

REPORT

Handläggare, enhet / *Handled by, department*
Håkan Sivencrona, Electronics

Datum / *Date*
2003-09-09

Beteckning / *Reference*
P300881

Sida / *Page*
1 (5)

Heavy-Ion Fault Injection in TTP-C2 Implementation

Summary

This report contains the results of validation experiments performed on the TTP-C2 (AS8202) chip implementation of the TTP protocol using heavy-ion fault injection in a bus and star topology carried out at Chalmers University of Technology, Göteborg, Sweden.

The results show that the TTP-C2 chip is sensitive for heavy-ions from a Californium source but that the fault-injected node did not violate the defined fail silence property where the node should either compute and transmit a correct message or not transmit at all. Neither in the bus nor the star topology was the node detected to conduct *any* fail silence violation.

The tests consisted of 3000 experiments in bus topology setup and 4000 experiments in the star topology setup. For higher confidence in the results more tests are needed. For comparison: the prototype implementation of the TTP protocol, TTP-C1 chip, was 4-5 times more sensitive.

Commission

TTTech Computertechnik AG has, as a continuation of heavy-ion fault injections, carried out on a prototype chip implementation of the time-triggered protocol class C, hereafter called TTP, decided to fault inject the next generation of TTP chip, TTP-C2. The first tests were carried out in the European Commission funded project Fault Injection Techniques in the Time-Triggered Architecture (FIT).

The experiments were carried out at Chalmers University of Technology, Department of Computer Engineering who possess the formal permit for use of the radioactive substrate, a Californium 252 source. The tests have been done in May 2003 (bus topology experiments) and August 2003 (star topology experiments).

Test Object

Ten pieces of the TTP-C2 AS8202 chip with the lid removed. All chips were after functionality checks found to work correctly.

One evaluation rack with Power PC hosts consisting of four nodes, PN211 (TTP-C2 with MPC555) including necessary software. The test setup was initially running with a "dummy" application provided by TTTech. One special test node, PL-03, was also received.

The star system, provided by TTTech and Vienna University of Technology: A TTP-C2 evaluation (PN211) cluster with switch implemented in FPGA.

The active star coupler consisted of two TTP-C2 chips, each for one channel. The FI node was still the PL-03 with slightly different design, and other oscillators.

SP Sveriges Provnings- och Forskningsinstitut, Box 857, 501 15 BORÅS, Tfn 033-16 50 00, Fax 033-13 55 02,
E-post info@sp.se, Org.nr 556464-6874

SP Swedish National Testing and Research Institute, Box 857, SE-501 15 BORÅS, SWEDEN, Telephone + 46 33 16 50 00, Telefax + 46 33 13 55 02,
E-mail info@sp.se, Reg.No 556464-6874

Detta dokument får endast återges i sin helhet, om inte SP i förväg skriftligen godkänt annat.
This document may not be reproduced other than in full, except with the prior written approval of SP.

Performance

The heavy-ion tests have been carried out using the same methodology as was used in the FIT project.

One communication controller (TTP-C2 chip) out of four nodes in the cluster was exposed to heavy-ions from the radioactive material. The heavy-ion injections took part inside a vacuum chamber, which protected the user and maintained the established vacuum to accelerate the fault frequency, since air attenuates the speed of the heavy-ions significantly. The chip pins were extended through the bottom plate of the chamber and attached to the test node. The setup is shown in Figure 2. The Californium source has been placed above the prepared chip. Both have been placed inside a vacuum chamber, see Figure 1.

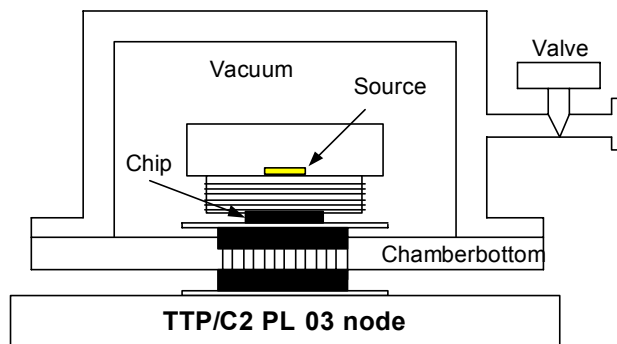


Figure 1: The fault-injected node in the TTP cluster.

The heavy-ion tests have not been carried out according to any standard procedure nor to fulfill or test the system against requirements of a particular standard.

The radioactivity of the source has not been measured, thus it has not been possible to calibrate the fault frequency, which minimizes the reproducibility of the tests. The source used is owned by the Department of Subatomic Physics at Chalmers University of Technology.

The experiments were furthermore only carried out during a limited time (approximately eight days), thus the results may change if the tests were continued for a longer time (the confidence of the results depends on the duration of the experiments).

No effort has been put on relating the carried out experiments and the resulting confidence in the results.

Furthermore, the monitoring software implemented is only designed to detect missing transmission from the fault-injected node and lost synchronization of other nodes. It is possible that this software may fail to detect discrepancies of the fault-injected system.

Fault Hypothesis

If the fault-injected node transmits data that is faulty, this data shall have such properties that the other nodes in the cluster should detect this faulty transmission and not lead to fault propagation where the system could be partitioned or reach an inconsistent state. If the fault-injected node does send such data that the things stated above happen, it is considered a fail silence violation.

Test System

The TTP cluster under test consisted of four nodes. It is pictured in Figure 2. Three nodes, not the fault-injected one, were connected to a lab PC with an RS232 connection. One node, not the fault-injected one, was designed to count the number of missed transmissions of the fault-injected node. This was triggered by the NULL-frame condition and when synchronization was lost.

The operational system used was ^{TTP}OS 3.4 for MPC555. The TDMA round during the star topology tests was 5ms, and the cluster cycle contained two TDMA rounds. The system setup is shown in Figure 2.

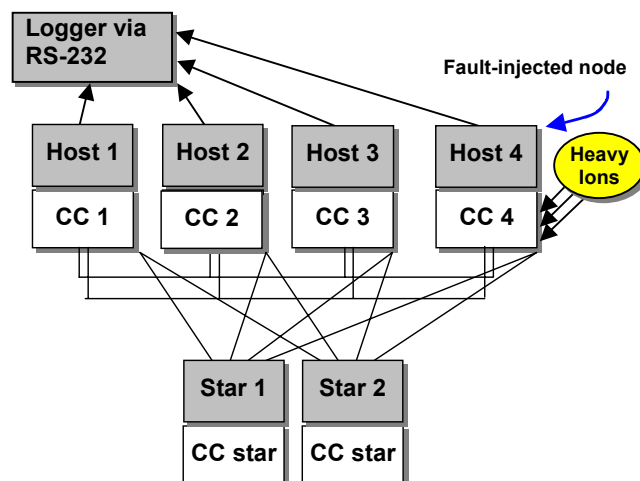


Figure 2: The two different TTP cluster setups under test, star and bus.

The monitoring software is implemented in the hosts to log information of the cluster behavior. This information, which is temporarily stored in a ring buffer, includes *controller state*, *error indication field*, arrival time of messages, and asymmetry of the signals. The ring buffer could be stored for further analysis if an error should be detected in the system. One experiment is concluded when the fault-injected node has been detected to transmit erroneously or not at all.

Results

Sensitivity

The TTP-C2 controller, test sample 1, is sensitive against heavy-ions. Latch-up-similar behavior has been observed several times, however no permanent failures have been observed. The chip seems to be robust, and persistent faults in the chip can be relaxed with a few seconds of power-off.

Fault Frequency

The FI node was observed to cease its transmission approximately one time every ten seconds when vacuum was established, as compared to one manifested error of 2-4 seconds with the TTP-C1 controller. The fault injection rate was anew increased by decreasing the pressure inside the vacuum chamber approximately once per hour. The failure rate was around 10 faults per second after the vacuum had re-established. After one hour the failure rate had decreased to approximately 100 faults per hour.

Detected Effects

Due to oscillator discrepancy on the fault-injected node, with too low precision, the tests were only possible to run until the node failed and tried to reintegrate, the reintegration could not occur automatically due to the precision of the oscillator (approximately 400 ppm). The whole cluster was thus reset after each detected FI-node failure.

In approximately one time every hour was the fault-injected node behaving as if affected by a permanent fault. However, in all these cases it was shown that a power-off of the whole node did reset the node so that it again worked. This relaxation time was around 10 seconds.

Only one chip was destroyed, and this was when the fault-injected node was not monitored.

Bus Topology

Approximately 3000 experiments were conducted in the bus topology setup. This means that the node was injected for parts of five days. No fail silence violations were detected during these experiments.

Star Topology

Approximately 4000 experiments were conducted in the star topology setup. In this case it means that the node was injected for parts of four days. No fail silence violations were observed during these days.

The result applies to the tested item only.

Conclusion

The results show that the TTP-C2 chip was sensitive for heavy-ions but that the fault-injected node did not violate the defined fail silence property described in *Fault Hypothesis*, where the node should either compute and transmit a correct message or not transmit at all. Neither in the bus nor the star topology was the node detected to conduct any fail silence violations.

The tests consisted of 3000 experiments in bus topology setup and 4000 experiments in the star topology setup. For higher confidence in the results it was concluded that more tests are needed.

Furthermore, the chip was much more robust as compared to TTP-C1 implementation, investigated in the referred FIT project. For comparison: the prototype implementation of the TTP protocol, C1 chip, was 4-5 times more sensitive.

**SP Swedish National Testing and Research Institute
Electronics-Software**

Lars Lundberg
Technical manager

Håkan Sivencrona
Technical officer