Design Optimization of Time- and Cost-Constrained Fault-Tolerant Distributed Embedded Systems

Viaceslav Izosimov, Paul Pop, Petru Eles, Zebo Peng
Embedded Systems Lab (ESLAB)
Linköping University, Sweden
Motivation

- Hard real-time applications
  - Timing constraints
  - Cost constraints

- Hardware solutions
  - MARS, TTA, X-by-Wire
    - Permanent faults
    - Costly for transient faults

- Online preemptive
  - Flexible

- Faults
  - Predictable
  - Transient
  - Intermittent

- Software solutions
  - Re-execution/rollback recovery
  - Checkpointing/rollback recovery
  - Replication, primary-backup...

- Off-line non-preemptive
  - Predictable
Outline

- Motivation
- System architecture and fault-model
  - Fault-tolerance techniques
- Problem formulation
  - Motivational examples
- Tabu-search optimization strategy
- Experimental results
- Contributions and Message
Fault-Tolerant Time-Triggered Systems

Time Triggered Protocol (TTP)
- Bus access scheme: time-division multiple-access (TDMA)
- Schedule table located in each TTP controller: message descriptor list (MEDL)

Messages:
Fault-tolerant protocol

Processes:
Re-execution and replication

Transients faults

Schedule table located in each TTP controller: message descriptor list (MEDL)
Fault-Tolerant Techniques

Re-execution

Replication

Re-executed replicas
Problem Formulation

- **Given**
  - **Fault model**
    - Number of transient faults in the system period
  - System architecture
  - Application
    - WCETs, message sizes, periods, deadlines

- **Determine**
  - **Schedulable** and **fault-tolerant** design implementation
    - Fault-tolerance policy assignment
    - Mapping of processes and messages
    - Schedule tables for processes and messages
Static Scheduling [Kandasamy et al. 03]

Contingency schedules

N_1: S_2
N_2: S_{12}
N_3: S_{14}

Transparent re-execution

P_1
P_2
P_2
P_3
P_4

Recovery slack

N_1
N_2
N_3

Root schedules

Contingency schedules

S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
S_9
S_{10}
S_{11}
S_{12}
S_{13}
S_{14}
S_{15}
S_{16}
S_{17}
S_{18}

2

m_1
m_2

Recovery slack
Re-execution vs. Replication

**Re-execution is better**

**Replication is better**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**Deadline**

**Missed**

**Met**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**TTP**

<table>
<thead>
<tr>
<th>S1</th>
<th>S2</th>
<th>E1</th>
<th>E2</th>
</tr>
</thead>
</table>

**Deadline**

**Missed**

**Met**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**TTP**

<table>
<thead>
<tr>
<th>S1</th>
<th>S2</th>
<th>E1</th>
<th>E2</th>
</tr>
</thead>
</table>

**Deadline**

**Missed**

**Met**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**TTP**

<table>
<thead>
<tr>
<th>S1</th>
<th>S2</th>
<th>E1</th>
<th>E2</th>
</tr>
</thead>
</table>

**Deadline**

**Missed**

**Met**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**TTP**

<table>
<thead>
<tr>
<th>S1</th>
<th>S2</th>
<th>E1</th>
<th>E2</th>
</tr>
</thead>
</table>

**Deadline**

**Missed**

**Met**

<table>
<thead>
<tr>
<th>N1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>N2</td>
<td>P1</td>
<td>P2</td>
<td>P3</td>
</tr>
</tbody>
</table>

**TTP**

<table>
<thead>
<tr>
<th>S1</th>
<th>S2</th>
<th>E1</th>
<th>E2</th>
</tr>
</thead>
</table>

**Deadline**

**Missed**

**Met**
Fault-Tolerant Policy Assignment

No fault-tolerance: application **crashes**
Fault-Tolerant Policy Assignment

No fault-tolerance: application crashes

Deadline

Missed

Deadline

No fault-tolerance: application crashes

Deadline
Fault-Tolerant Policy Assignment

No fault-tolerance: application *crashes*

Optimization of fault-tolerance policy assignment

<table>
<thead>
<tr>
<th>N₁</th>
<th>P₁</th>
<th>P₂</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>N₂</td>
<td>P₃</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTP</td>
<td>S₁</td>
<td>S₂</td>
<td>m₂</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N₁</th>
<th>P₁</th>
<th>P₂</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>N₂</td>
<td>P₃</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTP</td>
<td>S₁</td>
<td>S₂</td>
<td>m₂</td>
</tr>
</tbody>
</table>

Deadline

Optimization of fault-tolerance policy assignment

<table>
<thead>
<tr>
<th>N₁</th>
<th>N₂</th>
</tr>
</thead>
<tbody>
<tr>
<td>P₁ 40</td>
<td>50</td>
</tr>
<tr>
<td>P₂ 60</td>
<td>80</td>
</tr>
<tr>
<td>P₃ 60</td>
<td>80</td>
</tr>
<tr>
<td>P₄ 40</td>
<td>50</td>
</tr>
</tbody>
</table>
Mapping and Fault-Tolerance

Best mapping without considering fault-tolerance

Deadline

Missed

Best mapping with considering fault-tolerance
Mapping and Fault-Tolerance

Best mapping without considering fault-tolerance

Simultaneous mapping and fault-tolerance

Met
Optimization Strategy

- Design optimization:
  - Fault-tolerance policy assignment
  - Mapping of processes and messages
  - Root schedules

- Three tabu-search optimization algorithms:
  1. Mapping and Fault-Tolerance Policy assignment (\textbf{MRX})
     - Re-execution, replication or both
  2. Mapping and only Re-Execution (\textbf{MX})
  3. Mapping and only Replication (\textbf{MR})
MRX Tabu-Search Example

N₁

P₁ P₂ P₄

N₂

P₃

TTP
S₁S₂ S₂E²

Design transformations

N₁

P₂ P₄

N₂

P₁ P₃

TTP
S₁S₂ S₂E²

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Tabu move & worse than best-so-far

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
MRX Tabu-Search Example

Current solution

Tabu move & better than best-so-far
MRX Tabu-Search Example

Design transformations

Current solution

Non-tabu & worse than best-so-far
MRX Tabu-Search Example

Current solution

Non-tabu & worse than best-so-far
MRX Tabu-Search Example

Design transformations

Current solution

<table>
<thead>
<tr>
<th></th>
<th>P₁</th>
<th>P₂</th>
<th>P₃</th>
<th>P₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabu</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wait</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

N₁

P₁

N₂

P₁

TTP

S₁ S₂

N₁

P₁

P₂

S₁

S₂

N₂

P₁

P₂

P₃

P₄

m₁

m₂

m₃
Experimental Results

Schedulability improvement under resource constraints

- Mapping and replication (MR)
  - Case study
    - Vehicle cruise controller
    - MRX: schedulable fault-tolerant application with 65% overhead

- Mapping and re-execution (MX)

- Mapping and policy assignment (MRX)

Average % deviation from MRX

Number of processes
Contributions and Message

- Contributions
  - Combined re-execution and replication
  - Optimization algorithms for fault-tolerance policy assignment
  - Efficient contingency schedule generation

**Optimization** of fault-tolerance policy assignment needed for cost-effective fault tolerance