De-RISC – Dependable Real-time RISC-V Infrastructure for Safety-critical Space and Avionics Computer Systems

Francisco Gómez Molinero[a], Miguel Masmano[a], Vicente Nicolau[a], Nils-Johan Wessman[b], Jan Andersson[b], Jimmy Le Rhun[c], Guillem Cabo[d], Sergi Alcaide[d], Pedro Benedicte[d], Jaume Abella[d]

[a]fentISS, Spain
[b]Cobham Gaisler, Sweden
[c]Thales Research & Technology, France
[d]Barcelona Supercomputing Center (BSC), Spain

Abstract: The world market for aviation and space computing systems faces a significant shift caused by the loss of momentum of the traditionally used PowerPC and SPARC instruction set architectures in the commercial domain. This means that the space industry is not able to leverage training, software tools, etc. from the commercial domain and this fuels a need to shift to architectures present in larger commercial markets.

The De-RISC project brings together leading European entities within the areas of fault-tolerant microprocessors, hypervisors, embedded safety-critical software and mixed-criticality systems in an effort to commercialize a complete technology stack consisting of an FPGA space grade development board, system-on-chip design and software stack. The goal is to create a platform for the aerospace industries implementing the open RISC-V microprocessor instruction set architecture together with specific features to address the needs of the target industries and to adopt modern commercial technology to allow leveraging technology development from other domains.

The presentation will provide an overview of the De-RISC project, the technology building blocks (XtratuM hypervisor, NOEL-V processor), and a snapshot of the current project status.

Keywords: XtratuM, RISC-V, RV64GC, space computing, fault-tolerant microprocessors, hypervisor, mixed-criticality, safety-critical

Introduction

Recently, an open-source instruction set architecture called RISC-V has become extremely popular and it is supported by a plethora of companies and research institutions [1]. RISC-V offers a unique opportunity to develop EU-based products for the aviation and space domains with no dependence on non-European technology or proprietary IP rights, which would impose licensing fees and export restrictions otherwise. In this context, Cobham Gaisler has released NOEL-V, a synthesizable VHDL model of a 64/32-bit processor that implements the RISC-V instruction set architecture [2].

At software level, the trend in embedded systems is to use multicore platforms to build mixed-criticality systems on top of the same (multicore) computer managed by a hypervisor. The XtratuM hypervisor, fully developed in Europe by fentISS, has been qualified for SPARC and ARM based platforms for space missions and is already present in more than 200 orbiting satellites of different space missions [3].

In this framework, the De-RISC project consortium [4] brings together the experience of Cobham Gaisler (CG) as designer and developer of high-reliability microprocessors and system-on-chip integrated circuits based on the SPARC architecture, which continues to be dominant in the European space industry, and it is gaining market share in the US and Asian markets; fentISS (FEN) as software designer and developer of the XtratuM hypervisor that has been qualified for space missions for LEON3FT and ARM-Cortex R5 and A9, and is being qualified for multicore platforms [5]; the Barcelona Supercomputing Center (BSC) as research center for design and analysis of time-predictable safety-related hardware/software high performance technologies, and Thales Research & Technology (TRT) as reference centre of research and development of mission-critical information systems.

The main goal of the De-RISC project is to productize a multicore RISC-V system-on-chip (SoC) design and to port the XtratuM hypervisor to that design, thereby creating a full platform consisting of hardware and software for future European developments within aerospace applications. This achievement will contribute to establish a baseline multicore system-on-chip platform based on the RISC-V processor, generating a board with a path to flight and adapting the XtratuM hypervisor for the RISC-V platform. The project innovation lies in the introduction of innovative multicore technologies and bleeding edge commercial technology into existing space platforms.

System-on-Chip Platform

The architecture of the proposed De-RISC SoC platform is based on lessons learned and feedback from users of the radiation-hard fault-tolerant GR740 multicore processor [6]. Figure 1 provides a general view of the scalable SoC in a configuration foreseen for future application specific standard product implementations.

NOEL-V processors are organized in multicore clusters (GPP elements) connected to a shared level-2 cache. A third cache level is also introduced where the processing elements are connected with the input/output elements through an IOMMU. An accelerator cluster and an embedded FPGA are foreseen as part of the final design. However, within the De-RISC project, only one cluster of processors is expected to be implemented due to the limited size of the target FPGA, and the accelerator extensions and eFPGA will not be provided for the FPGA implementation.

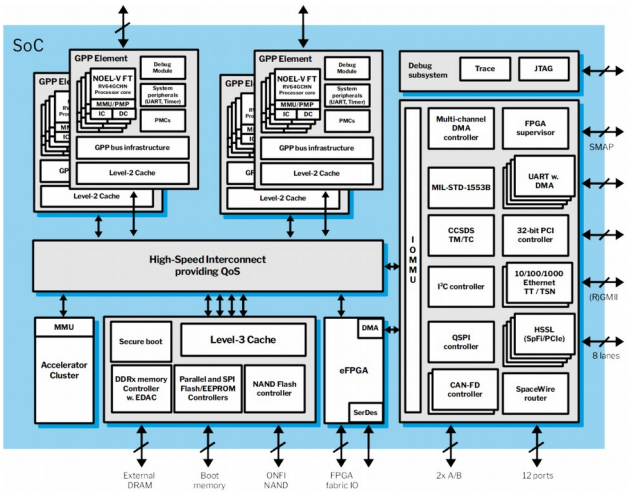

Figure 1. De-RISC SoC platform

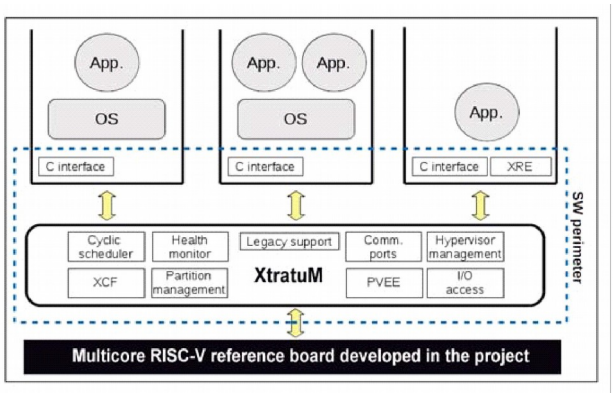

Figure 2. Typical XtratuM configuration

Software platform

On the software side, the XtratuM hypervisor will be ported to the hardware architecture defined in the previous section and the required run-time systems, in particular the ARINC-653 compatible LithOS run-time of fentISS [7], will be ported on top of the RISC-V XtratuM. The hypervisor will be enhanced to support multicore architectures, avoiding time interference when using shared resources by taking advantage of the mechanisms provided by the hardware. The starting point for the innovation proposed in the project is the XtratuM hypervisor and the associated guest operating systems (OSs) and run-time systems provided by FEN, and its schedulability analysis tool Xoncrete. Figure 2 shows a typical configuration with XtratuM running on top of the hardware platform developed in De-RISC: the block diagram illustrates a XtratuM-based system architecture with two partitions containing their corresponding guest OSs and their corresponding applications and a third partition containing a bare XtratuM run-time environment (XRE) with another application. XRE is a component provided with XtratuM for isolating a partition's application from the low-level management required by the Partition Virtual Execution Environment (PVEE, see figure 2). The XtratuM building blocks provide the services needed by safety-critical systems such as partition management, resource virtualization, scheduling, inter-partition communication, the XtratuM configuration, and the health monitoring service which detects faults in the hardware and in XtratuM itself.

Error detection and correction features

In addition to the health monitoring service that detects faults in the hardware and in XtratuM itself, the SoC platform has features for handling radiation-induced effects while allowing software to continue operating transparently.

The fault-tolerance features of the platform are implemented in the same way as have been done for current generations of LEON-based space-grade microprocessors. Memory elements are typically among the design elements more sensitive to radiation effects and the SoC design implements protection mechanisms for all on-chip and off-chip memories. Logic and other design elements are hardened against radiation effects using mitigation measures adapted for the programmable target technology.

For the hardware platform (FPGA-based board) developed within the De-RISC project, there will also be functionality on the board that guards against build-up of errors in the FPGA configuration memory.

Performance monitoring support

Although processors already incorporate Performance Monitoring Units (PMU), also known as statistics units, to track events such as instructions, cycles, and access counts, they are intended for average behavior characterization or debugging purposes. However, the timing verification and validation (V&V) of critical (e.g. safety critical) real-time applications on multicores have shown to require further monitoring support for an effective (V&V) process [8].

The platform will be extended with appropriate monitoring support in the form of a PMU specifically designed to monitor interference in multicore shared resources such as the interconnects used by the cores to reach the different shared caches or memories. For instance, it can measure how many cycles a specific master (e.g. a core) had to wait for being granted access to a given resource (e.g. a shared L2 cache) used by other masters. Figure 3 illustrates such an extended PMU for a shared interconnect.

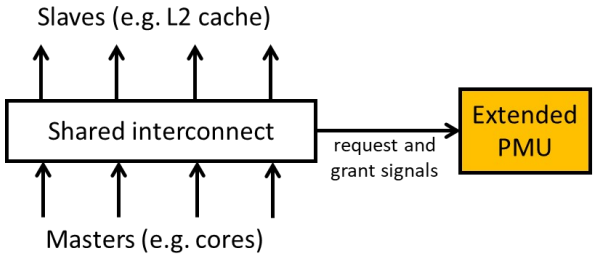

Figure 3. Extended PMU for a shared interconnect

The type of events that will be monitored include:

- Contention cycles: how many cycles each individual master has been delayed by the other individual masters, analogously to [9].
- Maximum latencies per access type: the maximum response time since a request is issued until it is responded per request type.
- Stall cycles and occupancy statistics for queues and buffers in shared caches.
- Statistics on implicitly generated activities such as shared cache evictions, invalidations due to coherence, and the like.

Use Cases and Validation

The technology developed in the project will be validated against the project requirements and through the use of space-specific use cases that will evaluate the project platform in typical space applications. The first application will be a Command and Data-Handling Application [10] developed by Thales Alenia Space Italy and previously used in the EMC^2 project over a LEON4 platform with the PikeOS hypervisor. The second application will be the generic LVCUGEN partitioned framework [11] provided by CNES to ease the development of complex payloads.

Project status

At the time of this writing the project has already completed the first reporting period and it is half-way to completion. The project started with a project requirement specification phase which collected the functional and non-functional requirements for the aerospace platform. It shortly followed by the design and implementation of the SoC IP as shown in figure 1 earlier. Figure 4 presents the SoC FPGA implementation with only one GPP element containing four CPUs, the more relevant I/O devices and some optimization in the IOMMU connection that allows L3 cache to be removed.

The other major hardware design block of De-RISC is the Safe Statistics Unit (SafeS-U), previously referred as PMU, implemented by BSC. This is depicted in figure 5.

It connects to the cluster-local AMBA bus providing maximum latency value for Worst-Case Execution Times (WCET) estimations and statistics on core contention. It also allows to setup interference quotas and raise interrupts in case they are exceeded.

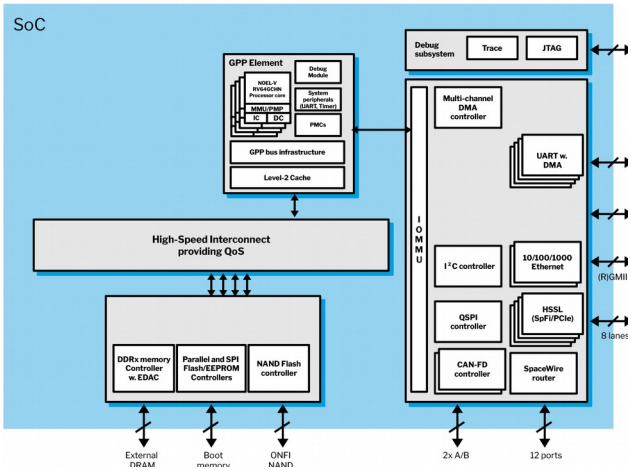

Figure 4. De-RISC SoC FPGA implementation

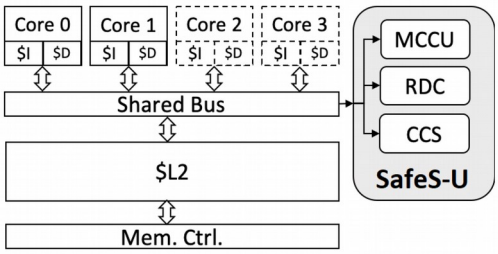

Figure 5. Safe Statistics Unit

The software development started with a monocore space-qualified version of XtratuM/NG (aka XNG) running on Zynq7000 MPSoCs. This version was extended to multicore by providing spin-locks for atomic operations and other required mechanisms. This version was ported to the RISC-V architecture and it was tested in the hardware platform of the project. The ARINC-653 compatible LithOS guest OS was ported over XNG. Some performance evaluation tests were run in the platform to allow comparison with other existing solutions.

At the time of this writing the development activities are almost complete. The project team will concentrate their effort in the validation activities which will apply the project validation strategy previously defined. Other remaining development activities will be: the implementation of the full virtualization extensions of RISC-V ISA (H-extensions) into the NOEL-V processor, the completion of a FPGA-based space grade development board, the support of the fully virtualized hardware platform by the hypervisor and the porting of guest OS of interest in the aerospace domain such as RTEMS and Linux.

Acknowledgements

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

References

[1] RISC-V Foundation. https://riscv.org/, accessed in May 2021.

[2] Cobham Gaisler. *“NOEL-V Processor”*, https://www.gaisler.com/noel-v, accessed in May 2021.

[3] fentISS. *“XtratuM”*, https://fentiss.com/products/hypervisor/, accessed in May 2021.

[4] *“De-RISC: Dependable Real-time Infrastructure for Safety-critical Computer”*, http://www.derisc-project.eu/, accessed in May 2021.

[5] Paco Gómez Molinero, Javier Coronel Parada, Miguel Masmano Tello, *“XtratuM: A space qualified Hypervisor for LEON-based Computers”*, GR740 User Day at ESTEC, 28th November 2019.

[6] Cobham Gaisler. *“GR740 Quad-Core LEON4 SPARC V8 Processor”*, https://www.gaisler.com/gr740, accessed in May 2021.

[7] fentISS, *“LithOS”*, https://fentiss.com/products/lithos/, accessed in May 2021.

[8] Enrico Mezzetti, Leonidas Kosmidis, Jaume Abella, Francisco J. Cazorla, *"High-Integrity Performance Monitoring Units in Automotive Chips for Reliable Timing V&V"*, in IEEE Micro, vol. 38, no. 1, pp. 56-65, January/February 2018.

[9] Javier Jalle, Mikel Fernandez, Jaume Abella, Jan Andersson, Matthieu Patte, Luca Fossati, Marco Zulianello, Francisco J. Cazorla, *"Contention-aware performance monitoring counter support for real-time MPSoCs"*, 2016 11th IEEE Symposium on Industrial Embedded Systems (SIES), Krakow, 2016, pp. 1-10.

[10] L. Pomante, D. Andreetti, F. Federici, V. Muttillo, D. Pascucci, *“Analysis and design of a Command & Data Handling platform based on the LEON4 multicore processor and PikeOS hypervisor*”, DAta Systems In Aerospace – DASIA 2017.

[11]Julien Galizzi, Jean-Jacques Metge, Paul Arberet, Eric Morand, Fabien Vigeant, et al.. *“LVCUGEN (TSP-based solution) and first porting feedback”*, Embedded Real Time Software and Systems (ERTS2012), Feb 2012, Toulouse, France.