# Safety, Reliability and Security of Industrial Computer Systems

Karama Kanoun, A Pasquini

# Safety, Reliability and Security of Industrial Computer Systems

K. Kanoun(*) and A. Pasquini(#)

(*)LAAS, 7 Avenue du Colonel Roche, 31077, Toulouse, France (kanoun@laas.fr)
(#)ENEA, Via Anguillarese 301, 00060, Roma, Italy (pasquini@casaccia.enea.it)

The papers collected in this special issue are extended versions of the best papers presented at Safecomp '99. Safecomp is a Conference organised yearly by the European Workshop on Industrial Computer Systems (EWICS), with the aim of reviewing the state of the art, experiences and new trends in the areas of computer safety, reliability and security and of the related applications. This is an area of growing interest for researchers, users and the society at large. The ubiquity and volume of embedded and networked computer systems and the global and complex nature of large-scale information and communication infrastructures require appropriate assurances about the dependability of the systems and of the services involved. Safecomp is contributing to satisfy this need since its first edition in 1979.

Because of its long tradition Safecomp offers the opportunity to observe how the research interests and the related industrial applications changed along the past years. There is now a stronger emphasis on techniques and methods for safety analysis, to ensure that the system satisfies the required dependability properties and that these properties are adequately implemented.

Several years of research and experience have also shown that safety is a property of the whole system rather than of its components. Then, the research focus is moving from an attention to the properties of the single system components to a more holistic approach considering the dependability properties of the system as a whole. Hardware, software and human co-operating in a system have to be considered together when designing, developing or evaluating a system. Only a holistic approach, that consider the system components in an integrated way, will catch the complex interactions and the strong inter-dependencies between them, and will ensure the correct interactions, the right allocation of functions and the ability to support each other and to tolerate the reciprocal typical weaknesses. These two trends are reflected by the papers selected for this special issue. Papers deal mainly with the safety analysis of systems or suggests methods and techniques for fault avoidance at the system level and for system validation.

Classical safety analysis techniques have demonstrated real value over the years especially when their results are evaluated in the framework of a plant safety case. However, there are still several problems during their application, mainly because of their complexity, and because each technique is based on different implicit assumptions. This may lead to inconsistencies when combining the results. The first two papers of this special issue address these problems. Paper [1] proposes a method for integrating design and safety analysis and for harmonising hardware safety analysis with the hazard analysis of software architectures. It also introduces an algorithm for the synthesis of Fault Trees which mechanises and simplifies the application of this technique. The applicability of the method is discussed by applying it to a prototypical distributed brake-by-wire system for cars. Paper [2] experiments #tests?? the verb experiment does not exist # a probabilistic approach in the safety analysis based on the usage of Bayesian Networks. This approach can provide some of the classical parameters usually obtained using Fault Tree Analysis, such as reliability of the Top Event or of any sub-system or the criticality of the components. Using Bayesian Networks several restrictive assumptions implicit in the Fault Tree methodology can be removed and various kinds of dependencies among components can be accommodated. The approach is applied for the analysis of a redundant multiprocessor system proposed in the literature.

Paper [3] presents a more specific verification activity: the approach used to verify the fault tolerance ability of a generic architecture developed for embedded safety critical systems. The approach is based on model checking techniques. The properties that guarantee the desired behaviour of the architecture components are specified as temporal logic formulae. A model checker is then used to verify that the behaviour of the components satisfies such properties even in presence of faults.

Safety analysis techniques such as the one proposed in [2], and sometimes even more localised activities such as the formal verification proposed in [3], can contribute to the preparation of a safety case that will be based on the estimated operational behaviour of the system. But, the real operational experience of the system will affect the validity of the safety case by providing new, up-dated and more correct information about the system behaviour. Changing regulatory requirements and modifications in the plant design may also affect the validity of the safety case. Paper [4] presents a process, supported by a tool, for an on going safety case evaluation and maintenance.

Paper [5] reports the approach used for the safety design of a control system for an anthropomorphic robotic manipulator to be used in the International Space Station. The control system is based on several subsystems produced by a Consortium of companies located in many countries. The paper describes the top-down analysis and specification process used to down flow the safety analysis to the subsystem level.

Use of statecharts represents a very appealing approach for preventing faults through good design practices, especially when temporal properties are not a critical issue. Statecharts are relatively simple if compared when compared to other formal specification techniques and are well understood by system experts and designers. But, their non-determinism may inhibit a formal verification of the system design. Paper [6] suggests an approach for overcoming this non-determinism by enforcing priorities. The approach is implemented in a tool and the paper describes its application for the specification and verification in a simple example.

Learning from our failures is the standard engineering approach for improving the dependability of systems (and not just computer systems). Standards and codes of practice reflect lessons learned from previous accidents. Nevertheless this learning process is not yet adequately systematised. There are no established techniques that help to insure that the design of new systems will take into account the accident reports concerning failures experienced with similar systems. Paper [7] shows a number of relatively simple graphical notations that can be used to improve the next generation of accident reports.

Increasingly computers support humans in carrying out functions requiring either prompt answers or the solution of complex problems, or decisions based on a large amount of information. The resulting system exhibits a tight integration of software and human resources. While automation was originally expected to decrease the risk arising from operator error, it does not remove people from the systems, automation merely increases the responsibilities of designers, and moves operators to higher level supervisory control and decision making. In addition, there has been growing recognition of the fact that moving humans to supervisory and emergency-response tasks brings new, previously underestimated risks. Errors in human decisions and actions still have the potential for extremely serious consequences. Paper [8] analyses the role of mutual awareness in supporting human cooperation and interactions, improving dependability, in air traffic control application.

These papers have been selected with a two steps process. A pre-selection was done by the International Program Committee among the 76 submissions for the Conference. Then, during the Conference, the Program Committee made the final selection by verifying the quality of the work reported by the papers through the presentations and the answers provided by the authors to the audience. The papers have then been reviewed and extended for the publication in this special issue. This long process would have not been possible without the help and support of many individuals. We would like to thank the authors for submitting excellent papers and for their patient revision work, the International Program Committee of Safecomp for the revision and selection of the papers, the Editor-in-Chief of the Journal who helped us with numerous questions we had along the way.

Karama Kanoun
General Chair of Safecomp ‘99

Alberto Pasquini
Program Chair of Safecomp ‘99

Papers included in the special issue:

[1] Y. Papadopoulos, J. A. McDermid, R. Sasse, G. Heiner, "Analysis and Synthesis of the Behaviour of Complex Programmable Electronic Systems in Conditions of Failure"
[2] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla, "Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks"
[3] C. Bernardeschi, A. Fantechi, S. Gnesi, "Formal Validation of Fault Tolerance Mechanisms inside GUARDS"
[4] T. P. Kelly, J. A. Mc Dermid, "A Systematic Approach to Safety Case Maintenance"
[5] P.G. Berthuizen, W. Kruidhof, "System and Software Safety Analysis for the ERA Control Computer"
[6] A.K. Bhattacharjee, S.D. Dhodapkar, S. Seshia, R.K. Shyamasundar, "PERTS: An Environment for the Specification and Verification of Reactive Systems"
[7] C. Johnson, "A Case Study in the Integration of Accident Reports and Constructive Design Documents"
[8] L. Rognin, J.P. Blanquart, "Human Communication, Mutual Awareness and System Dependability. Lessons learnt from Air Traffic Control field studies"