Fault tolerance mechanisms on SpiNNaker

May 13, 2015

Fault tolerance mechanisms

1 Introduction

2 SpiNNaker Fault tolerance info from datasheet

2.1 ARM 968 (4.3)

Fault insertion

- ARM9TDMI can be disabled.
- Software can corrupt I-RAM and D-RAM to model soft errors.

Fault detection

- Self-test routines, run at start-up and during normal operation, can detect faults.
- A chip-wide watchdog timer catches runaway software.

Fault isolation

- Defective locations in the I-RAM and D-RAM can be mapped out of use by software.
- The ARM968 unit can be disabled from the System Controller.

Reconfiguration

- Software will avoid using defective I-RAM and D-RAM locations.
- Functionality will migrate to an alternative Processor in the case of permanent faults that go beyond the failure of one or two memory locations.

2.2 Vector interrupt controller (5.5)

Fault insertion

It is fairly easy to mess up vector locations, and to fake interrupt sources.

Fault detection

A failed vector location effectively causes a jump to a random location; this would be messy!

Fault isolation

Reconfiguration

A failed vector location can be removed from service (provided there are enough vector locations available without it). Alternatively, the entire vector system could be shut down and interrupts run by software inspection of the IRQ and FIQ status registers.

2.3 Counter/timer (6.4)

Fault insertion

Disabling a counter (by clearing the E bit in its control register) will cause it to fail in its function.

Fault detection

Use the second counter/timer with a longer period to check the calibration of the first?

Fault isolation

Disable the counter/timer with the E bit in the control register; disable its interrupt output; disable the interrupt in the interrupt controller.

Reconfiguration

If one counter fails then a system that requires only one counter can use the other one.

2.4 DMA controller (7.5)

Software can introduce errors in data blocks in SDRAM which should be trapped by the CRC hardware.

Fault insertion

The CRC unit can detect errors in the data transferred by the DMA controller.

Fault detection

The DMA controller will time-out if a transaction takes too long.

Reconfiguration

The local processing subsystem is shut down and its functions migrated to another subsystem on this or another chip. It should be possible to recover all of the subsystem state and to migrate it, via the SDRAM, to a functional alternative.

2.5 Communications controller (8.7)

Fault insertion

Software can cause the Communications Controller to misbehave in several ways including inserting dodgy routing keys, source IDs, destination IDs.

Fault detection

Parity of received packet; received packet framing error; transmit buffer overrun.

Fault isolation

The Communications Controller is mission-critical to the local processing subsystem, so if it fails the subsystem should be disabled and isolated.

Reconfiguration

The local processing subsystem is shut down and its functions migrated to another subsystem on this or another chip. It should be possible t

2.6 Router (10.12)

The Communications Router has some internal fault-tolerance capacity, in particular it is possible to map out a failed multicast router entry. This is a useful mechanism as the multicast router dominates the silicon area of the Communications Router. There is also capacity to cope with external failures. Emergency routing will attempt to bypass a faulty or blocked link. In the event of a node (or larger) failure this will not be sufficient. In order to tolerate a chip failure several expedients can be employed on a local basis:

- P2P packets can be routed around the obstruction;
- MC packets with a router entry can be redirected appropriately.

In most cases, default MC packets cannot sensibly be trapped by adding table entries due to their (almost) infinite variety. To allow rerouting, these packets can be dropped to the Monitor Processor on a link-by-link basis using the diversion register. In principle they can then be routed around the obstruction as P2P payloads before being resurrected at the opposite side. Should the Monitor Processor become overwhelmed, it is also possible to use the diversion register to eliminate these packets in the Router; this prevents them blocking the Router pipeline whilst waiting for a timeout and thus delaying viable traffic.

Fault detection

- packet parity errors.
- packet time-phase errors.
- packet unroutable errors (e.g. a locally-sourced multicast packet which doesn't match any entry in the multicast router).
- wrong packet length.

Fault isolation

- a multicast router entry can be disabled if it fails - see initialisation guidance above.

Reconfiguration

- since all multicast router entries are identical the function of any entry can be relocated to a spare entry.
- if a router becomes full a global reallocation of resources can move functionality to a different router.

2.7 Inter-chip transmit and receive interfaces (11.3)

The fault inducing, detecting and resetting functions are controlled from the System Controller (see 'System Controller' on page 66). The interfaces are 'glitch hardened' to greatly reduce the probability of a link deadlock arising as a result of a glitch on one of the inter-chip wires. Such a glitch may introduce packet errors, which will be detected and handled elsewhere, but it is very unlikely to cause deadlock. It is expected that the link reset function will not be required often. Fault insertion The only programmer-accessible features implemented in these interfaces are software reset and a disable control, both accessed via the System Controller. In normal operation these interfaces provide transparent connectivity between the routing network on one chip and those on its neighbours.

Fault detection

- Monitor Processors should regularly test link functionality.
- an input controlled by the System Controller causes the interface to deadlock (by disabling it).
- the interface can be disabled to isolate the chip-to-chip link. This input from the System Control- ler is also used to create a fault.

Reconfiguration

- the link interface can be reset by the System Controller to attempt recovery from a fault.
- the link interface can be isolated and an alternative route used.

2.8 SDRAM interface (13.5)

Fault insertion

The DLL can be driven by software into pretty much any defective state.

Fault detection

The DLL delay lines can be tested for stuck-at faults and relative timing accuracy.

Fault isolation

A defective or out-or-spec delay line can be isolated.

Reconfiguration

A defective or out-or-spec delay line can be isolated and replaced by using the spare delay line.

2.9 System controller

15.5 Fault-tolerance The Ethernet interface will only be used on a small number of nodes; most nodes are insensitive to faults in its functionality as they will not attempt to use it.

2.10 System RAM (17.3)

Fault insertion

- It is straightforward to corrupt the contents of the System RAM to model a soft error – any processor can do this. It is not clear how this would be detected.

Fault detection

- The Monitor Processor may perform a System RAM test at start-up, and periodically thereafter.
- It is not clear how soft errors can be detected without some sort of parity or ECC system.

Fault isolation

- Faulty words in the System SRAM can be mapped out of use.

Reconfiguration

- For hard failure of a single bit, avoid using the word containing the failed bit.
- If the System RAM fails completely the only option is to use the SDRAM instead, which will probably result in compromised performance for the fascicle processors due to loss of SDRAM bandwidth. An option then would be to relocate some of the fascicle processors' workload to another chip.

2.11 Boot ROM (18.3)

Fault insertion

Switch the 'Boot area switch' to remove the Boot ROM from the reset location.

Fault detection

If the Boot ROM fails the boot process will also fail, which will be detected at start-up.

Fault isolation

Switching the Boot ROM out of the boot area should render it harmless.

Reconfiguration

When the Boot ROM is switched out of the boot area the System RAM is switched into the boot area. A neighbour 'nurse' chip can initialise the System RAM with the boot code and retry initialisation.

3 Methods

4 Examples