Opportunities

- Safety-critical systems is a small market
  - Previously not cost-effective to design dedicated hardware
    - Except for radiation-tolerance constraints in space
  - But 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 user base

- Open-source Hardware
  - LEON Sparc is a European success story in Space
  - Recent rise in popularity with RISC-V
  - Opportunity for community-driven designs with safety constraints in mind

www.derisc-project.eu
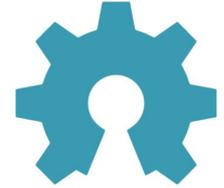
RISC-V open-source standard

- RISC-V instruction set
  - Maintained by RISC-V International
  - Permissive open-source licence
  - Efficient and modular ISA, with optional extensions
  - Some peripherals : interrupt controller, MMU, etc.

- Technical Groups and Special Interest Groups
  - Security Standing Commitee
  - Cache Management Operation Task Group
  - Functional safety SIG

- Industrial associations
  - OpenHW Group
  - CHIPS Alliance

www.derisc-project.eu
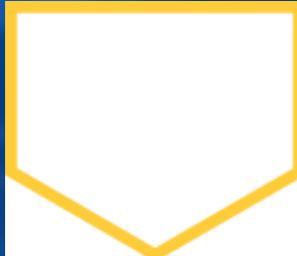
De-RISC approach

De-RISC project overview

- Dependable realtime infrastructure for Safety-critical Computers
  - H2020 Fast Track to Innovation project
  - 4 partners: Fentiss, Cobham Gaisler, Barcelona Supercomputing Center, Thales R&T
  - Started in October 2019 for 30 months

- Goal: to develop a full computing platform for space
  - Multicore NOEL-V architecture on FPGA
  - XtratuM hypervisor
  - Advanced monitoring and interference mitigation
  - Validation with space applications

- Made in Europe

www.derisc-project.eu

De-RISC approach

- Leveraging the RISC-V architecture for critical systems
  - High-performance NOEL-V core
  - Designed with fault-tolerance capabilities

- Building a full platform
  - A complete SoC with a wide selection of peripherals
  - A full software stack with certifiable hypervisor and RTOS
  - Advanced monitoring capabilities with SafeSU
    - Request duration, Cycle contention, Max. contention control

- Minimized interference channels
  - Private scratchpad memories
  - Multiple L2 busses and partitioned L2 cache
  - Multichannel DDR controller

www.derisc-project.eu
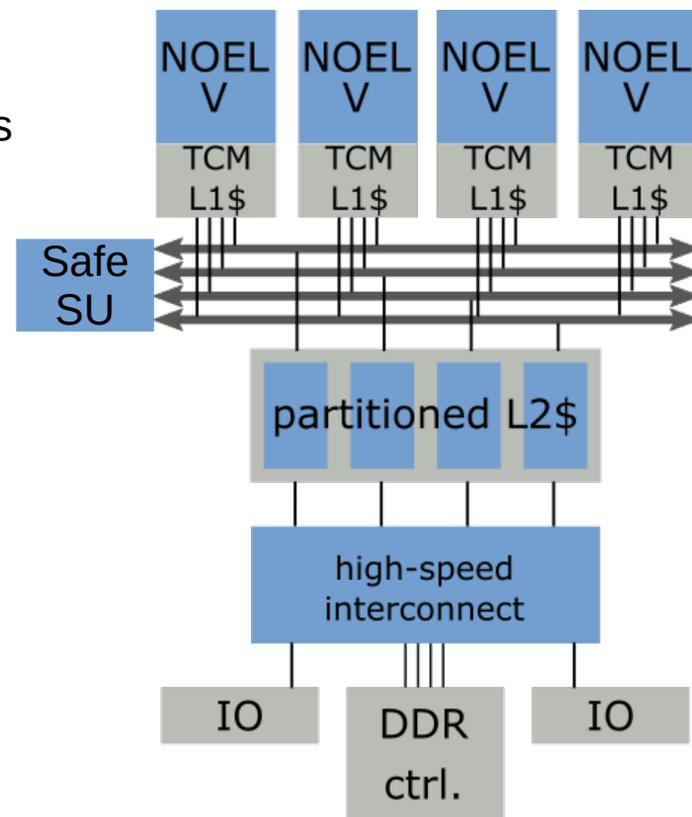
De-RISC hardware overview

- Quad-core SoC
  - Extensible to multiple clusters
  - Provision for Accelerators

- Implemented on FPGA
  - Xilinx KCU105 prototype board
  - DeRISC embedded board
  - Plans of future ASIC version

- Space-grade IO
  - SpaceWire, SpaceFibre, CANbus
 - MIL-STD-1553 provision

www.derisc-project.eu
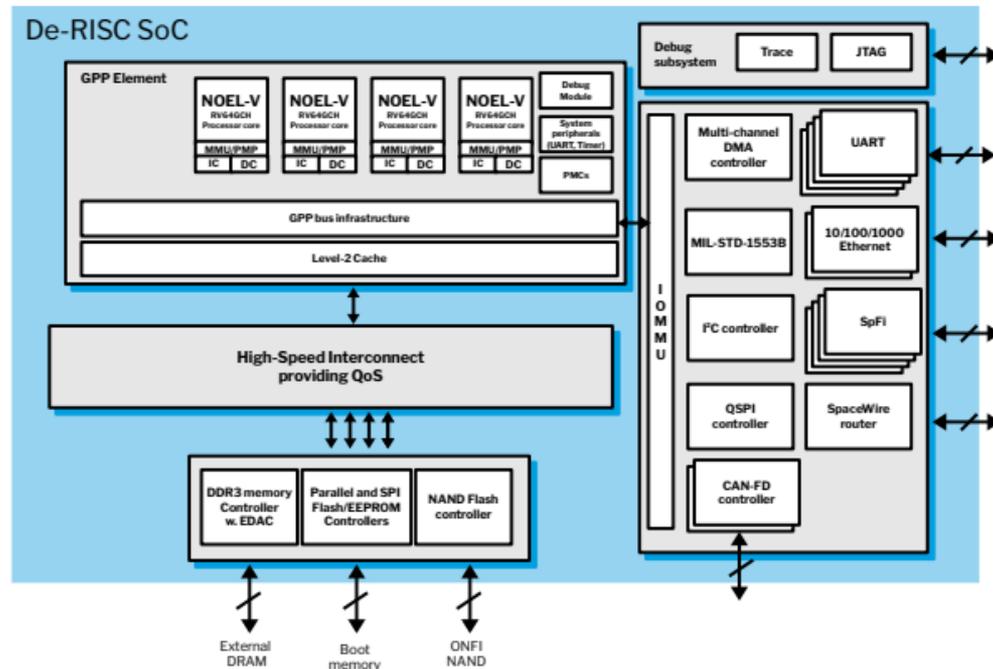
De-RISC software overview

- XNG
  - Lightweight hypervisor
  - Simple XRE execution environment
  - Support of LithOS as guest-OS, support of Linux and RTEMS in development
  - Used in OneWeb constellation

- LithOS
  - ARINC-653 RTOS running in a XNG partition
  - Planned certification ECSS level B (expected after end of project)

Multicore RISC-V reference board developed in the project

www.derisc-project.eu
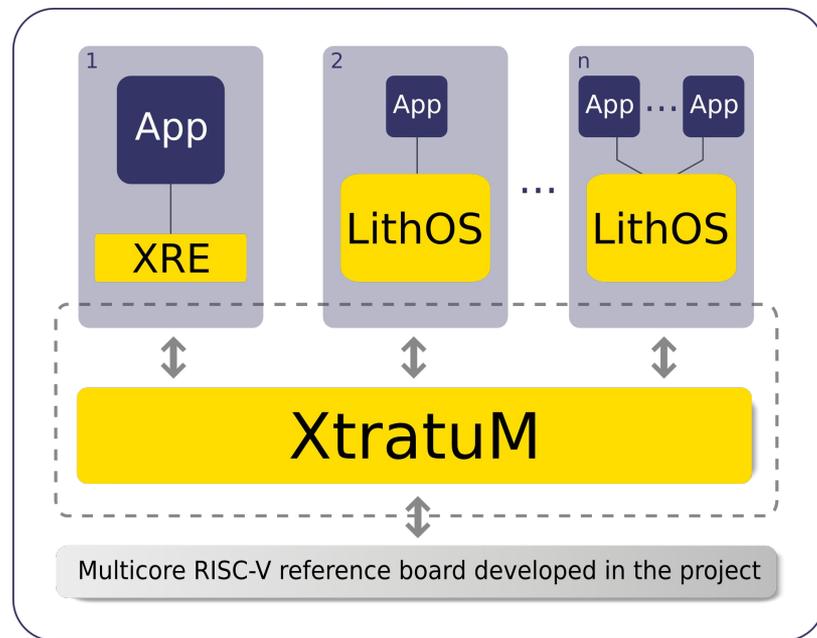
De-RISC validation use cases

- Basic benchmarks
  - Standards for performance estimation such as Dhrystone, Coremark
  - RISC-V ISA compliance suite
  - Stressing benchmarks to characterize interference channels

- Representative space payload software
  - Based on LVCUGEN from CNES
  - Hyperspectral image compression as data-intensive application
  - Realtime services as critical application

- Space use case for comparison with previous platforms
  - Control & Data Handling application from Thales Alenia Space Italy
  - Previously used in EMC² project on LEON-4 platform

www.derisc-project.eu
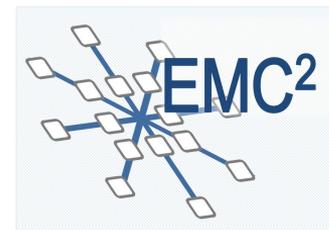
Flight software use-case

- Critical partitions based on LVCUGEN services
  - TM/TC messaging
  - IO server

- Memory-intensive partitions
  - CCSDS-123 lossless image compression
    - Hyperspectral data cube
    - Predictor and propagation
  - Additional stressing benchmarks in some configurations

- Validation of time and space isolation
 - Using SafeSU to monitor timing interference
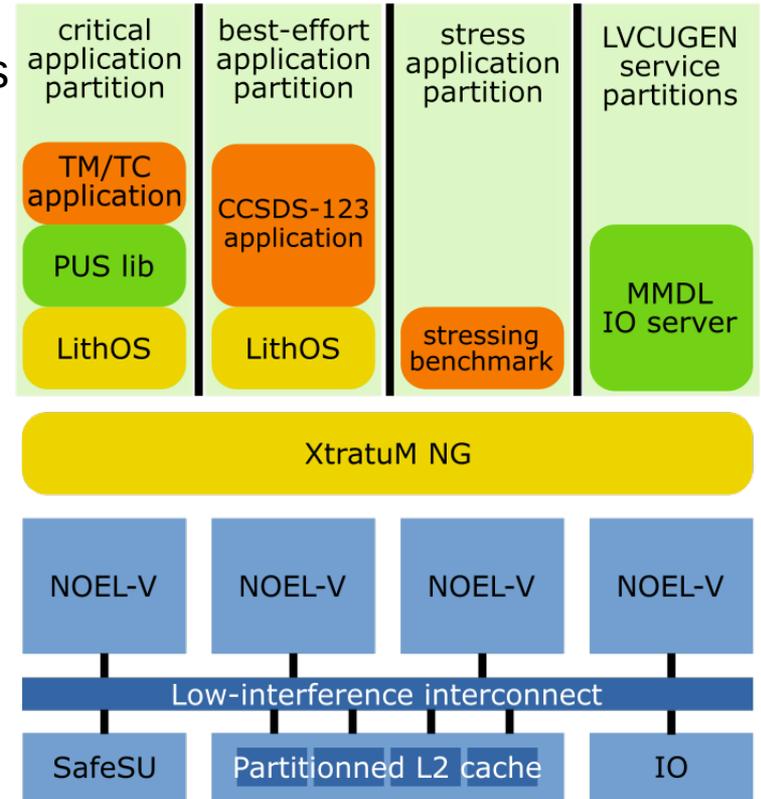
Current status

- Prototype SoC is functional on FPGA ✅
  - Scheduled integration of new features (incl. H extension)
  - Integration of SafeSU monitoring unit ✅
  - Flight-capable 6U cPCI Space Serial board in development
- Successful porting and integration of hypervisor and RTOS ✅
  - XtratuM Next Generation with SMP support, LithOS guest OS ✅
  - Linux and RTEMS porting as guest OS ongoing (out of scope of the project)
  - Development and deployment tools ✅
- Validation phase is started
  - Performance and stressing benchmarks ported ✅
  - Ongoing integration of space use-cases

www.derisc-project.eu

Conclusion

- Current challenges of safety-critical systems
  - Robustness
  - Timing interference on multicore COTS
  - New challenges of cybersecurity and export control

- Current solutions
  - Fault-tolerant technology
  - Observability and Deterministic Platform Software
  - Rising opportunities with Open Source Hardware

- De-RISC approach
  - Open-source, safety- and determinism-oriented multicore SoC
  - Complete and certifiable software stack
  - Advanced interference measurement and mitigation techniques
  - Validation with representative use-cases

www.derisc-project.eu
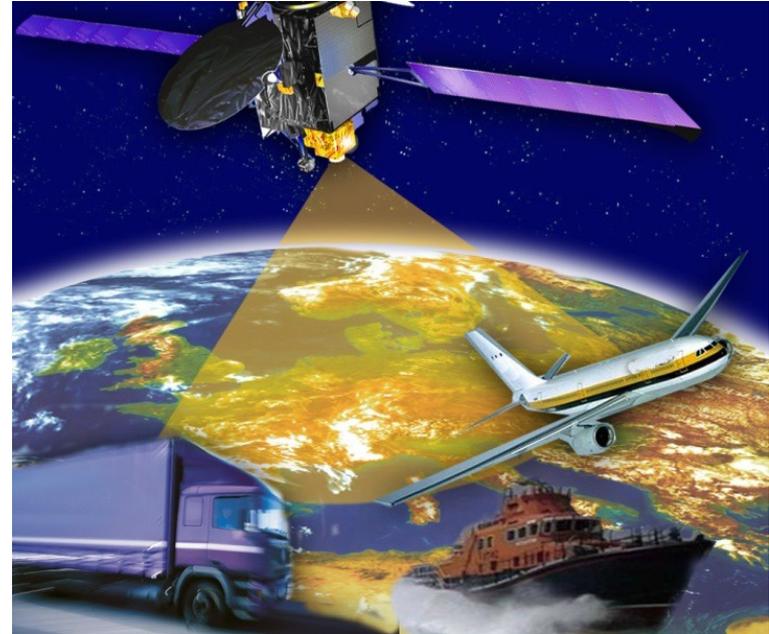
www.derisc-project.eu

(twitter) @DeRISC_H2020_EU   (in) De-RISC   (✉) info@derisc-project.eu