

RVIS 2025

Enhancing Maintainability and Reliability in Space Applications: A RISC-V Based System Controller for High-Performance Data Processing Units for Small Satellites Using LiteX

Daniel Garbe, Clemens Horch, Konstantin Schäfer

System Controller

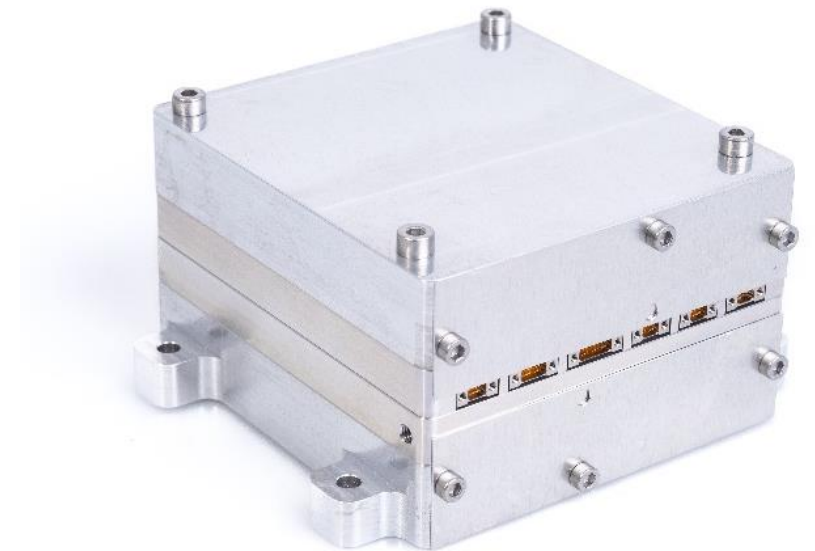
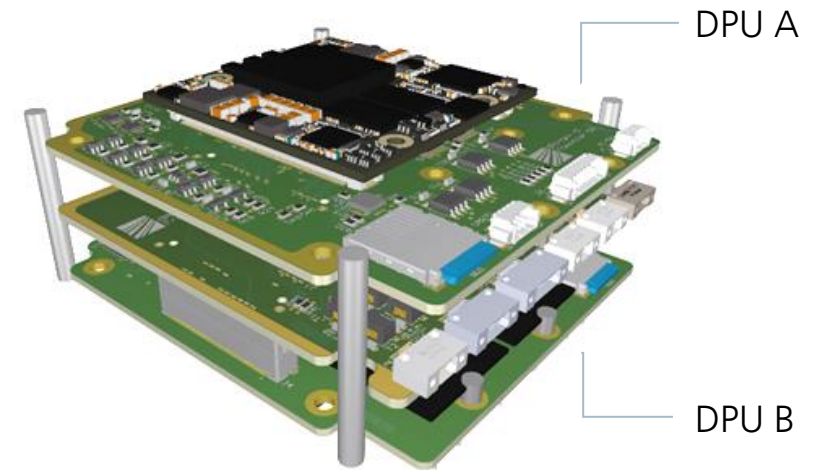
Properties

In EMI Data Processing Unit (DPU):

- Latch-Up protection
- Power rail supervising and control
- Boot medium selection and redundancy hand-over

In general:

- Autonomous FDIR to configurable error syndromes (power, computational, interfaces)
- CSP capable
- Permanently powered on



Overview system architecture

MPSoC and System Controller

Latch-Up Protection

- Power Monitoring up to 12 channels
- Soft- and hard latch-up detection
- Power switches on component level

Redundancy and FDIR

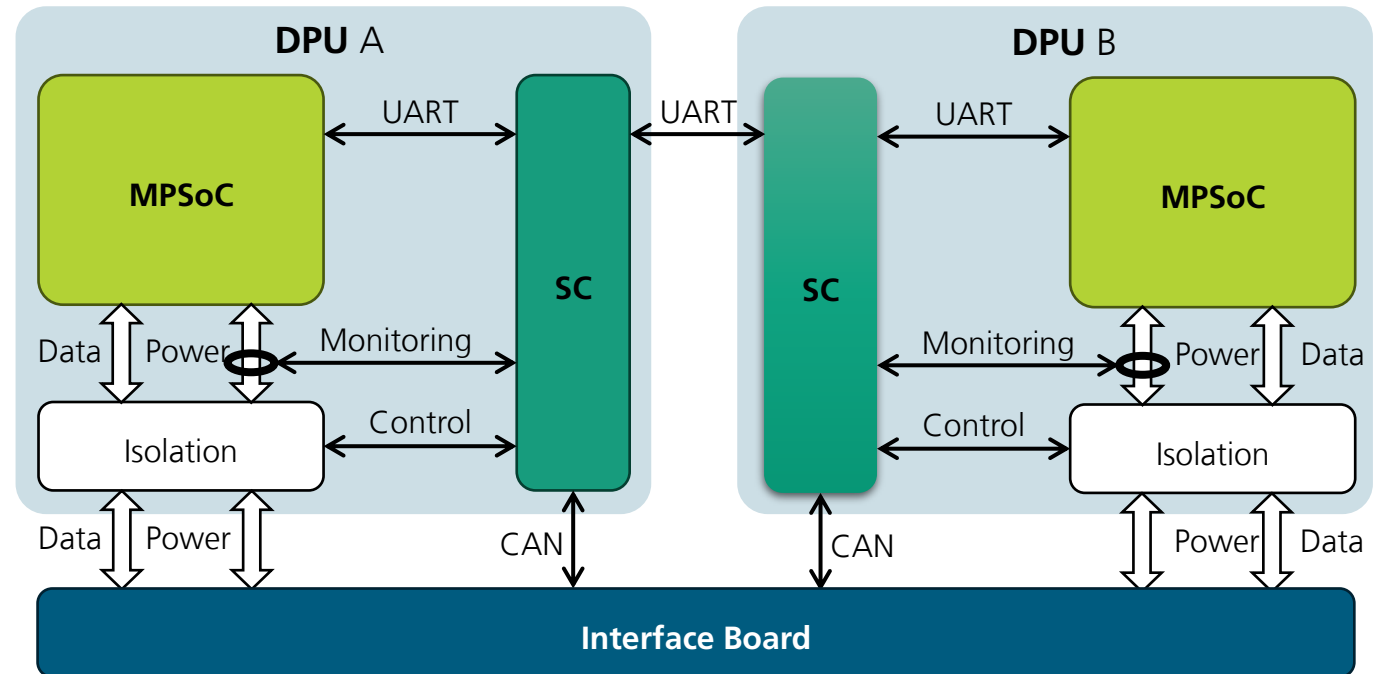
- Distributed FDIR in hard- and software
- Optional automatic boot medium failover

Housekeeping

- Voltages, Currents, Power consumption
- Faults, statistics, causes etc.

Interfaces and protocols

- UART, redundant CAN
- CSP 1.6 or 2.0 (CAN/KISS)
- Interconnects: SCs and SC/MPSoC



System Controller

Why is a RISC-V softcore used?

Maintainability

- Reusable hardware
- Modular code base

Reliability

- FDIR concept embracing fail-safe firmware updates
- RISC-V ecosystem with high-reliability (DMR/TMR)

Flexibility

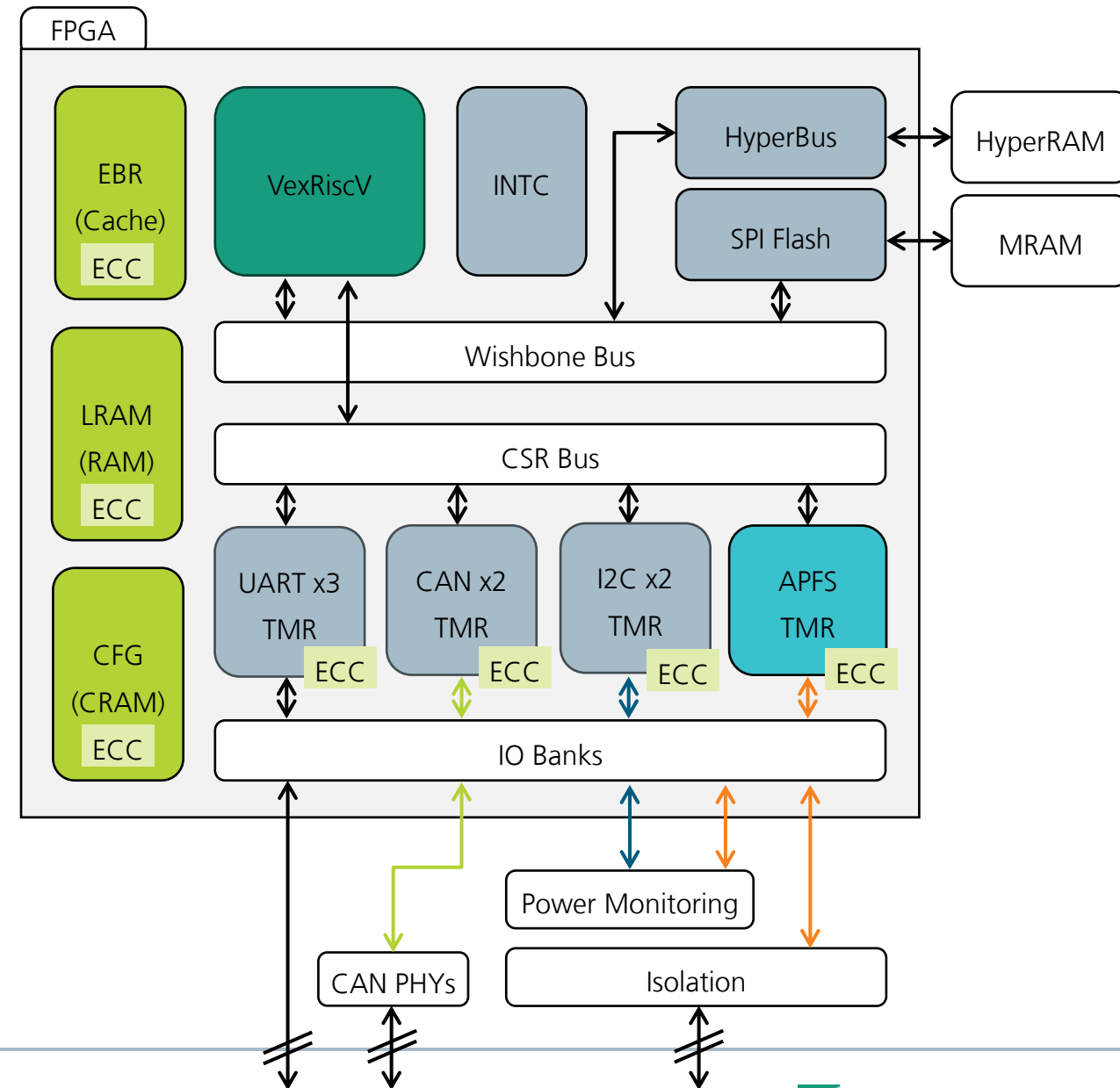
- Reconfigurable interfaces and hardware with “plug-and-play” character
- Fast project related changes / shunting of damaged hardware

System Controller

Architecture of SoC and Peripherals

LiteX

- Python-based hardware description framework
- Providing standardized SoC Cores (no DMR/TMR) and Peripherals
- Highly modular and reusable software design
- Easy to adopt to FDIR concepts (to a certain degree)
- Zephyr support



Fault analysis

Major insights

A/DSET

- *Clock* supervising needed
- Transient timespan may coincide with clock period
- ECC augmented *bus design*
- Oversampling in analog domain needed

SEU/MBU

- ECC protected configuration
- Registers and FIFOs: ECC of block memories: or LiteX inferred ECC design

SEL

- Configuration: reconfiguration needed

From LiteX SoC perspective

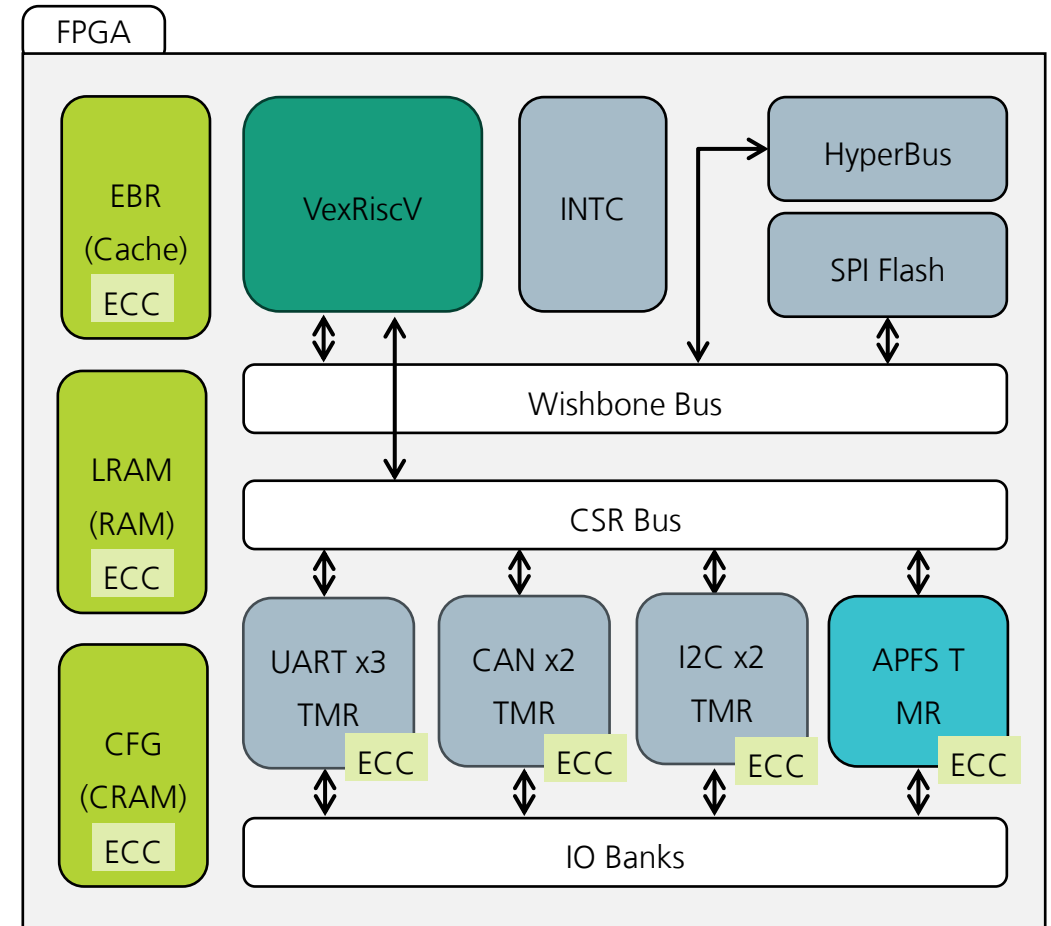
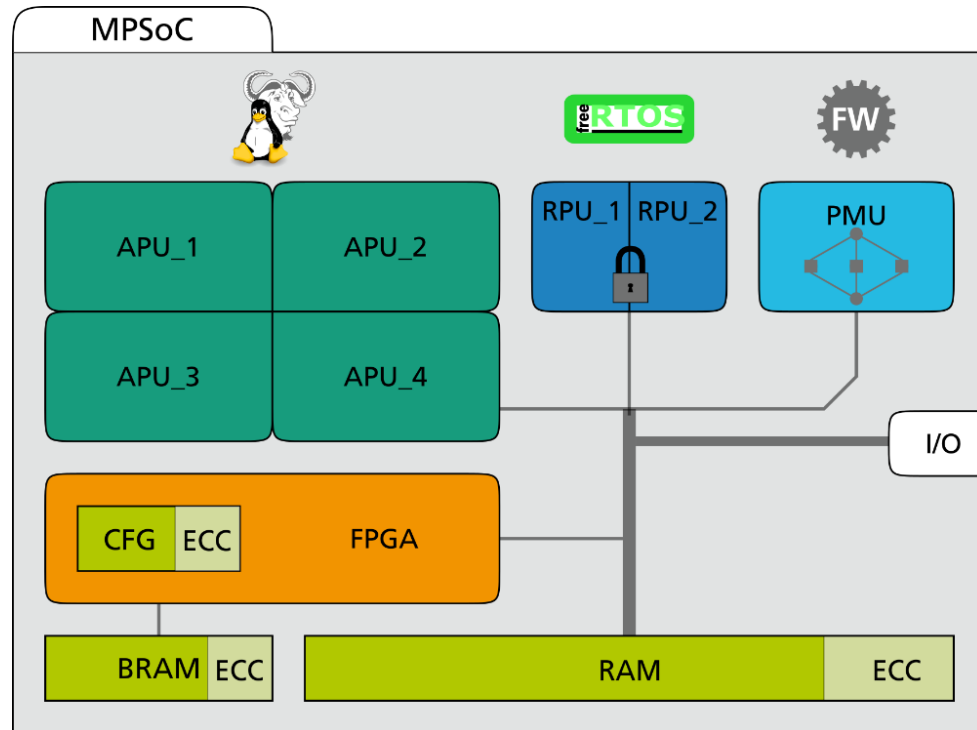
- TMR favorable, but challenging to implement for pre-generated Verilog cores
- SEU, MBU, SEFI and SEL require distributed software approach for FDIR of cores + watchdogs

From System Controller's perspective

- High-reliability of interfaces and GPIOs
- Accessing registers and IO must be fault-tolerant

Similarity of FDIR demands

MPSoC and SC FPGA



FDIR concepts

Applying to LiteX and Software

Triple Modular Redundancy

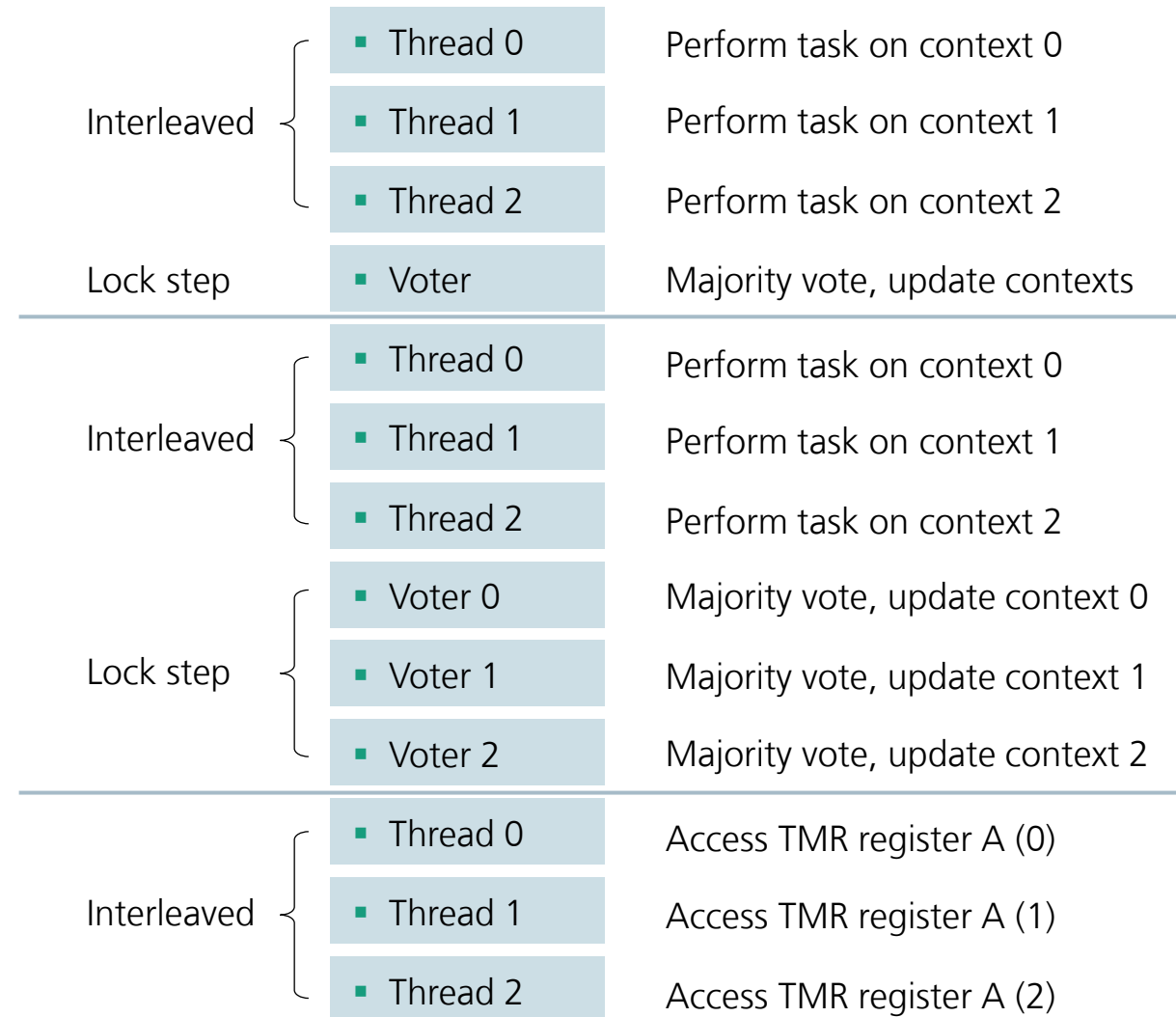
- Interface peripherals (LiteX modules): hardware
- LiteX cores interleaved threaded redundancy / lock steps
- Distributed instruction mimicking → software diversity

Triplication and Majority Vote

- With exception to finite-state-machines

ECC augmented Bus Design and Registers

- CSR: DSET/SEU ✓
- Wishbone: high throughput ✗



Contact

Daniel Garbe
Embedded Systems Group
daniel.garbe@fraunhofer.de

Fraunhofer EMI
Ernst-Zermelo-Str. 4
79104 Freiburg
www.emi.fraunhofer.de



Fraunhofer-Institut für Kurzzeit-
dynamik, Ernst-Mach-Institut, EMI