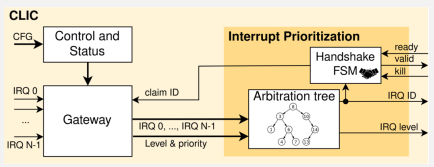
SentryCore: A RISC-V Co-Processor System for Safe, Real-Time Control Applications

Michael Rogenmoser[1], Alessandro Ottaviano[1], Thomas Benz[1], Robert Balas[1], Matteo Perotti[1], Angelo Garofalo[1,2], Luca Benini[1,2]
[1]Integrated Systems Laboratory, ETH Zurich; [2]Department of Electrical, Electronic, and Information Engineering, University of Bologna

Real-time

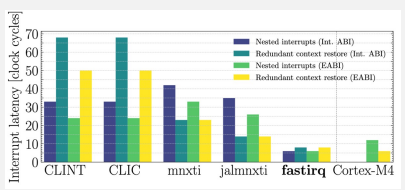
CLIC:
Core-Local
Interrupt Controller

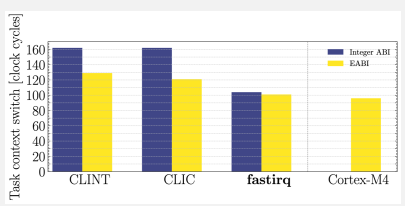
Provides advanced interrupt handling



fastIRQ Extension

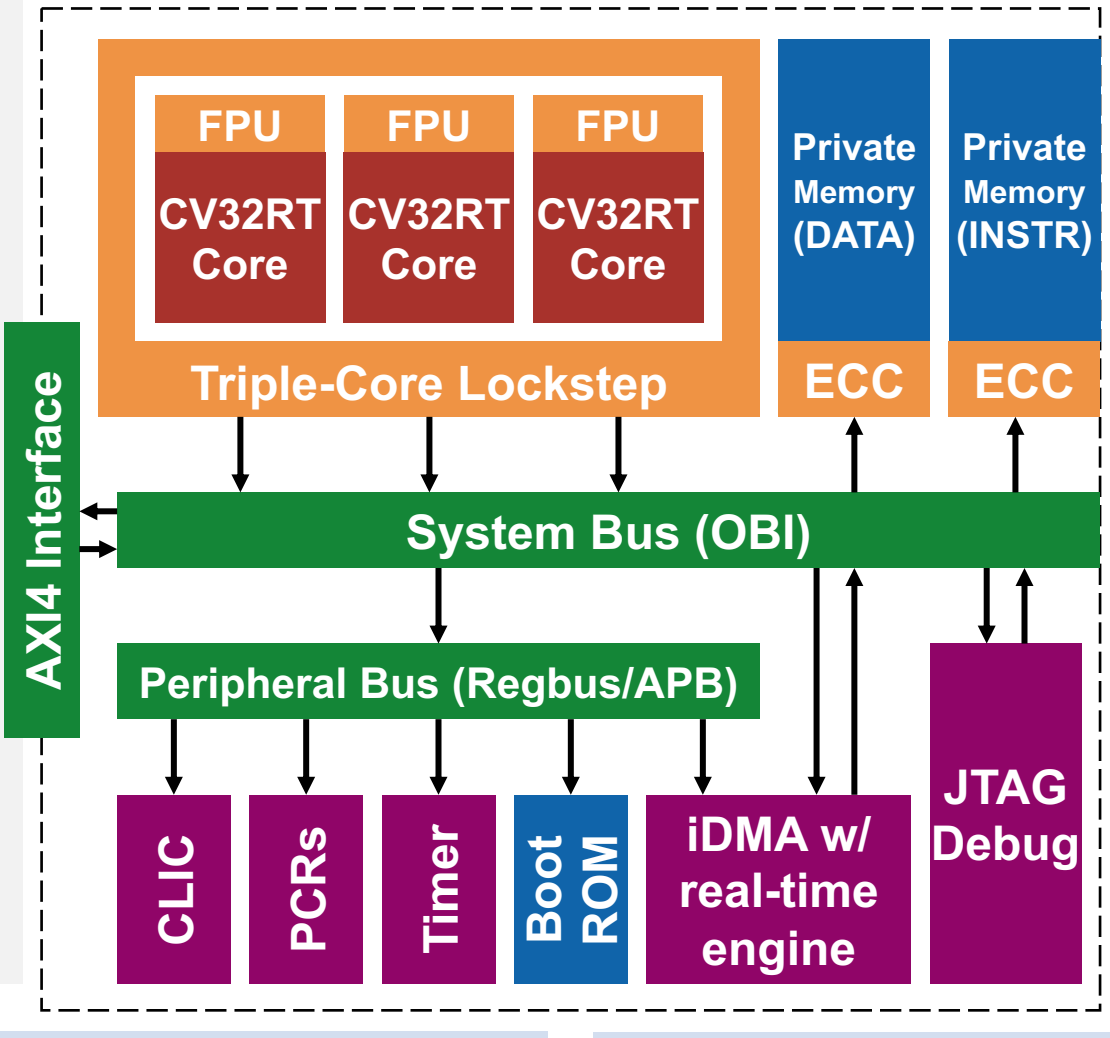
Provides low interrupt latency and fast context switch





Automotive SoCs are growing in complexity towards mixed-criticality systems (MCS) but still require reliable, real-time control.

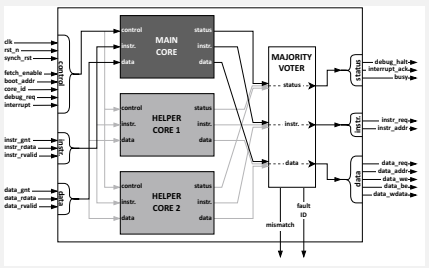
We present a dependable 32-bit RISC-V-based mega-IP for safety-critical, real-time MCS subsystems.



Reliability

TCLS:
Triple-Core Lockstep

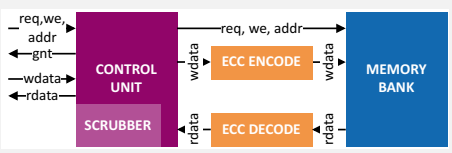
Majority-voted cores with state recovery for reliable execution



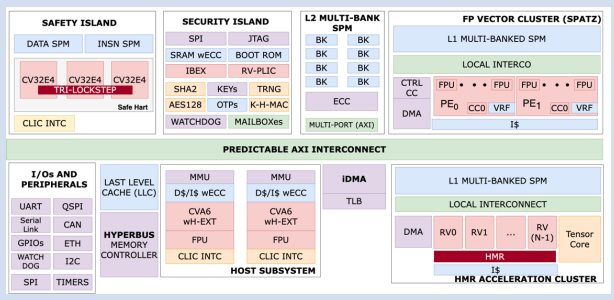
ECC-protected memory

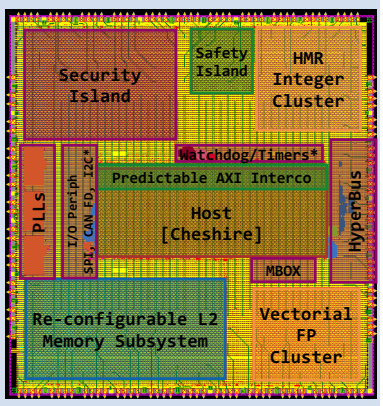
Reliable data storage with Hsiao code single error correction, double error detection.

Efficient sub-word storage and scrubber to correct latent errors.



The Carfield Mixed-Criticality System





Modules marked with (*) are not in scale

Dedicated support for multiple real-time Operating Systems

FreeRTOS

ThreadX

RTIC
Real-Time Interrupt-driven Concurrency

SentryCore Configuration

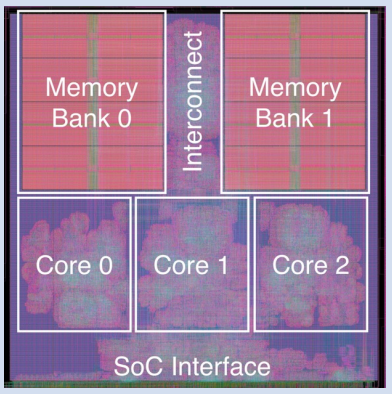
- CV32RT, FPU (32bit), CLIC
- TCLS, ECC Memory
- 64 bit AXI interface, no DMA
- 128 KiB ECC-protected Memory

Physically separated TCLS Cores

- 20 µm margins
- Avoids multi-bit error from a particle

Implementation Results

Clock Frequency	500 MHz
Area	0.42 mm²
Power (preliminary)	50-70 mW



Try it out on pulp-platform github!
github.com/pulp-platform/safety_island