SAFETY MECHANISMS FOR HIGHLY CONFIGURABLE RISC-V BASED AUTOMOTIVE CPU

Ravindranath Munnan, Senior Principal Hardware Architect
Dr. Varadan Savulimedu Veeravalli, Principal Functional Safety Architect
Andrew Johnston, Senior Functional Safety Manager
{Varadan.Veeravalli, Andrew.Johnston}@imgtec.com

CHALLENGES

- **Increasing compute performance** and **low latency** requirements
- Shrinking **technology nodes** → Increasingly Susceptible to transient and permanent faults
  - Compromising functionality → Need for safety mechanisms
- Need to meet stringent **safety** and **quality** requirements driven by market and customers
- **Mixed criticality** applications and centralised compute requirements to reduce overall BOM cost in Automotive product

SAFETY MANAGEMENT

- 3rd Party **Certified ISO 26262 ASIL-D** systematic development process is in place
- Safety procedures as per ISO 26262 to ensure that the architectural metrics for random hardware failures are met:
  - FMEA → Ensure all safety requirements are properly identified
  - Both transient and permanent faults are considered
  - BFR, FTA, DFA, FMEDA
- Safety analysis are conducted throughout the product life cycle → ensure all safety requirements are met

SAFETY MECHANISMS

- Safety Mechanism (SM) → Functions implemented to detect and control random hardware failures
- Distributed SMs created using hardware (or) information (or) time redundancy, e.g.:
  - FSR → Function specific replication
  - PP → Parity protection
  - E2E → End-to-end protection
  - DMR → Dual modular redundancy
  - FSMP → Finite state machine protection
  - ECC → Error correcting codes (SEC-DED)
  - WDT → Watchdog timers
  - FSS → Function specific SMs to control faults in the logic
- Depending on the targeted ASIL level the appropriate Distributed SMs are employed

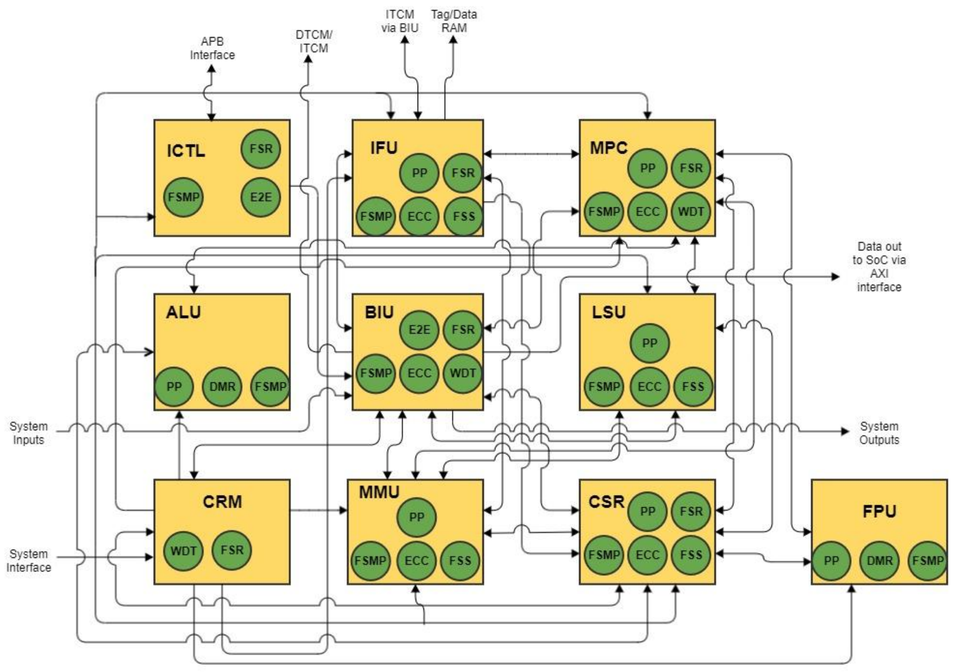

Figure 1. RISC-V CPU with distributed closely-coupled safety mechanisms

SPLIT-LOCK MICROARCH

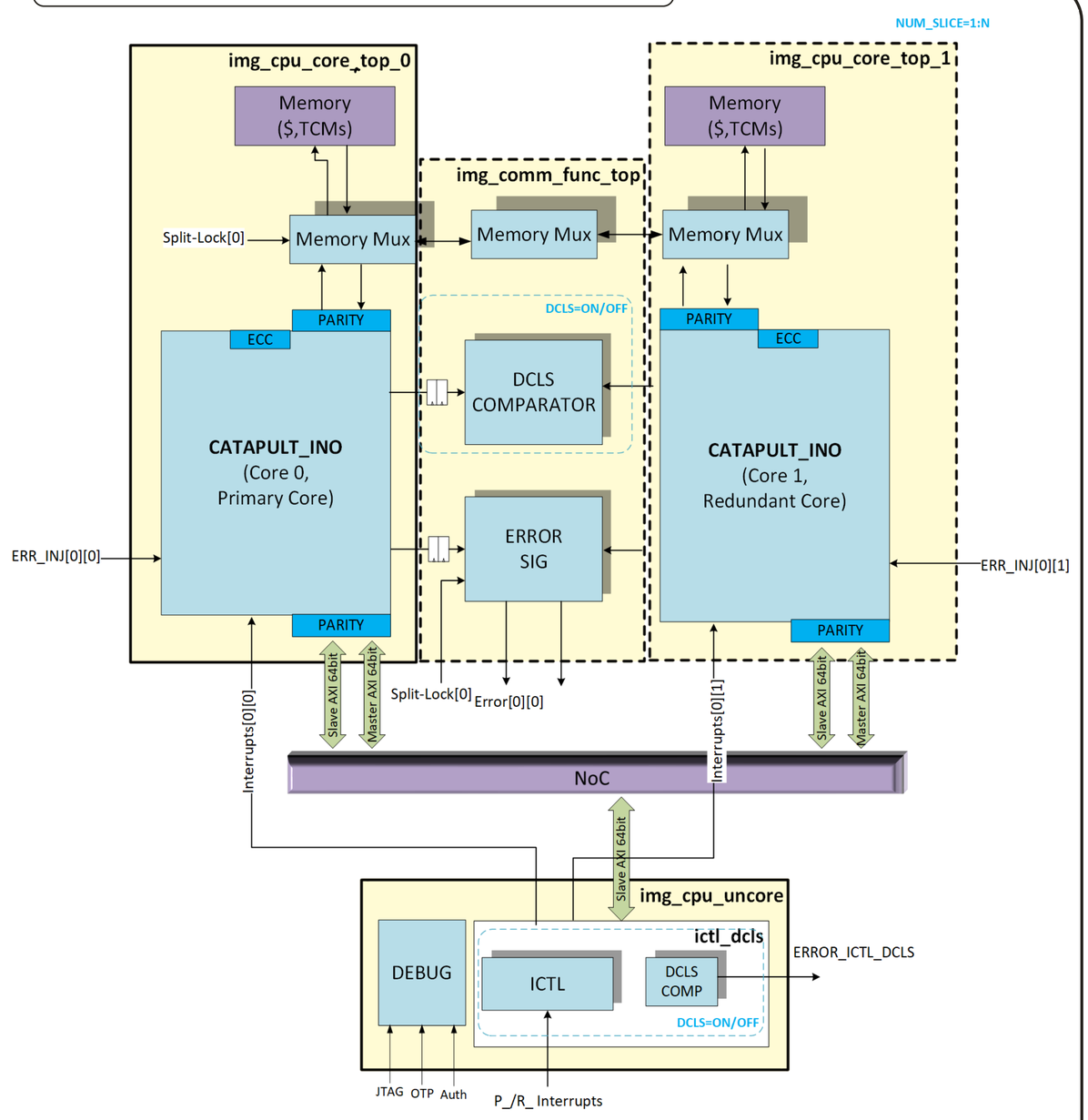

Figure 2. Dual Core CPU with Split Lock Configurability

- **Runtime configurable** Split-mode for **performance** and Lock mode for Safety critical applications
- Configurable memory sharing to trade-off between PPA and Safety needs
- **Floorplan friendly design** approach for **Multi-Core Scalability** and quick physical design convergence
- Self-checking Safety mechanisms for enhanced Latent Fault coverage
- Meets ASIL-D fault metrices (SPFM > 99%, LFM > 90%)

BENEFITS

- Based on RISCV ISAs, provides best **performance density** as compared to the competing ISAs
- **Scalable**: Suitable for Mixed Criticality Applications
- Excellent Configurability and balance between Performance and Functional Safety (ASIL-B to ASIL-D)
- Supports Multi-Core configurations
- Multi-application, embedded systems including **GPU**

CONCLUSION

- RISC-V CPU for mixed critical applications is proposed
- Safety integrity of ASIL-B achieved with **Distributed Safety Mechanism** (SPFM > 90%, LFM > 60%)
- Safety integrity of ASIL-D achieved with DCLS

FUTURE WORK

- Target other sectors: industrial, aerospace, rail, etc.
- Refine the SMs based on soft error data
- Continued analysis of the weakness of the functional architecture to random hardware failures