Power Matters.™

Microsemi

Developing Fault-Tolerant Systems using RISC-V Softcore Processors

Sathish Odiga

6th RISC-V Workshop, May 8-11, 2017

© 2017 Microsemi Corporation. Company Proprietary

Motivation

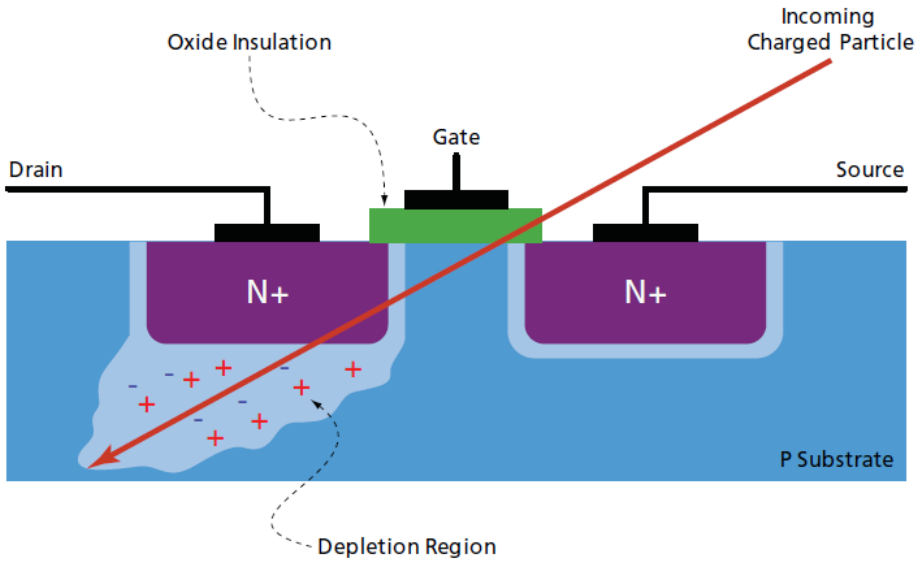
- Safety-critical systems must be designed to be fault-tolerant to provide safety, reliability and availability.
  - Unfortunately, semiconductor devices are susceptible to single-event upsets (SEUs) which makes the fault-tolerant design a challenge.

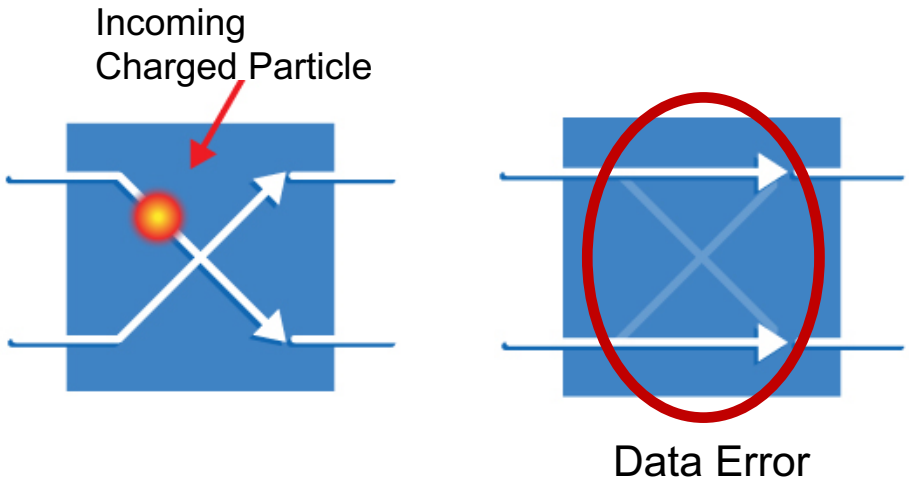
- Safety-critical systems are reaching sophisticated levels of complexity and they heavily rely on software running on embedded processors.
  - Need methodologies for fast error detection and recovery from SEUs in the embedded processor without impacting performance.

© 2017 Microsemi Corporation. Company Proprietary

Single Event Upsets (SEUs)

- SEUs are radiation-induced transient faults which alters the logic state of memory elements.
  - Rewriting the memory elements recovers the system
- Data errors in control logic due to SEUs may cause system to operate incorrectly.
- SEUs used to be a concern only for aerospace applications.
- SEUs are becoming a major concern at ground level as well.
  - Due to low core voltage, decrease in transistor geometry, and increase in switching speeds.
  - A reality in communication and automotive applications.

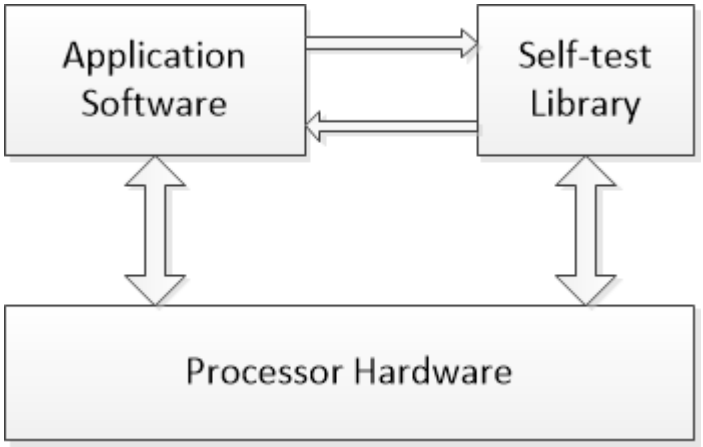




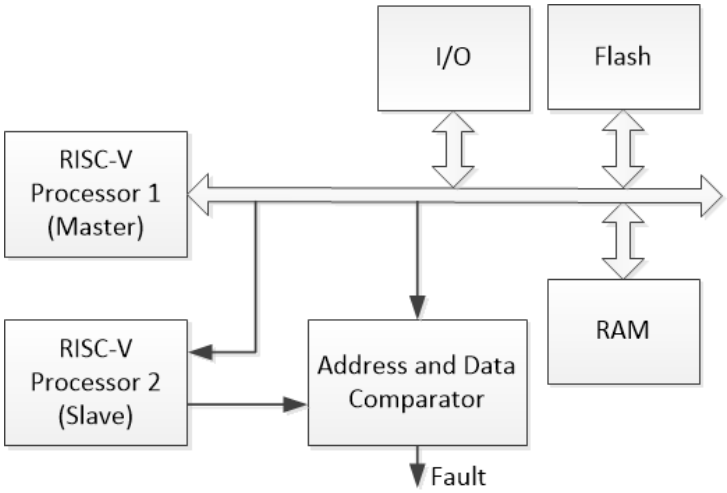
© 2017 Microsemi Corporation. Company Proprietary

Fault Detection Mechanisms

- Self-test libraries can be used to test processor functionality.
  - Processor executes STL periodically
  - Consume processor bandwidth



- Lockstep processor architecture provides real-time diagnostics using additional slave processor and comparator.
  - Two identical processors run in lockstep with address and data compared for consistency.
  - Fast error detection
  - No impact on processor performance
  - Delayed lockstep and spatial separation of cores increases reliability



© 2017 Microsemi Corporation. Company Proprietary

Fault Recovery Mechanisms

- Reset to re-execute the application
  - Long recovery delay
- Switch to safe state
  - Fail-safe operation
- Rollback through checkpointing
  - Reverts the processor state back to previous error-free state
    - Needs to save processor's context periodically, called checkpointing.
  - Saves re-execution time in the presence of faults
  - Can be implemented in software or hardware
    - Software checkpointing is not an ideal solution for real-time applications
    - Hardware checkpointing gives faster recovery and suits real-time applications

© 2017 Microsemi Corporation. Company Proprietary

RISC-V Processor Advantages

- RISC-V open source licensing provides flexibility to customize your processor for safety-critical requirements
  - Processor internal memory blocks protection using SEC-DED
  - Bus interfaces protection using error correcting codes
  - Block level hardware redundancy for error detection/correction
  - Selective hardening
  - Hardware based checkpointing and rollback
  - Logic optimization for performance
- Extensible ISA
- Portability
  - Platform independent RTL
- Security due to open source ISA
  - Deep inspection of source code builds trust

© 2017 Microsemi Corporation. Company Proprietary

Fault-Tolerant Platform

- FPGAs are attractive in safety-critical applications
  - Low development time and cost compared to ASICs
  - Flexible to implement custom hardware
- FPGA's SEU susceptibility varies by FPGA type
  - SRAM FPGAs
    - Both routing configuration and functional logic are susceptible to SEUs
  - Antifuse FPGAs
    - Routing configuration is immune to SEUs
    - SEU-hardened DFFs and Clocks
    - One-time programmable
  - Radiation-Tolerant Flash FPGAs
    - Routing configuration is immune to SEUs
    - SEU-hardened DFFs and Clock sources
    - Reprogrammable
  - Flash FPGAs
    - Routing configuration is immune to SEUs
    - Reprogrammable

© 2017 Microsemi Corporation. Company Proprietary

Fault-Tolerant Platform (Cont.)

- Antifuse FPGAs are the most common FPGAs used for safety-critical applications.
- Flash FPGAs are becoming more popular for safety-critical applications due to
  - SEU immunity
  - SEU protected block RAMs
  - Built-in self-test
  - Design separation methodology for spatial redundancy
  - Security
  - Reprogrammable
  - Non-volatile
  - Low power

Flash FPGAs are the ideal hardware platform to implement safety-critical designs

© 2017 Microsemi Corporation. Company Proprietary

Summary

- All semiconductor devices are susceptible to SEUs.
- Processors are being used in all safety-critical applications and they need to be protected from SEUs.
- Lockstep processor architecture detects/mitigates transient faults inside a processor.
- RISC-V based softcore processor is the right choice for safety-critical system design.
  - Customizable for safety and performance needs
- Flash FPGA is the ideal hardware platform for implementing fault-tolerant systems.

© 2017 Microsemi Corporation. Company Proprietary

Thank You

© 2017 Microsemi Corporation. Company Proprietary