

Fault Handling in the Time-Triggered Architecture

The Time-Triggered Architecture (TTA) is a distributed computer architecture for the implementation of highly dependable real-time systems. The core building block of the TTA is the Time-Triggered Protocol (TTP), a communication protocol specifically designed for safety-critical fault-tolerant applications in the automotive and aerospace industry. A TTA system has fault tolerance implemented in both hardware and software. Whereas the hardware relies on redundant nodes and duplicated communication channels, the software uses algorithms that control such basic services as membership agreement, clique avoidance, and clock synchronization. Fault tolerance is dependent on the network topology used.

A TTA system consists of a set of TTA nodes connected by a replicated interconnection network. Each TTA node comprises a host computer, a communication network interface (CNI) and a communication controller with two bi-directional communication ports. Each of these ports is connected to an independent channel of the dual-channel interconnection network. The CNI is an interface between the application layer and protocol layer of a TTA node, with the TTP protocol running on the TTP communication controller and applications running on the host subsystem. All nodes communicate via these channels using the service of the communication controller that executes the time-triggered communication protocol TTP.

The TTP protocol implements broadcast communication that proceeds according to an a priori established time-division multiple access (TDMA) scheme. This scheme divides time into slots, each being statically assigned to a particular node. During its slots a node has exclusive write permission to the interconnection network. The slots are grouped into rounds. In the course of a round every node is granted write permission in exactly one slot. Furthermore, nodes always send in slots, having the same relative position within a round; finally, the slots assigned to a particular node have the same length in each round. A distributed fault-tolerant clock synchronization algorithm establishes the global time base needed for the distributed execution of the TDMA scheme.

A cluster cycle comprises several TDMA rounds and multiplexes the slots assigned to a node in succeeding TDMA rounds between different messages produced by the node (this is similar to the TDMA round, which multiplexes the communication channels between several nodes). Every node has knowledge – stored in read-only memory (ROM) – of the complete communication pattern (and not only of the slot assigned to itself). These data are called message descriptor list (MEDL) and allow nodes to know a priori the types of messages being sent or received. Thus, there is no need for transmitting sender IDs or message IDs explicitly.

TTP relies on a single-fault assumption and claims that a single fault in any of its constituent parts (nodes, communication channels) should not impact the operation of the system. The fault hypothesis of the protocol assumes that a TTA node is fail-silent. A fail-silent component either delivers correct service or does not deliver any service at all. If the delivered service is untimely or the value of the delivered service does not comply with the specification, a fail-silence violation in the time domain has occurred. It is the duty of the protocol to assure that no fail-silence violations in the time domain occur, i.e., the messages from one node

Fault Handling in TTA

should be transmitted within the predefined time interval. Fail-silence violations in the value domain are to be handled by such error detection mechanisms (EDM) as membership agreement and clique avoidance.

At present there are two TTA-based network topologies available. The bus topology uses a broadcast bus where all nodes are electrically connected to each other. The star topology has all nodes connected to each of the replicated channels of the interconnection network via bi-directional links. In the bus topology each node is equipped with a local bus guardian, in the star topology two redundant hubs (one for each communication channel) implement central bus guardians, whereby no bus guardians are needed at local nodes. A bus guardian is a supervising unit that acts as a failure mode converter to protect the communication channels from temporal transmission errors.

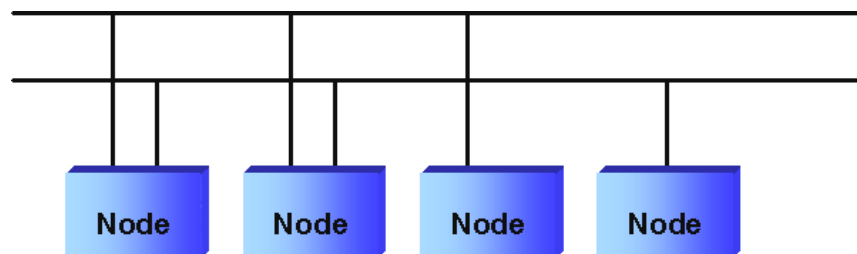


Figure 1: TTA bus topology

The EC-funded research project FIT (Fault Injection into the Time-Triggered Architecture) allowed for a large number of fault injection experiments. Their objective was to validate TTA by testing its fault handling capabilities. To begin with, a TTA cluster with the bus topology and TTP-C1 communication controllers was exposed to software-implemented fault injection (SWIFI) and heavy-ion fault injection experiments. The hardware setup consisted of four active TTA nodes with local bus guardians interconnected by redundant busses. As there was no clear physical separation of fault containment regions (FCR) between the bus guardians and the TTP protocol units, several cases of error propagation were observed. Four types of arbitrary faults could be classified: Slightly-off-specification (SOS) failures, reintegration errors, asymmetric faults, and babbling idiots. Even though error propagation occurred in the TTA system, the error detection mechanisms of TTP detected the failures and the system took recovery actions by means of restart.

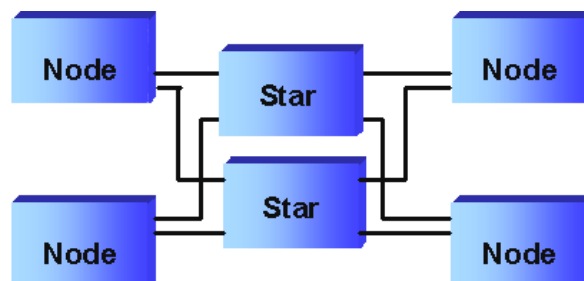


Figure 2: TTA star topology

Fault Handling in TTA

To continue with, a TTA cluster with the star topology and TTP-C1 communication controllers was subjected to software-implemented fault injection and heavy-ion fault injection experiments. Similar to the experimental setup with the bus topology, the hardware setup consisted of four regular TTA nodes and two central bus guardians. Fault isolation capabilities in the star topology were significantly better than in the bus topology because the fault containment regions were physically separated. The central bus guardians proved to be an excellent solution to the error propagation cases found in the TTA cluster with local bus guardians. Apart from a few asymmetric faults, no SOS failures, reintegration errors or babbling idiots could be observed.

That issue could only be addressed by a modification of the fault hypothesis in the TTP protocol. The protocol code was slightly modified such that in the scenario when a node is acknowledged in only one channel, it acts as if the transmission was acknowledged. This modification does not affect the basic properties of the TTP protocol. The same set of software-implemented fault injection and heavy-ion fault injection experiments was repeated in a TTA cluster whose star topology and TTP-C1 version of the communication controller were based on the modified protocol. The fact that all types of failures could be isolated by the central bus guardians justified the modification of the fault hypothesis in TTP.

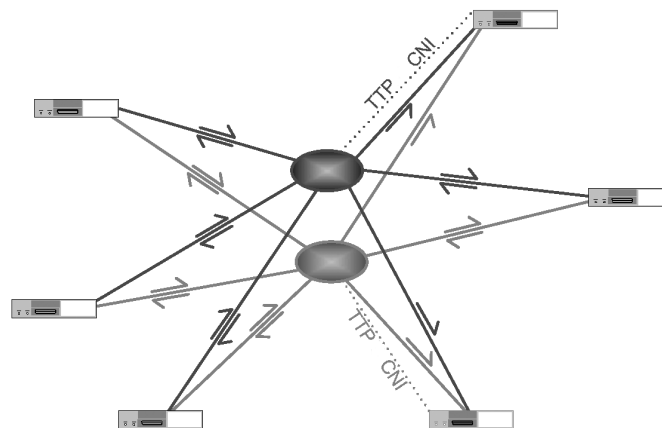


Figure 3: TTA star network architecture

The experiences gained in the fault injection experiments were exceedingly useful in evaluating and improving the fault handling capabilities of TTA. They formed the basis for the revision of the TTP protocol and the design of the TTP-C2 communication controller. The current TTP protocol – specification 1.0 was released in July 2002 – includes all the necessary changes to avoid error propagation in TTA systems with a star and bus topology. The TTP-C2 communication controller is based on a chip model specifically designed in 2001 to fulfill the fault hypothesis of the revised TTP protocol.

In 2003 the SP Swedish National Testing and Research Institute conducted heavy-ion fault injection experiments to validate TTA with TTP-C2 communication controllers. The tests were carried out in a bus and star topology using the same methodology as in the FIT project. Although the fault-injected node proved to be sensitive to heavy-ions, it did not violate the fail silence property of TTP. The TTP-C2 is far more robust than the TTP-C1, i.e., faults in the chip could be relaxed with a few seconds of power-off. According to the

Fault Handling in TTA

report of SP Swedish National Testing and Research Institute, the fact that no fail silence violations were observed with TTP-C2 communication controllers in the star and the bus topology makes TTA one of the most reliable distributed computer architectures for highly dependable real-time systems.

Cluster Topology	Communication Controller	Protocol Specification	Findings	Solutions
bus	TTP-C1	0.1	asymmetric faults, reintegration errors, SOS failures, babbling idiots	fault hypothesis in protocol specification modified
bus	TTP-C1	0.1 (modified)	asymmetric faults	central bus guardian for star topology developed
star	TTP-C1	0.1 (modified)	no arbitrary faults observed	TTP-C2 designed
bus/star	TTP-C2	1.0	no arbitrary faults observed	TTP-C2 not automotive qualified
bus/star	TTP-C2NF	1.0	no arbitrary faults observed	TTP-C2NF fully automotive qualified

Figure 4: Overview of experimental setups, findings, and solutions

References

- A. Ademaj, H. Sivencrona, G. Bauer and J. Torin: "Evaluation of Fault Handling of the Time-Triggered Architecture with Bus and Star Topology". In: IEEE International Conference on Dependable Systems and Networks (DSN 2003), San Francisco, USA, June 2003.
- H. Sivencrona, P. Johannessen and J. Torin: "Protocol Membership in Dependable Distributed Communication Systems – A Question of Brittleness". In: SAE 2003 World Congress & Exhibition, Session on In-Vehicle Networks, Detroit, MI, USA, March 2003.
- G. Bauer, H. Kopetz and W. Steiner: "The Central Guardian Approach to Enforce Fault Isolation in the Time-Triggered Architecture". In: Proceedings of the Sixth International Symposium on Autonomous Decentralized Systems (ISADS 03), April 2003.
- H. Sivencrona: "Heavy-Ion Fault Injection in TTP-C2 Implementation". Report of the SP Swedish National Testing and Research Institute, September 2003.

Fault Handling in TTA

Page 5

Contact

TTTech Computertechnik AG
Schoenbrunner Strasse 7
A-1040 Vienna, Austria
Tel.: +43 1 585 34 34-0
Fax: +43 1 585 34 34-90
E-mail: office@tttech.com
Web: www.tttech.com