Reliable NoC in the Many Core Era

Structural fault-tolerance on the NoC circuit level

Dinesh Kumar Ravindran
Universität Stuttgart

Advisor: Dipl.-Inf. Michael Imhof
Outline

- Motivation
- Introduction to Fault Tolerance
- Fault Tolerance on NoC
- Mitigation Schemes
- Comparison & Summary
Outline

- Motivation
- Introduction to Fault Tolerance
- Fault Tolerance on NoC
- Mitigation Schemes
- Comparison & Summary
Motivation

- Technology Scaling
  - Process Variations
    - Voltage Variation
    - Temperature Variation
    - Cross talk
  - Environmental Effects
    - Alphas, neutrons
    - Electromagnetic Interferences
    - IR drop

- Increase in timing faults
- Transients
- Single Event Upsets
Motivation(2)

Increase in timing faults
  Transients
  Single Event Upsets

Reliability?

Fault Tolerant Design

Impact on Area, Performance, Power

Testing and Diagnosis
Effect of Fault on NoC

Robust Design
Outline

✓ Motivation
• Introduction to Fault Tolerance
• Fault Tolerance on NoC
• Mitigation Schemes
• Comparison & Summary
Single Events

- **Single Event Transient (SET)**
  - Caused by charged particles
  - Hits Combinational node
  - Temporary incorrect logic value (pulse/glitch)

- **Single Event Upset (SEU)**
  - Sequential element hit
  - May hit directly on the nodes of transistor
  - Inversion in the stored value
- Path is sensitizable
- Pulse is not suppressed by Inertial Delay of gates along the path
- The Transient pulse arrives at the input of sequential element during latching condition
- Masking Effects
Vulnerability Factor

- **Timing Vulnerability Factor (TVF)**
  - The fraction of time the element is susceptible to SEU.

- **Architecture Vulnerability Factor (AVF)**
  - Probability that an error in an element results in system level undetected error.
Outline

✓ Motivation
✓ Introduction to Fault Tolerance

• Fault Tolerance on NoC
• Mitigation Schemes
• Comparison & Summary
Fault Tolerance on NoC

- Sensitive Elements on NoC
  - Input Buffer of Router
  - Links Between the Router
  - Router Hardware

- Effect
  - Loss of Packet on best case - Retransmission
  - Router Crash on worst case

Router no longer operational!
Effect of Fault on Network Layers

PL: Physical Layer
DL: Datalink Layer
NL: Network Layer
TL: Transport Layer

Fault or defect
Data Corruption
Packet Corruption
Packet Loss
Simulation Results

- Simulation Results for Fault injected on Input Buffers of the Router and on the Router Links Pseudorandomly

Effect of Crosstalk

- 21% Packet-routing error
- 8% Payload error
- 5% Router Crash
- 66% No Effect

Effect of SEUs

- 6% Packet-routing error
- 12% Payload error
- 2% Router Crash
- 80% No Effect

REF: [FCK+07]
Outline

✓ Motivation
✓ Introduction to Fault Tolerance
✓ Fault Tolerance on NoC

• Mitigation Schemes
• Comparison & Summary
• Tolerates timing errors due to crosstalks and delay in the wires
• SEUs
• The length of tolerable timing error is \( \delta \)

REF: [FCK+07]
TS-HC-TMR - Delay faults

\[ \text{Clk} \]
\[ \text{Clk} + \delta \]
\[ \text{Clk} + 2\delta \]

Input data
Data 1  Data 2  Data 3

Voter Output
Data 1  Data 2

Maximize \( \delta \)!

Tolerates only delay fault upto \( \delta \)

REF: [FCK+07]
TS-HC-TMR - SEUs

- Tolerates any number of SEUs on different bit positions – as TMR is implemented at bit level
- Does not Tolerate when a same bit position is affected in two different modules
Error Detection and Correction is achieved by using:

- Redundant latch which uses delayed clock
- Comparator to generate error signal
- Mux to select input based on error signal

REF: [EKD+03]
Razor – Timing Error

REF: [EKD+03]
Razor - Soft Error

Shadow Latch is Critical Element!

REF: [EKD+03]
What is different in Razor Flipflop Design?
• No additional delay in the Data path
• Power Reduction
• Dynamic Voltage Scaling

REF: [EKD+03]
Razor - NoC Link Protections

Sender -> Pipeline Buffer 1 -> Pipeline Buffer 1 -> Pipeline Buffer 1 -> Receiver

Input: 0 → Main Flip Flop (Clk)
Output: 1

Err to XOR

Clk + δ

Razor FF

Shadow Latch
AVF results for SEU and crosstalk faults

AVF results of SEU & Crosstalk Faults

- SEU
- Crosstalk
- SEU+Crosstalk

AVF(%) for:
- Hamming Code
- Hamming Code+Razor/Terror
- Triple Sampling+Hamming Code
Outline

✓ Motivation
✓ Introduction to Fault Tolerance
✓ Fault Tolerance on NoC
✓ Mitigation Schemes

• Comparison & Summary
## Comparison

<table>
<thead>
<tr>
<th>TS-HC-TMR</th>
<th>RAZOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time and Space Redundancy</td>
<td>Time and Space Redundancy</td>
</tr>
<tr>
<td>Vulnerability (AVF): 0%</td>
<td>Vulnerability (AVF): 33%</td>
</tr>
<tr>
<td>Area: 200% +</td>
<td>Area: 50% +</td>
</tr>
<tr>
<td>Performance: Acceptable</td>
<td>Performance: Minimal impact</td>
</tr>
<tr>
<td>Power: High Penalty</td>
<td>Power: Minimum Overhead</td>
</tr>
</tbody>
</table>
Summary

- Each scheme has its own advantage and disadvantage
- Tradeoff between Power, Area, Performance, and AVF
- In State-of-art NoC design – TMR and Error Correcting Codes are widely used.
- Razor is preferred in some applications because of minimal power overhead and dynamic voltage scaling.
Outline

- Motivation
- Introduction to Fault Tolerance
- Fault Tolerance on NoC
- Mitigation Schemes
- Comparison & Summary
Thank you!

Reliable NoC in the Many Core Era
Minimum Delay of Combinational Circuit in a pipeline stage must satisfy $\text{Min. Delay} > T_{\text{delay}} + T_{\text{hold}}$

REF: [EKD+03]
SEUs on Pipelined Router

- Four Stage Pipelined Router
- Effect of SEU on Router

**Routing (RT)**

- **Virtual Allocator (VA)**
  - Stage 1: Packet in Misdirected
  - Stage 2: Input VC is assigned to invalid or reserved VC

- **Switch Allocator (SA)**
  - Stage 3: Entire flit is misdirected Loss of data

- **Cross Bar**
  - Stage 4: Single Bit Upset

REF: PNK+06
• Basic idea
  • Protect the Pipeline Registers with Razor FF
  • In case of Power overhead – protect at least the critical stages
    - Virtual Channel Allocator, Switch Allocator