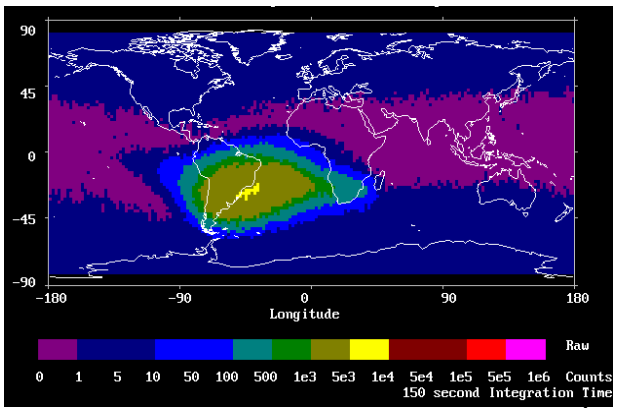
System-Level Mitigation of SEFIs in Data Handling Architectures, A Solution for Small Satellites

Mrs. Shazia Maqbool

Supervised By Dr. Craig I Underwood

Overview

- Context
- Mitigation Scheme
  - ➢Architecture - Top Level Description
  - ➢Realization - Protocol Gets Defined
  - ➢Implementation - Test Cases
- Conclusions

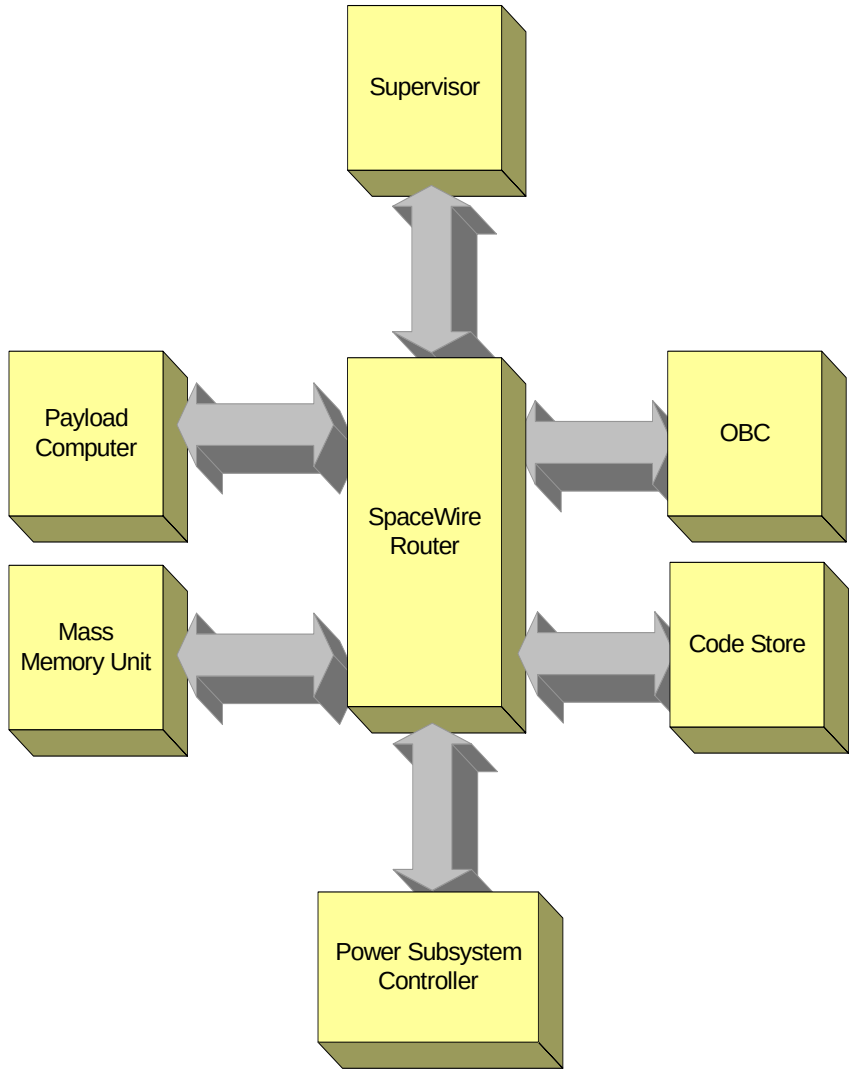


Single Event Functional Interrupts (SEFIs)

- A type of anomaly in microcircuits caused by a single ion strike
- Occurs in sensitive cross-section of the device
- User doesn't have direct access to fault location
- Signatures
  - An upset rate higher than expected
  - Non responding device
  - In a communication network SEFI is an event, which stops communication
  - Variations in device current consumption
- During a SEFI, device is unavailable to the system
- Device is potentially recoverable
  - Recovery involves resetting or power cycling
  - System recovery requires restoring the device functionality followed by its state recovery

System Architecture

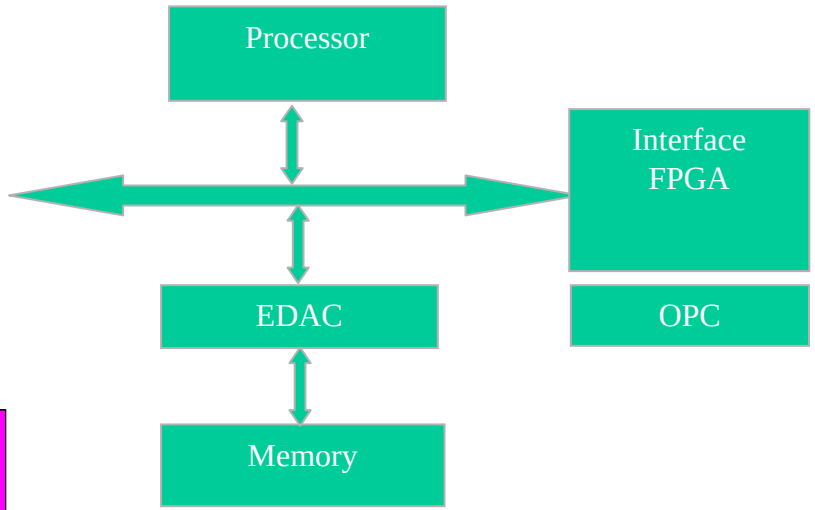
- A fast data network interlinks all units
  - Scalable
  - Distributed
  - Reusable
- A system level SEFI mitigation
- A diagnosis and recovery (DAR) packet from each unit acts as an indicator of health status for the unit
- The supervisor intervenes when a packet does not arrive or it does not match expectation



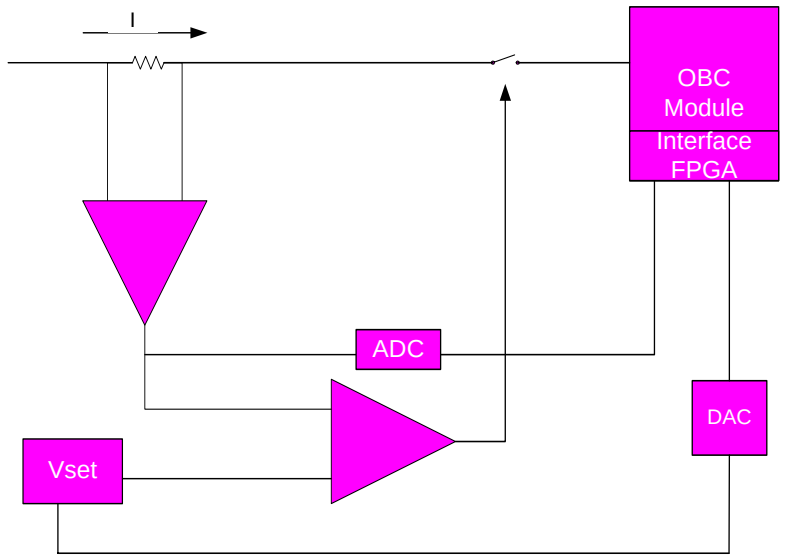
On-Board Computer

Possible source of fault

- Processor
- Memory
- Network interface



The OBC Subsystem



Over-Current Protection Circuitry (OPC)

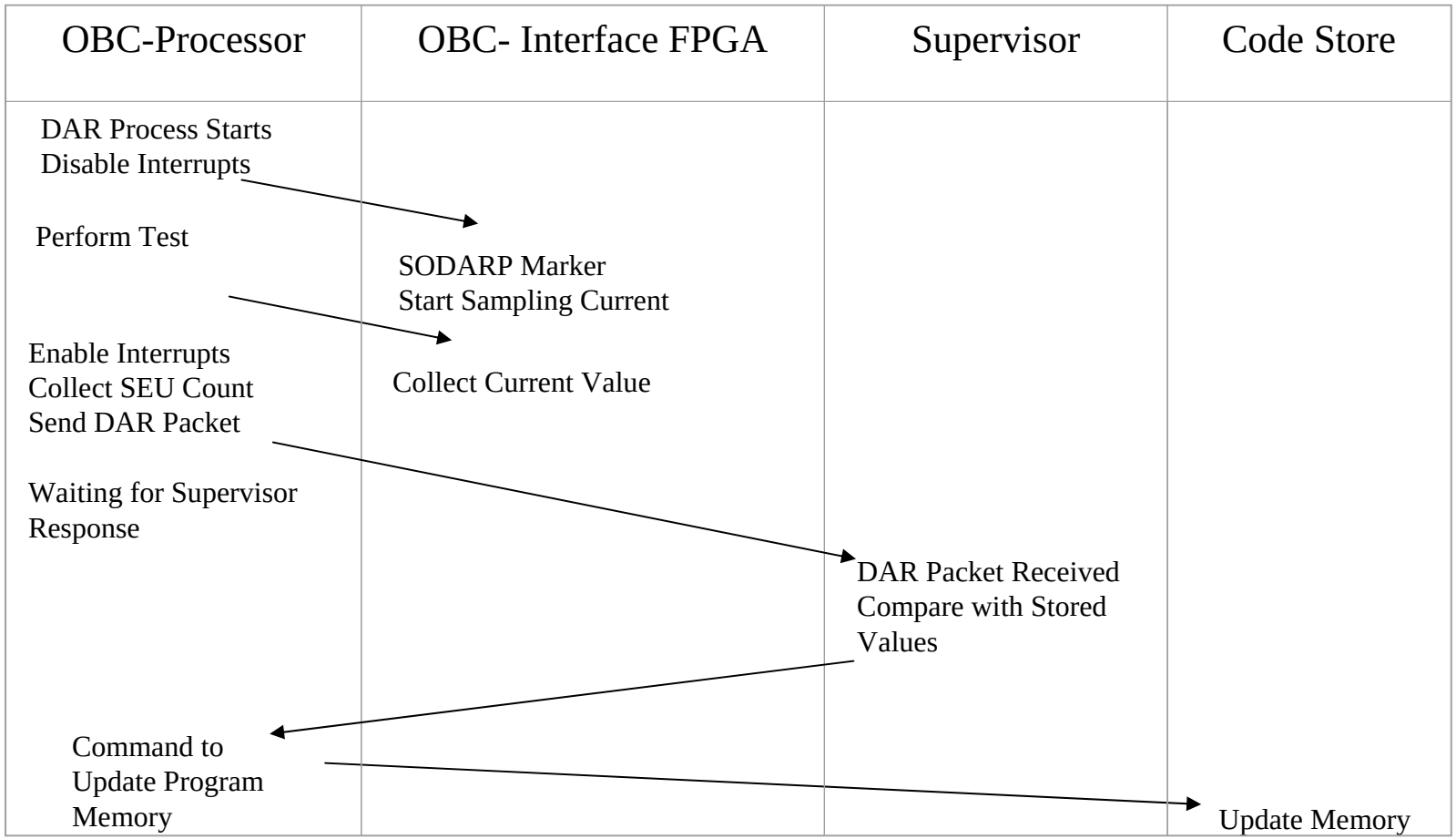
Required underlying mitigations

- EDAC
- OPC

SEFI Signatures

Device Type	Signatures
Microprocessor	Screech Non responsive Calculation errors Current Variations
Memory	Upset rate higher than expected
Network interface	Invalid packet Non responsive Link establishment time-out Transmit and receive time-out

Diagnosis And Recovery (DAR) Packet Flow



Recovery Method

Fault Type	Recovery Procedure
Screech	Reload program memory
Packet time-out (Network problems)	Detect faulty interface and apply recovery
Packet time_out (Processor Problem)	Maskable interrupt NMI, Reset
Current consumption variations	Power cycle and reload memory
SEU count exceeding threshold	Reload memory
Test task result mismatch	Reset and reload memory

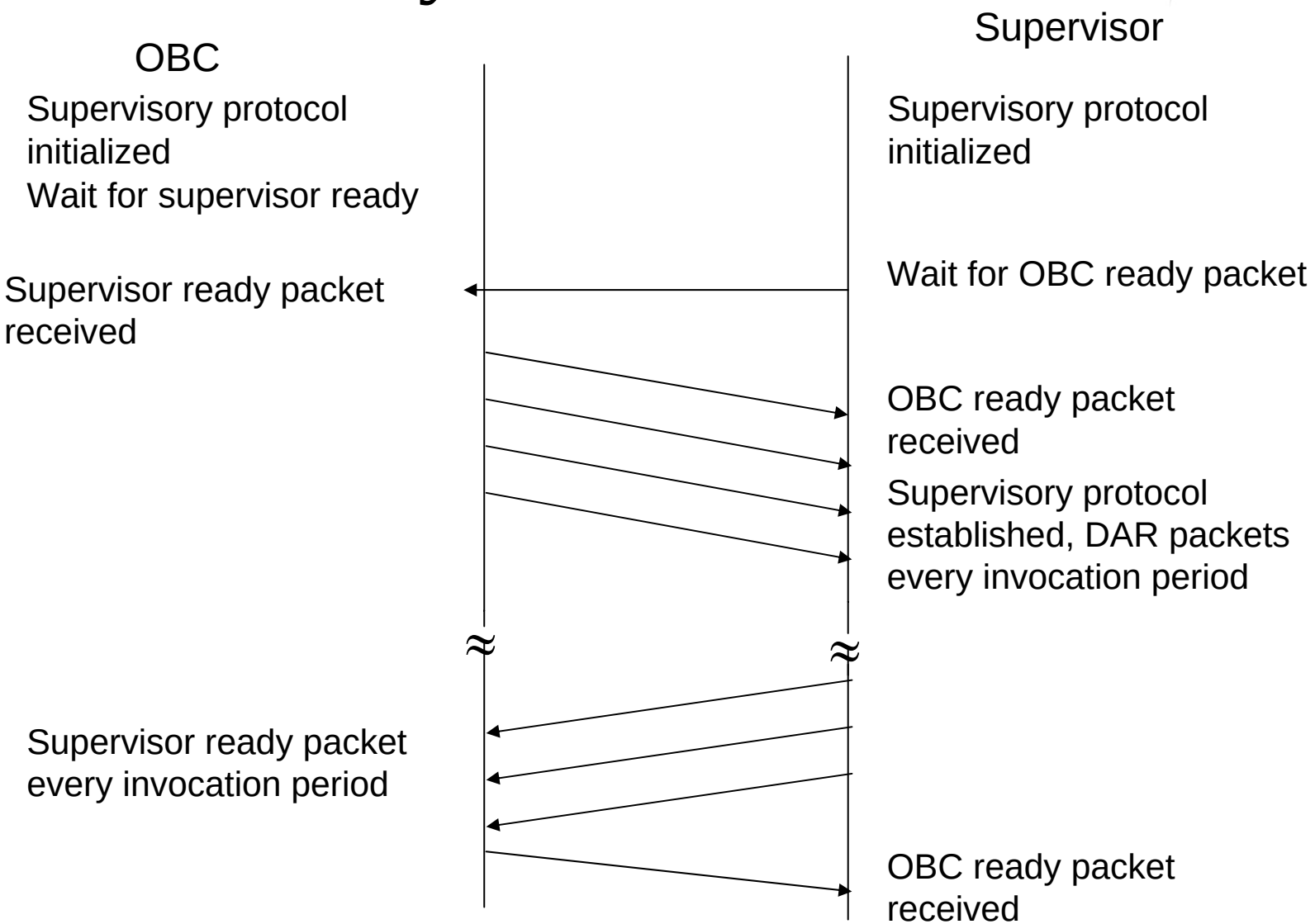
Recovery Method (2)

In case of a processor reset and power cycle, the OBC should be allowed sufficient time for reinitialization

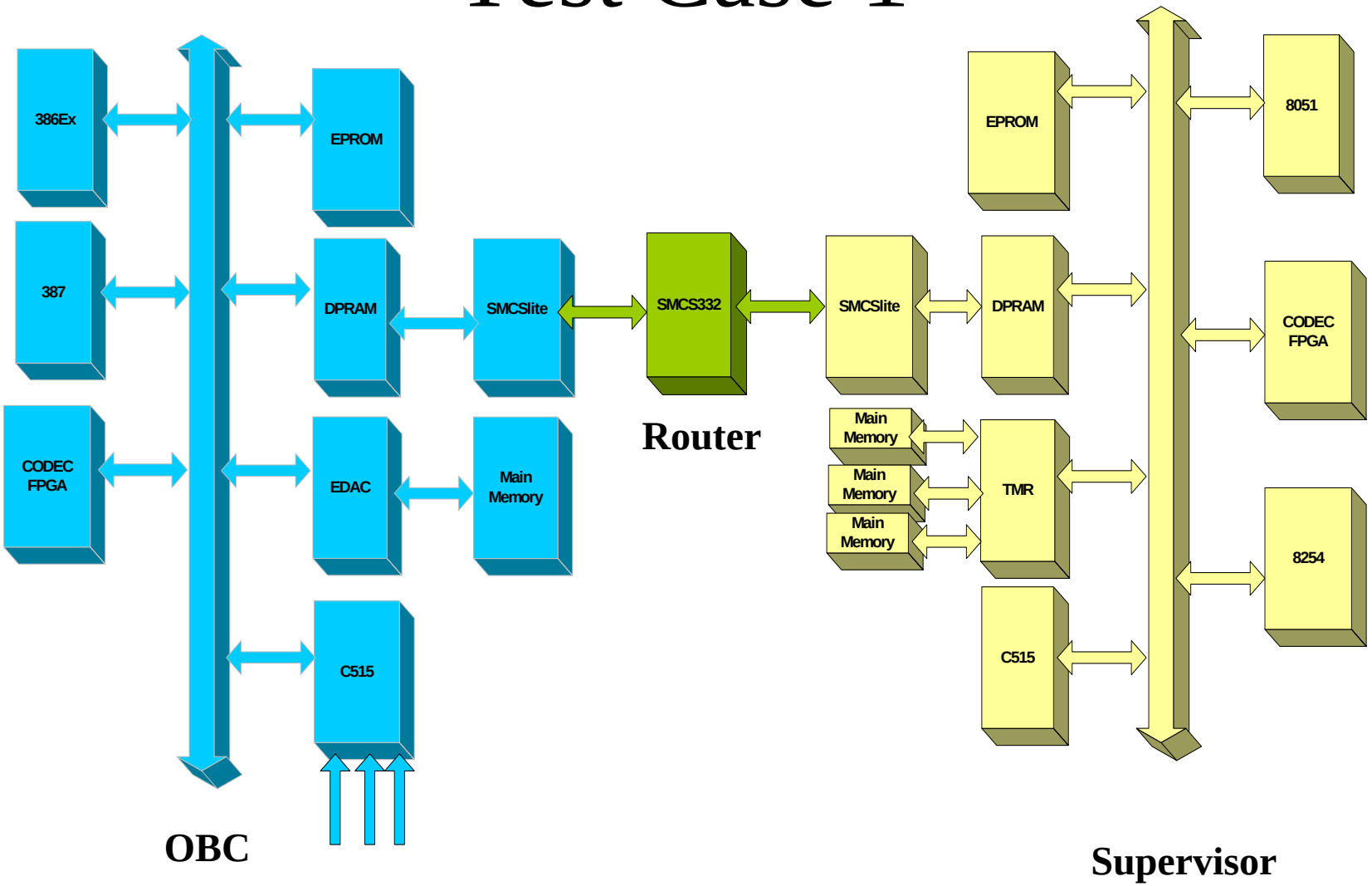
The supervisor needs to keep a record of recoveries applied

Consecutive recovery cycles needs to be avoided

Synchronization

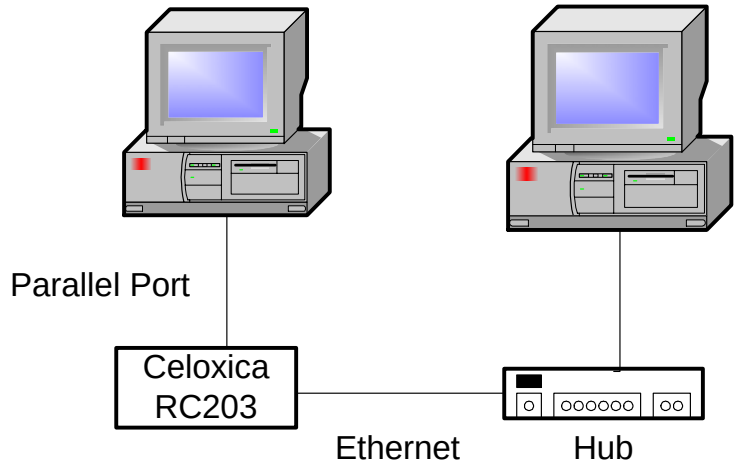


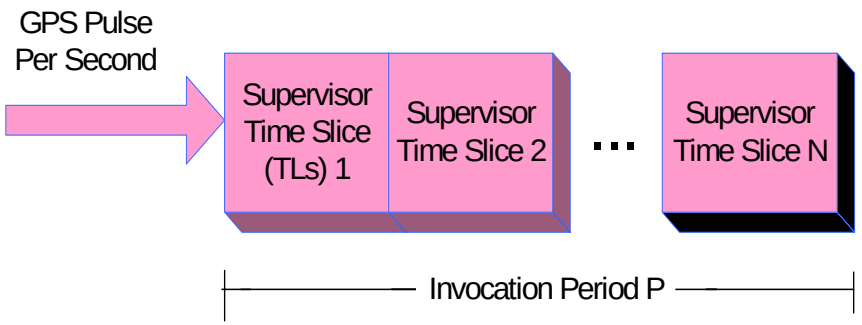
Test Case 1


386Ex
387
CODEC FPGA
EPROM
DPRAM
EDAC
C515
SMCSlite
Main Memory
OBC
SMCS332
Router
SMCSlite
DPRAM
Main Memory
Main Memory
Main Memory
TMR
C515
EPROM
8051
CODEC FPGA
8254
Supervisor
Analog Voltage

Test Cases

- Test Case1
  - Supervisor time slice
  - Invocation period
  - OBC computational overhead
  - Worst case detection and recovery latencies for each fault mode





- Test Case 2
  - Demonstration of the synchronization protocol
  - DAR packet generation and processing time
  - Time required by CODEC FPGA

Conclusions

A system-level approach has been presented to mitigate SEFIs in data handling architectures

- Upset detection is not straightforward, limits effectiveness of currently available mitigation techniques
- Increasing SEFI susceptibility in all major data handling device technologies
- A system level intelligent supervisor allows monitoring of a wide range of devices with minimal overhead
- Synchronization is straightforward
- Requires significantly low processing capabilities, requires at least two timers for interface and one timer for each underlying unit
- Two test cases are produced to evaluate the mitigation scheme performance
- Future work will require investigation into adding resource management, redundancy management and scheduling capabilities to the supervisor, thus leading to an adaptive, autonomous and highly capable data handling architecture

Thank You!