Multi-Chip NoC Approach for Automotive Applications

Tomohiro Yoneda (National Institute of Informatics)
Masashi Imai (Hirosaki University)
Atsushi Matsumoto (Tohoku University)
Hiroshi Saito (University of Aizu)
Recent automobiles are equipped with many ECUs

Conventional ECU configuration

Sensors/Actuators

ECU1

ECU2

ECUi

ECUn

CAN, FlexRay, etc.
Recent automobiles are equipped with many ECUs

- Centralized ECU approach

Intelligent Sensors/Actuators

CAN, FlexRay, etc.

Interface cores

CPU cores

Centralized ECUs
Recent automobiles are equipped with many ECUs

Centralized ECU approach

Any ECU can access any sensors/actuators

ECUs efficiently used by balancing loads
Tasks continuously executed even if some ECUs become faulty
(i.e., faulty ECU does not result in malfunction of its specific functions)
Backgrounds

- **Centralized ECU approach**
  - NoC (Network-on-Chip) based
    - Scalable and flexible
    - Some European projects
  - Multi-Chip NoC based
Metrics in ISO 26262

- **Single-point fault metric**

<table>
<thead>
<tr>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 90%</td>
<td>≥ 97%</td>
<td>≥ 99%</td>
</tr>
</tbody>
</table>

- **Latent-fault metric**

<table>
<thead>
<tr>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 60%</td>
<td>≥ 80%</td>
<td>≥ 90%</td>
</tr>
</tbody>
</table>

- **Probabilistic metric for random hardware failures**

<table>
<thead>
<tr>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 10^{-7} 1/h</td>
<td>&lt; 10^{-7} 1/h</td>
<td>&lt; 10^{-8} 1/h</td>
</tr>
</tbody>
</table>
Trial to evaluate metrics

- Simple example based on our NoC approach

Safety mechanisms

- SM1: Modified Pair & Swap method
  [Imai, Yoneda DFT2011]

- SM2: Dependable Deadlock-free routing
  [Imai, Yoneda ASYNC2011]
## Single-point fault metric

<table>
<thead>
<tr>
<th>Element</th>
<th>Failure rate (fit)</th>
<th>Safety-related?</th>
<th>Failure mode</th>
<th>Distribution</th>
<th>Violate safety goal?</th>
<th>Safety mechanism</th>
<th>Diagnostic coverage</th>
<th>Residual or Single-point failure rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0〜P3</td>
<td>1000</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>○</td>
<td>SM1</td>
<td>99%</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R0〜R3</td>
<td>100</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>○</td>
<td>SM2</td>
<td>99%</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>40</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td>none</td>
<td>0%</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SM1: Modified Pair & Swap  
SM2: Dependable routing algorithm

\[
1 - \frac{20 + 2 + 20}{4000 + 400 + 40} \times 100 = 99.1\% \quad \text{(ASIL D)}
\]
## Latent fault metric

<table>
<thead>
<tr>
<th>Element</th>
<th>Failure rate (fit)</th>
<th>Safety-related?</th>
<th>Failure mode</th>
<th>Distribution</th>
<th>Violate safety goal in combination with other failures?</th>
<th>Safety mechanism</th>
<th>Diagnostic coverage</th>
<th>Latent failure rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0〜P3</td>
<td>1000</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>○</td>
<td>SM1</td>
<td>100%</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R0〜R3</td>
<td>100</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>○</td>
<td>SM2</td>
<td>100%</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>40</td>
<td>○</td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all</td>
<td>50%</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SM1: Modified Pair & Swap
SM2: Dependable routing algorithm

\[
\left\{1 - \frac{0}{4440 - 42}\right\} \times 100 = 100\% \quad (\text{ASIL D})
\]
Probabilistic metric for random hardware failures

- $\omega_{\text{all}} = \omega_{\text{core}} + \omega_{\text{network}} + \omega_{\text{ex}}$
  - $\omega_{\text{all}}$: Failure rate of the whole system
  - $\omega_{\text{core}}$: Failure rate of the cores
  - $\omega_{\text{network}}$: Failure rate of the on-chip network
  - $\omega_{\text{ex}}$: Failure rate of the external IO
Probabilistic metric for random hardware failures

\[ \omega_{\text{core}} \]

- \[ \omega_{\text{core}} = 5 \text{ (fit)} \]

When 2 cores are down, the detection mechanism does not allow to start up the system again. Note that the system can continue to work correctly, even if the second core becomes faulty during the operation.

Tolerate up to two faulty cores, \textit{i.e.}, third fault leads to non-safe state

Contribute to longer MTTF
When a router or link is down, the detection mechanism does not allow to start up the system again. Note that the network can continue to work correctly, even if a router or link becomes faulty during the operation.

ω_{network} = 0.5 (fit)

Tolerate a router or link fault, \textit{i.e.,} second fault leads to non-safe state

Contribute to longer MTTF
Probabilistic metric for random hardware failures

- $\omega_{\text{ex}} = 20$ (fit)

- $\omega_{\text{all}} = 5 + 0.5 + 20 = 25.5$ (fit)  ASIL B or C

- For ASIL D, some safety mechanism of external IO is at least needed