Fault Tolerant Architectures

Claudio Pinello
(pinello@eecs.berkeley.edu)

Triple Modular Redundancy

- Fairly expensive (200%+ overhead)
- Fast detection time
- Fast isolation + recovery time
- Comparator is a single point of failure
- Used in aerospace applications, good resilience to radiation

- Use voting to elect majority result and isolate at-fault CPU
Implementing fail silence: ECUs

- Fast detection + isolation, no recovery
- Use EDC if comparator is not fail-silent

FOR MORE INFO...  

More techniques for FS

- SMT compares results of redundant threads, with average overhead <100%

FOR MORE INFO...  
Steven K. Reinhardt and Shubhendu S. Mukherjeem, Transient fault detection via simultaneous multithreading, Proceedings of the 27th (ISCA), 2000
More advanced topics:
the DIVA approach

- Latency in detection + isolation
- even more for recovery, but fault tolerant

FOR MORE INFO...
Todd M. Austin, DIVA: a reliable substrate for deep submicron microarchitecture design, Proceedings of the 32nd Annual ACM/IEEE (MICRO-32), 1999

Communication protocols

- TDMA
- FTDMA
- EventTriggered
  - e.g. CAN, priority based

<table>
<thead>
<tr>
<th></th>
<th>MS0</th>
<th>MS1</th>
<th>MS2 …</th>
<th>MSn</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS0</td>
<td>MS0</td>
<td>MS1</td>
<td>MS2 ...</td>
<td>MSn</td>
</tr>
<tr>
<td>MS0</td>
<td>MS0</td>
<td>MS1</td>
<td>MS2 ...</td>
<td>MSn</td>
</tr>
<tr>
<td>MS0</td>
<td>MS0</td>
<td>MS1</td>
<td>MS2 ...</td>
<td>MSn</td>
</tr>
</tbody>
</table>

m0 idle m1 … mk
TTA/TTP

- TDMA-based
- redundant channels
- Fail silent nodes
- FT synchronized clocks
- many FT services at the network interface level
  - synch, membership, fault detections, bus guardian, etc
- Commercial solutions well established

http://www.tttech.com

FlexRay (FTDMA)

- Developed with most of the same goals as TTA/TTP, mixes Time Triggered and Event Triggered communication
- Currently it defines mostly the communication protocol and some FT services
  - synch, bus guardian, etc.
- Leaves more flexibility in the definition of the system, many error-handling decisions left to host
- It is being adopted and backed by more and more car manufacturers, strong consortium support

http://www.flexray-group.com
Choose different bus alternatives
  e.g. TTP is an integrated solution, same behavior can be approximated with 2 CAN + SW

OSEKtime OS, FTcom

• FTcom is part of OSEKtime standards
  – defines how application may request FT services to communication infrastructure
  – depending on underlying protocols, some services will be implemented in OS
• It defines a platform!
Conclusions

• Fault tolerance can be achieved in many ways
• different trade-offs between cost, reaction times, fault coverage
• there are attempts at defining platforms to simplify fault tolerant deployment