Fault Mitigation Schemes for Future Spaceflight Multicore Processors

Rafi Some, Kim P. Gostelow, John Lai, Leonard Reder, Jim Alexander, Brad Clement

Jet Propulsion Laboratory, California Institute of Technology

June 20, 2012
Goal

• Achieve fail-operational and graceful-degradation behavior in realistic flight mission scenarios, such as Mars Entry-Descent-Landing (EDL) and Primitive Body proximity operations.

• Follow a policy-based approach: reliability achieved depends upon the resources committed.
What is Multicore?

Tilera TILE64 Multicore Chip
Where is Multicore?

Maestro processor – path-to-flight
• RadHard by Design
• Floating-point
• 49 cores at 44 GOPS (RAD750 is 0.2 GOPS)

Opera Software
• VxWorks (mostly)
• OpenMP, MPI, other libraries

Development Tools
• Tile-Eclipse + other tools
Multi-core processors can offer many advantages over a single-core architecture

- Parallel processing
- Power throttling
  - This is essential to all that follows
  - Real-time software fault tolerance and recovery

But they also bring their own issues to be solved

- Unprotected data packets when routing through the network and cores
- A failed core impedes data routing to the destination core along its coordinate
Some Network Fault Mitigations

Some single-bit errors can be corrected through Hamming Codes on address and data:

Node failures can be accommodated by using a virtual network:
The Demonstration Application

TRN: Terrain-Relative Navigation for EDL

Notes:
- A box is one or more threads
- A circle is an object
- A thread has an input FIFO and an event loop

- **imu queue (iq)**
- **image buffer (ib)**
- **image processing (ip)**
- **filter**
- **map**

**Message path**
- **Function call**

- **red:** there is an image associated with this marked imu measurement

**sensors**
- camera
- imu

**40 threads/cores**

**image-request**
**image-return**

**predicted camera pose**

**used/discarded**

**feature matches**

**filter state and covariance**
Graceful Degradation

The nature of the vision processing in this application allows easy implementation.

Lost cores means loss of performance only.

Many cores dedicated to parallel processing of image data.

Supervisor recovers full processing capability.

Failed core Replacement core.

Devoted to Image Processing.
Fail-operational Fault Tolerance

Fail Operational

Applied to the filter

Fault: Voter masks error

Detect and voting

Recover TMR

Replacement core
Policy-based Computing

Supervisor
1. Initially creates the application
2. Monitors health and performs fault recovery
3. Carries out policies: power/cores/reliability

Rewire filter for TMR.

Thread must be “repeatable”, e.g., no shared memory – a function.

Policy change:
Increase resilience
Status

• Implemented
  – Hardware fault mitigations
  – TMR with voter

• Real-time, policy-based actions designed, now being implemented
References


