Title: Porting an ECSS qualified flight boot loader software to RISC-V architecture

As RISC-V processors are introduced to European space missions the RISC-V software ecosystem can be leveraged. Mission criticality sets requirements on the software design, its development processes and that quality is ensured, and the proof thereof. Evidence is a factor when choosing software for reuse in missions. Essential for all computer systems is a reliable boot procedure responsible for starting the flight software that implements the actual function in the spacecraft. However, the boot start-up code is typically highly platform specific consisting of low-level initialization and machine code difficult to reuse between platforms and processor architectures without major porting efforts.

This presentation will describe the approach taken to port GRBOOT to RISC-V, GRBOOT is an existing ECSS-qualified SPARC boot loader. Rather than reusing a non-qualified RISC-V boot loader. The reason being the amount of work needed to re-engineer evidence able to claim Category B compliance to the ECSS-E-ST-40C/ECSS-Q-ST-80C [1] software standards.

Background

European space has a long heritage in SPARCv7 and SPARCv8 computer systems and the use of board or even project specific boot loader solutions.

During the 2010s ESA gathered boot requirements with input from industry leading to a specification with common requirements, summarised in the "SAVOIR Flight Computer Initialisation Sequence Generic Specification" [2] document. The specification is appliable to both On-Board Computers and Payload computers. The requirements are not only functional but also include requirements on the software engineering process and product assurance compliance.

Note SAVOIR documents are restricted to European member states.

Mission and board specific boot loaders developed in the past typically resulted in varying compliance to SAVOIR and repetitive review. The GRBOOT flight boot loader software was originally designed for the ESA JUICE mission in 2015 [3], to provide a common boot loader for several different Payload computers based on the LEON3-FT processor. The computers were interfaced to the same SpaceWire network for maintenance such as application uploads from ground implemented by a software named Standby in SAVOIR.

Since then, GRBOOT [4] has been ported to GR740/LEON4 and during 2024/2025 also to the GR765/LEON5 platform within an ESA funded activity. GRBOOT has been validated on a GR765 FPGA prototype in LEON5 configuration. Verification activities and a product

assurance flow have been applied in parallel to the development to ensure compliance to design processes and quality goals are met.

RISC-V is being introduced

With the GR765 developed by Frontgrade Gaisler under ESA funding, RISC-V becomes available to space applications that require a space grade processing solution. Migrating existing space applications to RISC-V will require a reliable boot loader solution as part of the software stack.

ESA has initiated a RISC-V software development activity where Frontgrade Gaisler is the prime. The project focuses mainly on porting existing software commonly used in European space to RISC-V, but also exploring new software solutions where RISC-V provides new possibilities. Relevant to the topic of this paper, the project includes two boot loader developments for RISC-V:

- Porting GRBOOT/STANDBY software to RISC-V in the GR765 platform, with tailored ECSS E40/Q80 Category B compliance
- Explore and prototype security extensions to GRBOOT through Authentication of boot images

Presentation and results

GRBOOT key functionality used in space will be presented and the on-going efforts porting the boot loader to RISC-V. Early results from the development will be presented including, changes made in the tool set have been required, identified SAVOIR requirements not possible on RISC-V, and techniques for gathering code coverage have been switched away from using simulator to relying on the toolchain. The benefits of using a simulator to gain code coverage on low-level boot initialization code, often difficult to gather from unit-tests, will be discussed.

[1] European Cooperation for Space Standardization, https://ecss.nl/

[2] “SAVOIR Flight Computer Initialisation Sequence Generic Specification”, SAVOIR-GS-002

[3] GR712RC Boot software, https://www.gaisler.com/products/gr712rc-boot-software

[4] GRBOOT Flight Boot Loader, https://www.gaisler.com/products/grboot