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

Jimmy Le Rhun[1], Sylvain Girbal[1], Johan Klockars[2], Nils-Johan Wessman[2], Fabio Malatesta[2] and Jan Andersson[2]

[1]Thales Research and Technology
[2]Frontgrade Gaisler

Abstract

The surging demand for high-performance and autonomous systems in space applications necessitates more powerful space MPSoCs and suitable software solutions. These platforms must meet stringent reliability, verifiability, and validation criteria, given the harsh environmental conditions that spacecraft used in deep space missions must endure. This paper introduces computing platforms based on the NOEL-V processor, a RISC-V processor designed to offer a safe, secure, and reliable computing platform. The development of such features was initiated within the De-RISC H2020 project and has continued with various parallel activities.

Introduction

Compared to general-purpose computers, the processors used in critical systems such as spacecraft avionics must satisfy stringent requirements. In addition to size, weight, and power constraints common in embedded systems, extra safety-, security- and reliability-related properties must be ensured according to strict standards and regulations. Space environment adds stringent fault-tolerance and reliability requirements, especially related to lifetime, cosmic radiation, temperature, and vibrations.

In many cases, off-the-shelf components (COTS) optimized for best average performance are barely suitable in the context of critical systems, as speculative mechanisms are detrimental to worst-case execution time and its analysis, and cybersecurity threats increasingly target low-level hardware mechanisms [1]. Moreover, in multi-core processors, shared hardware resources can cause timing interference and/or be subject to cyberattacks, requiring new isolation techniques to protect applications from each other. Software-only mitigation techniques exist [2] but are often detrimental to performance.

In this challenging context, access to the hardware source code described in a high-level hardware description language, hardware with sufficiently detailed documentation, and especially RISC-V, offers the opportunity to address, in part or fully, these requirements at hardware level.

First, the availability of source code allows audit, formal analysis and documentation of low-level mechanisms that were often black boxes in regular COTS, such as interconnect arbitration or cache management. Implementation of open standards, such as the RISC-V ISA, eases such efforts.

Critical systems are usually integrated in niche markets that cannot afford the cost of dedicated dependable ASICs, with the notable exception of the space domain. The RISC-V ecosystem is an opportunity to devise and implement new dependability-oriented hardware mechanisms, especially as the final product is often FPGA-based.

Lastly, within RISC-V International, the critical-systems community shares ideas and advocates for suitable mechanisms and extensions, e.g. in Functional Safety Special Interest Group [3] and Trusted Execution Environment Task Group among others.

Developed Solutions

The NOEL-V is a RISC-V architecture processor specifically engineered for space applications. As a synthesizable VHDL model, it offers multiple options for customization, allowing System-on-Chip (SoC) designers to develop solutions that meet their specific requirements. In its most advanced configuration, the NOEL-V processor features the GCBH extensions of the 64-bit RISC-V instruction set.

In the following sections, we will discuss relevant safety and security features that are either already deployed or under development.

Isolation & Partitioning

The RISC-V H extension enables the use of Virtual Supervisor and Virtual User modes, which facilitate the creation of virtual machines capable of running complex operating systems unmodified. This is a notable departure from the para-virtualization solutions currently in use in European space computers. By leveraging this capability, in conjunction with hypervisor software, it is possible for different applications with different criticality levels to share the same hardware platform through the isolation in time and memory space of their execution environments. As an illustration, let us consider a use case developed as part of the De-RISC project. This particular use case utilized the LVCUGEN framework [7], which was

executed on an SoC based on the NOEL-V architecture and controlled by the Xtratum XNG hypervisor [4]. In this scenario, critical partitions responsible for essential satellite operations such as ground-to-satellite communications, positioning, and mission control run on the same computer as non-critical partitions that performed payload computation tasks, such as image compression. The different partitions do not interfere with one another thanks to Xtratum and to innovative hardware features minimizing interference channels.

In order to minimize interference channels between the cores and the memory, NOEL-V supports an address-striped multi-bus interconnect towards the multi-port L2 cache and between the L2 Cache and the DRAM memory controller. It allows bus transactions to complete independently of traffic from other cores, while private scratchpad memories allow processing of critical sections in isolation, and the RISC-V IOMMU [8] ensures the partitioning of the IO devices' memory space.

Reliability

The cache memories of the NOEL-V processor are resilient to radiation-induced Single Event Upsets (SEUs) through a patent-protected error correction scheme [5]. This scheme is capable of correcting single bit errors, detecting double bit errors, and even detecting 3-bit and 4-bit adjacent bit errors. The correction process occurs transparently within the cache controller, with no requirement for software intervention or additional memory accesses. Furthermore, the caches are equipped with a hardware scrubber that can be automatically activated to prevent error accumulation. These features have been validated through FPGA-based radiation testing, and their performance has been documented in academic papers such as [6].

The NOEL-V processor can be connected to a DRAM memory controller that incorporates advanced fault tolerance measures. The controller employs a robust error correction code that provides double device correction, ensuring the accuracy of data even in the event of one full device failure and random SEU-induced errors on other devices. The DRAM memory controller was developed within a European Space Agency activity and is available under the product name FTADDR.

Integrity

In a typical program execution, the call stack is used to keep track of the sequence of function calls, including the return addresses of each function. An attacker can exploit vulnerabilities in a program by overwriting the return address with a malicious address, causing the program to execute arbitrary code. A shadow stack provides an additional layer of protection by maintaining a separate stack of return addresses, separate from the regular call stack. The return addresses on the shadow stack are stored in a secure memory region that is protected from modification by the attacker. This has been implemented in the NOEL-V according to the RISC-V extension draft for control flow integrity, Zisslpcfi. This extension also includes landing pads which make it possible to enforce that indirect jumps and calls can only go to specific points in a program, thereby closing off another attack vector.

Perspectives

The NOEL-V processor is already available on the Frontgrade Gaisler website, within the GRLIB VHDL IP library, under both GNU GPL and commercial licenses. Demo bitstreams for several FPGA evaluation boards are also available.

The design of an octa-core radiation hardened ASIC version is ongoing, with a preliminary release target of H2-2024. In the presentation, we will be showcasing benchmark results obtained from the NOEL-V octa-core system, along with detailing the various additional features and extensions that are currently being actively developed.

Acknowledgments

The De-RISC project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869945.

References

[1] Paul Kocher et al., "Spectre attacks: Exploiting speculative execution". *40th IEEE Symposium on Security and Privacy* (S&P'19), 2019.

[2] S. Girbal et al., "Deterministic Platform Software for hard real-time systems using multi-core COTS". *34th Digital Avionics Systems Conference*, DASC'2015.

[3] RISC-V International, Functional Safety Special Interest Group, https://lists.riscv.org/g/sig-safety

[4] N. -J. Wessman et al., "De-RISC: the First RISC-V Space-Grade Platform for Safety-Critical Systems," *2021 IEEE Space Computing Conference (SCC), Laurel, MD, USA*, 2021, pp. 17-26

[5] Patent number WO2023277746A1, DATA VALIDATION AND CORRECTION USING HYBRID PARITY AND ERROR CORRECTING CODES, Magnus Hjorth, Frontgrade Gaisler AB

[6] Ádria B. de Oliveira et al., "NOEL-V FT and GRSCRUB IP: Fault Tolerance Characterization of a Complex System-on-Chip on Xilinx Kintex UltraScale FPGA", *Poster session of RADECS 2022*

[7] J. Galizzi et al., "LVCUGEN (TSP-based solution) and first porting feedback". Embedded Real Time Software and Systems (ERTS2012), Feb 2012, Toulouse, France. ⟨hal-02192398⟩

[8] RISC-V IOMMU Specification, Version 0.9, January 2023, https://github.com/riscv-non-isa/riscv-iommu