TIRAN: Flexible and Portable Fault Tolerance Solutions for Cost Effective Dependable Applications

O. Botti[1], V. De Florio[2], G. Deconinck[2], F. Cassinari[3], S. Donatelli[4], A. Bobbio[4], A. Klein[5], H. Kufner[5], R. Lauwereins[2], E. Thurner[5], E. Verhulst[6]

[1] ENEL S.p.A., R&D, Via Volta 1, I-20093 Cologno Monzese (Milano), Italy Tel: +39-02-7224-5553, Fax: +39-02-7224-5465, botti@pea.enel.it
[2] K.U.Leuven, Dept. Elektrotechniek, Kard. Mercierln 94, B-3001 Heverlee, Belgium
[3] TXT Ingegneria Informatica, Via Socrate 41, I-20128 Milano, Italy
[4] Università di Torino, Dip. di Informatica, C.so Svizzera 185, I-10149 Torino, Italy
[5] Siemens AG, Dept. ZT SE 2, Otto-Hahn-Ring 6, D-81730 München, Germany
[6] Eonic Systems, Nieuwlandln 9, B-3200 Aarschot, Belgium

Abstract. Available solutions for fault tolerance in embedded automation are often based on strong customisation, have impacts on the whole life-cycle, and require highly specialised design teams, thus making dependable embedded systems costly and difficult to develop and maintain. The TIRAN project[1] develops a framework which provides fault tolerance capabilities to automation systems, with the goal of allowing portable, reusable and cost-effective solutions. Application developers are allowed to select, configure and integrate in their own environment a variety of software-based functions for error detection, confinement and recovery provided by the framework.

1 Industrial Motivations and Answers to the Market Needs

Market investigations with users and producers of automation systems have recognised the benefits offered by dependable systems, not only in the classical area of safety-critical tasks, but also in mission-critical ones, due to the high economic impact of failures. Moreover, dependable embedded systems were judged costly and difficult to develop and maintain, as they generally need strong customisation, impacting on the whole life-cycle, and requiring highly specialised design teams.

New proposals for fault tolerance (FT) should be based on pre-built and easily reusable solutions, customisable for different applications and portable on commercial and proprietary real-time operating systems (RTOS). The TIRAN project addresses these urgent needs raised from the market of real-time embedded automation systems.

[1] ESPRIT Project 28620 TIRAN — "Tailorable fault tolerance frameworks for embedded applications".

P. Amestoy et al. (Eds.): Euro-Par'99, LNCS 1685, pp. 1166–1170, 1999.

TIRAN is a 24-month ESPRIT project. It provides a FT solution that will be developed on different platforms to allow an estimation of the reusability, and will be used on three different pilot applications to study its efficacy in making the applications more dependable. This paper describes the TIRAN solution and positions it with respect to the emerging standards and market trends.

The TIRAN solution is built around a software framework which provides fault tolerance capabilities to automation systems. Application developers are allowed to select, configure and integrate in their own environment a variety of software-based FT functions for fault masking, error detection, isolation and recovery, available in the framework. The framework includes techniques, tools and documentation to support the developers when combining the selected functions into their own fault tolerance strategies to obtain the required level of dependability.

The use of formal techniques to support requirement specification and predictive evaluation, together with the intensive testing on pilot applications, aims at guaranteeing the correctness of the framework, and to quantify the fulfilment of real-time, dependability and cost requirements, providing also valuable guidelines to the configuration process for the different users.

2 The Industrial Environment: Pilot Applications, Exploitation, and Market Access

The TIRAN Consortium includes large European suppliers and end-users of mission critical systems in their application fields. ENEL (the main Italian electricity supplier, the 3rd largest world-wide) and SIEMENS (the leading German company in the field of electrical engineering and electronics, one of the largest worldwide), EONIC Systems (B) (supplier of very high performance and application specific small RTOS for DSP processors and embedded ASIC cores), TXT Informatica (I) (provider of systems and services in many fields of real-time automation), the University of Leuven (B) and the University of Turin (I), particularly active on the R&D edges of fault tolerance and performance evaluation.

The project results, driven by industrial users' requirements and market demand, will be integrated with an existing off-the-shelf tool supplied by its producer (Virtuoso of Eonic Systems), will be ported onto commercial and proprietary RTOS (Windows CE, VxWorks, TEX), that will represent the basis for services offered by a system integrator (TXT), and are to be tested and adopted by two large end-user companies (ENEL, SIEMENS) within their application fields.

Pilot applications from Energy Distribution (ENEL, primary substation automation system) and Industrial Automation (SIEMENS, airfield lightcontrol system), bring a wide variety of requirements to the framework development and allow a deep validation of project results. Broad exploitation of results and market access are guaranteed in different sectors by the involved users, the tech-

nology providers and by third party association with market leaders—e.g., WindRiver.

Functional	Error processing / Fault treatment	Error detection
		Fault containment / Error isolation
		Fault masking
		Error recovery
	Monitoring	Target monitoring
		Fault injection
Non-Functional	Portability	Platform and RTOS independence
	Flexibility	Configurability and scalability
	Performance	Hard real-time
		Soft real-time

Table 1. Classification of user requirements.

3 The TIRAN Approach to Fault Tolerance

TIRAN bases its fault tolerance strategy on the concept of "framework", which translates into the conjoint use of a layered system of fault tolerance mechanisms arranged into a library and of a sort of configuration tool by means of which the user expresses a number of recovery strategies. This is combined with a formal assessment of the performance of the framework approach. Industrial requirements have been summarized in Table 1. This section briefly describes the role and structure of the FT library, the configuration tool, and the techniques for framework validation and evaluation.

The FT Library. This is the central component of the TIRAN strategy. The system is made of three "layers": a *basic layer*, with entities related to fault containment, fault masking, error detection, isolation, and recovery mechanisms, a *control layer*, constituting a sort of "backbone" component for a coherent coordination of the entities in the basic layer, and a *monitoring and fault injection layer*, introduced for debugging purposes on embedded targets and substantially given by a hypermedia distributed tool. In particular the TIRAN control layer collects all relevant information concerning the current structure and status of the user application and of the basic TIRAN tools. This layer also coordinates recovery and interprets user-defined recovery strategies. The monitor describes the structure of the system (user application plus TIRAN framework components) and reports in a hypertextual structure all the events taking place at the basic layer and at the control layer. This component is also responsible for managing software fault injection services.

Configuration. A special component of the framework is a tool which offers a secondary application level that comes into action the moment an error is detected in the system. This level executes recovery scripts, to be coded by the user in a special "Recovery Language". With that, the user can configure strategies for recovery and reconfiguration. Special support towards design diversification (e.g., by means of recovery blocks) is under consideration.

Framework Validation and Evaluation. To prove the efficacy of the proposed framework it is important to assess the performance of the generic library and

of its portings running on the different supported platforms. To reach these goals two techniques will be used in TIRAN: a probabilistic approach centred around modelling and measurements associated with fault injection.

Probabilistic modelling will be carried out using stochastic Petri nets [1]. Measurements of the system using software and physical fault injection on the pilot target environments will complement predictions providing a deep characterisation of the framework behaviour.

4 Comparison with Other Works

This section positions TIRAN with respect to other emerging fault tolerance approaches. In order to compare different approaches we selected a number of attributes, i.e., positive aspects and qualities of each approach, and assessed each approach with respect to these attributes. Doing this we can position each approach and research project into a unique spectrum (see Fig. 1). Five attributes have been selected: *efficiency* of the approach, measured by response times; *transparency*; *portability*; *cost* of adoption; *flexibility*, i.e. the effectiveness of the approach. Four orthogonal approaches have been considered (see below). Five ranking levels have been defined to measure the different approaches, ranging from low to high. The attributes and approaches constitute, in a sense, a *base* for discussing in more formal terms current fault tolerance trends.

System Approach. Embedding fault tolerance in the hardware and/or in the operating system is typically characterised by: high efficiency; high transparency; medium portability (good for the functional part of the user-application, bad portability of the features offered by the approach); no development or maintenance costs (for the customer), typically high costs for acquiring the target system with respect to general-purpose systems (ranking: low); bad flexibility. Project GUARDS [5] is partly based on this approach.

Library Approach. This approach consists in embedding a number of fault tolerance mechanisms and tools in the form of a library. The approach is characterised by: medium efficiency; medium transparency; high portability (in principle); low-to-medium development and maintenance costs; medium flexibility. An Example of this approach can be found in Project Isis.

Metaobject Protocols and Reflection. The idea of MOP's [4] is to open the implementation of an object-oriented language so that the developer can adopt and program different, custom semantics, adjusting the language to the needs of the user and to the requirements of the environment. It is characterised by medium efficiency; high transparency and full separation of functional concerns from dependability concerns; medium-to-high portability; medium development and maintenance costs; medium flexibility. An architecture including this approach is Friends [3].

The Recovery Language Approach. This approach is based on a language that constitutes a sort of secondary application layer, devoted to the execution of system-wide recovery strategies, which comes into action whenever an error is

detected by one of the basic fault tolerance elements of a FT framework or of the underlying runtime systems. This approach is characterised by: medium efficiency; medium-to-high transparency; high portability; medium development costs and low maintenance costs; medium flexibility. Figure 1 summarizes and compares the above orthogonal approaches.

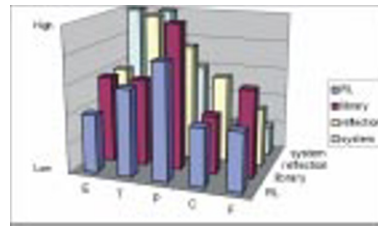

Fig. 1. A ranking of the orthogonal approaches according to five attributes.

TIRAN Positioning. TIRAN adopts a mixture of the library and of the recovery language approach for managing confinement/masking-level, detection-level and isolation-level tasks, with specific hooks to the underlying run-time system. The approach does not require object orientation and can be effectively used to add fault tolerance features to existing distributed or parallel applications.

5 Current Status and Outlook

Previous experiences within the EFTOS project [2] showed the feasibility of the TIRAN framework approach and pointed out the major required improvements. TIRAN started with a revision of the industrial requirements to allow a wide usability of results and to promote the development of an industrial product. A suitable general architecture was identified to allow the satisfaction of a wide range of performance requirements, from soft to hard real-time. Relevant novelties concern the flexibility and portability issues, the adoption of market standards, the integration of the framework within commercially available solutions supplied by their producers, as well as the adoption of formal validation techniques. The development of the FT framework has started: a concept demonstrator is available, the first framework prototype will be ready in October 1999, portings on VxWorks and Windows CE are scheduled for March 2000, while the final release of the product and its portings is planned for October 2000.

References

[1] M. Ajmone Marsan et al. *Modelling with GSPNs.* J. Wiley, NY, 1994.
[2] G. Deconinck et al. Industrial embedded HPC applications. *Supercomp.*, 69:23–44.
[3] J.-C. Fabre and T. Pérennou. FRIENDS: A flexible architecture for implementing fault tolerant and secure applications. *Proc. of EDCC-2*, Taormina, Oct. 1996.
[4] G. Kiczales et al. *The Art of the Metaobject Protocol.* MIT Press, MA, 1991.
[5] D. Powell. Preliminary definition of the GUARDS architecture. Technical Report 96277, LAAS-CNRS, January 1997.