SmallSat Payload Control & Data Processing: High-Reliability and High-Security With RISC-V

Gerard Rauwerda[1]*, Camiel Vletter[1], Dave Marples[1], Marco Ottavi[2], Bruno Forlin[2], Sybren de Jong[3], and Hans Dekker[4]

[1]Technolution, Gouda, The Netherlands, [2]University of Twente, Enschede, The Netherlands, [3]Royal NLR, Amsterdam, The Netherlands, [4]Irdeto, Hoofddorp, The Netherlands

Abstract

This work presents a Control & Data Processing Unit targeted at SmallSats which sits between a platform and its instruments. It includes a (possibly radiation-hardened) FPGA with a RISC-V softcore and optional accelerators, allowing for edge processing. This opens the door for payload control, encryption and data processing in space. The CDPU also reduces time-to-orbit by removing the need to design an instrument for a specific platform.

Introduction

RISC-V is an open instruction set architecture (ISA) created in 2010 at UC Berkeley [1]. It has since grown to be used worldwide. This paper proposes a demonstrator, developed as part of the TRISTAN project, which paves the way for getting RISC-V into space. Previous work [2, 3] has presented the challenges involved in achieving this. We aim to address some of these challenges, particularly with respect to high-energy particle protection and security aspects.

We define a satellite as comprising a *platform* and one or more *instruments*. The platform provides power to the instruments, is the satellite's structural support, and is used for offboard and inter-instrument communication. Each instrument performs at least one payload function (e.g. Earth Imaging).

This paper proposes a *Control & Data Processing Unit* (CDPU) for satellites to provide a standardised interconnect between the platform and its instruments. This CDPU is aimed at SmallSats in the micro and mini satellite classification, as defined in [4], meaning satellites with a mass in the order of 10 to 1000 kg. These classes of satellite have enough capacity margin (volume and weight) for the instruments we target.

Problem description

Instruments have a hard dependency on their SmallSat platform. They are designed to interface with a specific satellite, and any change in platform nearly always introduces significant mission delays.

Further, most contemporary scientific and commercial satellites do not encrypt instrument data, nor concern themselves with intra-satellite hardware security. The data collected by the satellite is often the satellite's business case, and satellites are constantly in view of potential attackers as they orbit the globe. Protecting these data becomes increasingly important, especially when out of downlink range. This problem is accentuated by the lack of edge processing, as this necessitates increased data volumes to be sent to earth via a high throughput downlink. The need for both encryption and edge processing could be addressed by adding compute capabilities between the instrument and the platform, with the additional benefit of breaking of the one-to-one binding between the platform and the instrument, enabling instrument portability.

Finally, a re-configurable data processing unit would allow changing mission requirements to be addressed, but comes with the risk that enabling reconfiguration could leave the platform vulnerable to malicious actors seeking to inject unauthenticated IPs (e.g. hardware trojans), or access vulnerable features before they are patched, such as micro-architectural attacks in the style of the Spectre [5] or Meltdown [6] vulnerabilities.

Solution proposal

The *Control & Data Processing Unit* (CDPU) is proposed to address the aforementioned problems, as shown in Fig. 1. The CDPU contains the RISC-V FreNox[1] softcore, accelerator logic, and two custom built SpaceWire [7] (SpW) interfaces. SpaceFibre [8] (SpFi) can also be used for higher data throughput. These logic blocks are implemented in a conventional or radiation-hardened FPGA, depending on mission requirements. The SpaceWire interfaces are developed to connect to specific platforms and instruments, thus reducing the effort required to support different platform/instrument combinations.

Specific interfaces for certain platforms and instru-

*Corresponding author: gerard.rauwerda@technolution.nl

[1] See: technolution.com/advance/insights/frenox/. Successfully used in high-grade security solutions. See: technolution.com/prime/

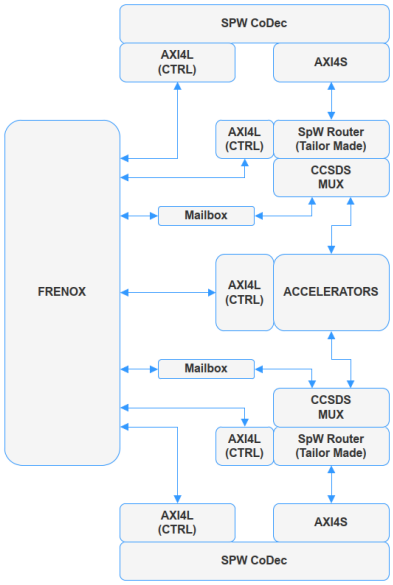

Figure 1: *Simplified architectural design of the CDPU.*

ments may be added. These are tailor-made and contain the corresponding SpW/SpFi connectors for the instrument or platform, as well as any necessary 'housekeeping' connectors for configuring the device.

In Fig. 1 we see the RISC-V microcontroller (FreNox) and optional accelerators that can be used for in-orbit computing and control. The accelerator logic blocks can be used to process large amounts of data, such as image analysis or combining measurements data. The RISC-V softcore can be used for control and security purposes including cryptographic key management used to secure the communication of data back to earth and the control of the instrument, platform, or accelerators, as well as mechanisms to ensure that software and/or firmware can be upgraded in a secure manner.

New protocols will be developed to deliver a secure update mechanism for the CDPU software based on NIST-recommended Post Quantum Cryptographic (PQC) primitives. This will ensure that the CDPU can be maintained securely throughout the mission, even in a post-quantum world.

PQC protocols may also be used for the encryption and authentication of raw and processed instrument data. The proposed solution will include a Root of Trust (RoT) in the CDPU to guard the identity of the device. These data will be injected during device manufacturing using a secure key generation and provisioning system (using Irdeto's 'Keys & Credentials'[2]).

These security measures will be enhanced with lightweight checkers. If a malicious third party or random event would affect the control flow or data integrity, a checker can prevent the propagation of the invalid or insecure state.

[2] See: `irdeto.com/connected-transport/keys-credentials/`

Conclusions

This paper proposes a *Control & Data Processing Unit* (CDPU) for use on SmallSats. This device targets satellites in the order of 10 kg to 1000 kg and is used as versatile interfacing unit between the satellite platform and a number of instruments. It will run on a radiation-tolerant FPGA and contains SpW and/or SpFi interfaces to connect between the platform and instrument(s), a RISC-V softcore, and optional accelerators.

The CDPU offers simpler recombination of instruments and platforms into differing configurations. It also enables edge computing to lower necessary data throughput to earth and thus latency. It further allows for the encryption of the valuable payload data and reconfigurability of the compute capabilities in the case of changing mission requirements.

Acknowledgements

The work presented in this paper is part of the TRISTAN project. TRISTAN has received funding from the Key Digital Technologies Joint Undertaking (KDT JU) under grant agreement nr. 101095947.

References

[1] Andrew Waterman. "Design of the RISC-V Instruction Set Architecture". PhD thesis. EECS Department, University of California, Berkeley, Jan. 2016. URL: `http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-1.html`.

[2] Stefano Di Mascio et al. "The Case for RISC-V in Space". In: *Applications in Electronics Pervading Industry, Environment and Society*. 2019, pp. 319–325. DOI: `10.1007/978-3-030-11973-7_37`.

[3] Luca Cassano et al. "Is RISC-V Ready for Space? A Security Perspective". In: *2022 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. 2022, pp. 1–6. DOI: `10.1109/DFT56152.2022.9962352`.

[4] Herbert J. Kramer and Arthur P. Cracknell. "An overview of small satellites in remote sensing". In: *International Journal of Remote Sensing* 29.15 (2008), pp. 4285–4337. DOI: `10.1080/01431160801914952`.

[5] Paul Kocher et al. "Spectre Attacks: Exploiting Speculative Execution". In: *Commun. ACM* 63.7 (June 2020), pp. 93–101. DOI: `10.1145/3399742`.

[6] Moritz Lipp et al. "Meltdown: Reading Kernel Memory from User Space". In: *Commun. ACM* 63.6 (May 2020), pp. 46–56. DOI: `10.1145/3357033`.

[7] S.M. Parkes and P. Armbruster. "SpaceWire: a spacecraft onboard network for real-time communications". In: *14th IEEE-NPSS Real Time Conference, 2005*. 2005, pp. 6–10. DOI: `10.1109/RTC.2005.1547397`.

[8] S. M. Parkes et al. "SpaceFibre: A multi-Gigabit/s interconnect for spacecraft onboard data handling". In: *2015 IEEE Aerospace Conference*. 2015, pp. 1–13. DOI: `10.1109/AERO.2015.7119317`.