Workplan for a PhD thesis within the PhD MAP-I program (2008)

To be developed in the University of Aveiro (IEETA) and in the premises of Critical Software, SA.

Supervisors:

(UA) Luís Almeida; (CSW) Rui Cordeiro

External co-supervisor:

Julian Proenza (Univ. Balearic Islands, Spain)

Title

Flexible, scalable and robust integration in large real-time safety critical systems.

Scope

Large real-time safety-critical systems such as power plants and utilities, large factories and process control plants, telecommunication switches, avionics, train control and others, are all examples of essential systems in modern economies and societies. Their construction is normally carried out as an interconnection of systems that need to be integrated properly to provide the desired service. This integration is naturally based on a network that must be flexible to allow configuration changes, preferably on-line, and scalable to allow the system to grow during its lifetime, while meeting real-time requirements and tolerating faults in the medium and in the system components, enforcing an adequate error confinement.

The main networking technology that is available today to meet these requirements is switched Ethernet [1]. Special switches support ring-topologies, the rapid spanning-tree protocol, fast isolation of faulty ports, static memory allocation to ports and or traffic classes or priority levels, beyond the usual support for VLANs, traffic prioritization, and other specific features.

Problem

However, certain types of errors, such as those associated to operation off specification in which the faulty components grab more resources than specified, are normally undetected by current networking equipment and can generate interference with the remaining system, possibly leading to resource exhaustion, either network bandwidth or queuing capacity, CPU bandwidth or memory [2] [3].

This problem can be dealt with at the application level but the application development is simplified if the integration layer enforces the component specifications directly [4]. This needs an appropriate architecture with adequate support at the communication protocol and programming middleware. Unfortunately, current solutions to provide this level of protection and robustness, such as those based on the time-triggered communications paradigm (TTE Switch [5] and PROFINET-IRT [6]), typically favor timeliness and fault-tolerance at the expense of flexibility and scalability. Other solutions being researched, such as the Flexible

Time-Triggered communication protocol over Switched Ethernet (FTT-SE) [7] and the Contract-based middleware [8] being developed in the on-going EU project FRESCOR, favor the timeliness aspect while improving flexibility but still lack adequate support for combined scalability and timeliness.

On the other hand, solutions based directly on switched Ethernet and on the services that the switches provide, such as Ethernet/IP [9], favor flexibility and scalability but lose in terms of timeliness and fault-tolerance.

Objective

The purpose of this work is to research architectures and communication protocols/middlewares based on switched Ethernet technology that facilitate building flexible and scalable systems of systems with support for tight timeliness and high level of fault-tolerance, as required for real-time safety-critical systems.

The work will take the FTT-SE protocol as a start point and improve its architecture model to achieve scalability. Two-tier architectures, will be considered, such as the one proposed for real-time sensor networks using the ZigBee protocol [10], with cells built around a synchronizer element that supports local real-time communication, interconnected by means of a second tier network that provides real-time support across cells. The architecture to be developed must, however, preserve the dynamic reconfiguration and adaptation capabilities of the FTT-SE protocol. Moreover, an adequate middleware layer must also be developed, for example, following the guidelines of the Contract-model middleware, to provide an abstract access to the required communication services while policing resource usage and enforcing components specifications.

[1] F. Dopatka and R. Wismuller, “Design of a Realtime Industrial-Ethernet Network Including Hot-Plugable Asynchronous Devices”, in ISIE’07 - The IEEE International Symposium on Industrial Electronics, June 2007, Vigo - Spain.

[2] Jork Loeser and Hermann Haertig. Low-Latency Hard Real-Time Communication over Switched Ethernet. In Proc. of the 16th Euromicro Conference on Real-Time Systems (ECRTS'04), pages 13{22, Catania, Italy, 30 July 2004. IEEE Computer Society.

[3] P. Pedreiras, R. Leite, L. Almeida. Characterizing the Real-Time Behavior of Prioritized Switched-Ethernet. RTLIA’03, 2nd Workshop on Real-Time LANs in the Internet Age, (satellite of ECRTS’03), Porto, Portugal, July 2003.

[4] J. Proenza, L. Almeida. Position Paper on Dependability and Reconfigurability in Distributed Embedded Systems. RTN’07, 6th Workshop on Real-Time Networks, (satellite of ECRTS’07), Pisa, Italy, July 2007.

[5] K. Steinhammer, P. Grillinger, A. Ademaj, and H. Kopetz, “A Time-Triggered Ethernet (TTE) Switch”, in DATE’06 - Design Automation and Test in Europe, Mar. 2006, pp. 794–799, Munich - Germany. ACM.

[6] PROFInet, “Real-Time PROFInet IRT”, http://www.profibus.com/pn, Dec. 2007.

[7] R. Marau, L. Almeida, P. Pedreiras. Enhancing Real-Time Communication over COTS Ethernet switches. WFCS 2006, IEEE 6th Workshop on Factory Communication Systems, Turin, Italy. June 2006.

[8] R. Marau, L. Almeida, P. Pedreiras, M. González-Harbour, D. Sangorrín, J. L. Medina. Integration of a flexible time-triggered network in the FRESCOR resource contracting framework. ETFA 2007, 12th IEEE International Conference on Emerging Technologies and Factory Automation. Patras, Greece, September 2007.

[9] Ethernet/IP (Industrial Protocol) specification. Available at www.odva.org.

[10] A. Koubaa, A. Cunha, M. Alves. A Time Division Beacon Scheduling Mechanism for IEEE 802.15.4/Zigbee Cluster-Tree Wireless Sensor Networks. Proc. of 19th Euromicro Conference on Real-Time Systems (ECRTS 2007), Pisa(Italy), July 2007, pp. 125-135