Proceedings of the 11th International Conference on Quality and Dependability
Sinaia, Romania, September 24th-26th, 2008
ISSN 1842-3566
Pages 128-136

An Interdisciplinary Research Project in the Field of Dependability of Socio-Technical Resilient Systems

Ioan BACIVAROV, Angelica BACIVAROV
Laboratorul EUROQUALROM, Universitatea "Politehnica" din Bucureşti, România
bacivaro@euroqual.pub.ro, angelica@euroqual.pub.ro

Abstract
The interdisciplinary researches developed in the frame of the project SOREZ - "Socio-technical systems resilient to errors / faults" have as purpose to improve the dependability - and especially of its main components- reliability and safety/security - of socio-technical systems, mainly through the use of errors/fault tolerance. For high functional importance systems (especially the electronic/information, nuclear, aeronautic and military ones) the failures may have important social-economic consequences. That's why, for these systems must adopted, beginning with the design stage, structures/strategies to avoid dangerous states. The thematic area of the theme of this grant is an important research domain, at both national and international level, as results from the papers of important recent scientific journals and international conferences in the field. A study of Defense Communication Agency (DCA) from USA, as well as a recent report of the European Research Program DPCS (coordinated by LAAS, France, one of the main European research centers in dependability) mentioned the importance of the researches in dependability field (considered in the synergy of its components: reliability, maintainability, safety/security a.o.) for high functional importance systems; these studies mention as a priority development of research programs concerning the problematic of dependability of socio-technical systems. An important research direction having as goal the reliability growth for high functional importance systems is the use of fault tolerance, an architectural attribute of a system which makes possible its operation, even in the presence of one or several faults in its structure. Certainly, in the context of critical socio-technical systems it is necessary to extend the researches to the error tolerant systems. At the same time, the studies mention that the approaches based exclusively on the technical aspects could be un-efficient in the case of the high functional importance systems, for which the human component could play an important role in the assurance of dependability/ security. That's why, a peculiar attention is given in the international researches to the human factor in complex systems. DHE (Designing for Human Error) became during the last period a large used method for the designers of high functional importance systems critical from the point of view of security or missions. From here the greater importance given in the last years to the studies related to human factors/errors, as suggested from the name of several European research networks mentioned bellow. At the European level a peculiar attention was given during the last years to the problem of dependability, especially for high functional importance systems, and in this context to the researches concerning fault tolerance techniques (the majority of these researches being effectuated in universities, or having universities as partners). Among the research projects / networks developed during the last years in this field, we could mention the following ones: TRUST – Testing and Consequent Reliability Estimation for Real-Time Embedded Software CONCORDIA – Integrated Environment for Reliable Systems JESSI-AC6 – Test Generation and Design for Testability Support PDCS – Predictably Dependable Computing Systems

Proceedings of the 11th International Conference on Quality and Dependability
Sinaia, Romania, September 24th-26th, 2008
ISSN 1842-3566
Pages 128-136

DARTS – Demonstration of Advanced Reliability Techniques for Safety-Related Computer Systems SCOPE – Software Certification on Programs in Europe PATRICIA – Proving and Testability for Reliability Improvement of Complex Integrated Architectures EMPA - Nano Reliability Network MONET- Network of Excellence in Model-Based and Qualitative Reasoning Systems AMETMAS-NOE – Network of Excellence in Advanced Methodologies and Tools of Manufacturing Systems. Terms as "dependability", "security" and "resilience" are among the key words for many research fields from FP5 and FP6, as well as under the new program FP7. At the same time, they are among the priority terms/thematics from national research programs done under the aegis of CNCSIS (risk management, dependability and security growth a.o.). We could mention the following PC6 research projects in the field: ReSIST - Resilience for Survivability in IST DESEREC - Dependability and Security by Enhanced Reconfigurability HIDENETS – Scenarios and Resilience Solutions ESFORS - European Security Forum for Web Services SERENITY - System Engineering for Security and Dependability HIDENETS - HIghly DEpendable ip-based NETworks and Services DESEREC - Dependability and Security by En-hanced Reconfigurability WS-Diamond - Web Services - DIAgnosability, Monitoring and Diagnosis CI2RCO - Critical Information Infrastructure Re-search Co-ordination Project IRRIIS - Integrated Risk Reduction of Information-based Infrastructure Systems SEINIT - Security Expert Initiative POSITIF - Policy-based Security Tools and Frame-work The interdisciplinary researches developed in the frame of this grant are in connection with three important research fields: high functional importance systems dependability, fault tolerance and human reliability/safety. The term of dependability is complex notion which includes the topics such as reliability, availability, confidentiality, safety and security. The most important technique for reliability growth is fault tolerance technique which will be used in the frame of this grant. At the same time another important research direction is human reliability/security, the human factor playing an important role in the case of majority complex, high functional importance systems. The implementation of high functional importance systems is very important in Europe, as well as in other developed countries, including USA and Japan; the results of these researches is the object of specialized conferences (as IFIP Working Conferences on Dependable Computing for Critical Applications (DCCA) or IEEE/IFIP International Conference on Dependable Systems and Networks, of the special issue of important journals (for example, Reliability Engineering& System Safety) and of specialized European research networks. The research related to fault tolerance were developed as a special research field during the last 30 years, related to the implementation of computer systems and of other systems of high functional importance systems (see, for example IEEE Transactions on Computers, IEEE Transactions on Reliability and Proceedings International Symposium on Fault-Tolerant Computers etc). The aspect related to dependable systems could be analyzed in two complimentary modes: system fault avoidance and fault tolerance, respectively. System fault avoidance could be used from the design phase by using reliable components and derating of systems components. But the complexity of the components/systems and the wear-out of components could limitate the use of this technique. Fault tolerance of a system is an architectural attribute that make possible the system operation, even in the system structure occur one or more failures. Fault tolerance is realized through a supplement of hardware/software resources of the system, through failure masking, or through the failure masking and system reconfiguration. It is important to mention that, generally, until now the researches concerning the fault tolerance considered mainly the technical components of the systems and no the human components. The researches regarding human factors intensified during the last two decades, based on the statistics that demonstrate the human failure are responsible for 25…40% of the failures of complex systems. The researches regarding human component, are mainly oriented to the high functional importance systems from military, but also civil field, and their results are the object of several international conferences (for example IEEE Symposium on Human Factors), or of special issues of prestigious journals from IEEE series. A special attention is given to the methods for human reliability/safety analysis, having as objective the identification of the criticality of human actions, determination of the corresponding probabilities,

minimization of the dependence among human actions etc Another important research direction in the field takes into consideration the human errors. The human error may be defined as an action which exceeds the acceptance limits. Some researches take into consideration development of interfaces between systems which limit the error risk. It is important for these interfaces to be adapted to the characteristics and limits of human operators. It is important to take into consideration and to model the complex interactions of all the involved factors (human, technical and ambiental ones). It is important to mention in this case the limits of some models based on the usual black-box concept. As demonstrated recent researches in the field, it is important to consider the non-deterministic character of human activity. The second step of our activities will take into consideration the structuring of the global system and the optimization of tasks for each sub-system. The researches to be done in the frame of this grant will take in consideration a quantitative evaluation related to human error/reliability as well as a deep study of the interaction technical-human in the dependability evaluation of high functional importance socio-technical systems. To conclude, the interdisciplinary researches which will be developed in the frame of this grant have as main objective the improvement of the dependability of socio-technical systems, which have a technical component, as well as a human one. The main points of these researches will be both human component, and on the global dependability evaluation of socio-technical high functional importance systems. These techniques are important and actual in the context of the researches in this field done at both international and national level. The research team includes specialists from each of the research domains and has as aim to bring theoretical and practical contributions concerning the dependability of socio-technical high functional importance systems. Among the objectives of this grant we could mention the following ones: - Development of the concept of socio-technical high functional importance system (STHFIS); - Quantification and modeling of the human component dependability in socio-technical systems (STS); - Development of new methods and models for human error analysis; - Development of a method for safety assurance and risk avoidance in STHFIS; - Proposal of strategies for fault/error tolerance in STHFIS; - Modeling of dependability performance for socio-technical systems with fault/error structure using specific indices; - Development of global models for dependability analysis/implementation in STHFIS with distributed structure, based on dynamic modeling of man-machine interactions and modeling of technical solidarity. These interdisciplinary researches will contribute at the development of new concepts from technical and human dependability and of an integrator vision in this important research field. Through this research, new approaches in reliability theory will be developed.

References:

[BSA1] xxx IEEE Transactions on Reliability, 1996-2006.
[BSA2] xxx IEEE Transactions on System, Man and Cybernetics, 1998-2005.
[BSA3] xxx ACM Transactions on Computer-Human Interactions, 1998-2004.
[BSA4] St. Philippi, Analysis of fault tolerance and reliability în distributed real-time system architectures, Reliability Engineering and System Safety 82 (2003) 195–206.
[BSA5] A. Mosleha, a.o. Model-based human reliability analysis, Reliability Engineering and System Safety 83 (2004) 241–253.
[BSA6] A. Crystal, B. Ellington, Task analysis and human-computer interaction, Proceedings of the 10th Americas Conference on Information Systems, New York, August 2004.
[BSA7] E. Naquina, Human reactions to technological failure, Organizational Behavior&Human Decision,, 93 (2004) 129.
[BSA8] C. Karat, C. Brodie (Eds), Special issue on HCI Research, Int. J. Human-Computer Studies 61 (2004) 565.
[BSA9] E. Fadiera, a.o. Safe design and human activity, Safety Science 41 (2003) 759–789.

Proceedings of the 11th International Conference on Quality and Dependability
Sinaia, Romania, September 24th-26th, 2008
ISSN 1842-3566
Pages 128-136
[BSA10] D. Wooa, Sociotechnical systems, risk management, Reliability Engineering System Safety 80 (2003) 253–269.
[BSA11] Special issue: Human reliability analysis, Reliability Engineering and System Safety 83 (2004).
[BSA12] xxx European perspectives on human resource management, Human Resource Management Review 14 (2004) 365–382.
[BSA13] J. W. Kim, a.o., A systematic approach to analysing errors of commission from diagnosis failure în accident progression, Reliability Engineering and System Safety 89 (2005) 137–150.
[BSA14] K. T. Kosmowski, Risk analysis în sociotechnical systems, SafetyNet Symposium, Athens, Greece, June 7-10, 2000.
[BSA15] M. Cheol Kim, a.o., A computational method for probabilistic safety assessment of I&C systems and human operators în nuclear power plants, Reliability Engineering and System Safety 88 (2005) 1–14.
[BSA16] P. Cacciabue, Human error risk management, Reliability Enng System Safety 83 (2004) 229–240.
[BSA17] Rasmussen J., Human error. Describing human malfunction, Journal Occupational Accidents. Nr. 4, 1992.
[BSA18] B. John, The GOMS Family -Analysis Techniques, ACM Trans Computer-Human Interactions, 6, 2000, 320-332.
[BSA19] S. D. Wood, D. E. Kieras, Modeling Human Error, http://www.soartech.com/pubs/IITSEC2002- SW.pdf.
[BSD1] Rasmussen J., Duncan K., Leplat J., New technology and human error, John Wiley and Sons London, 1997.
[BSD2] Leplat J. et Terssac G., Les facteurs humains de la fiabilite dans les systemes complexes, Ed. Octares, 2001.
[BSD3] G. Apostolakis, a.o., Methods for safety and reliability methods for safety and reliability, Plenum, New York, 2000.
[BSD4] xxx Classification of human reliability data for use în Probabilistic Safety Assessment, IAEATECDOC-1048, 2004.
[BSD5] xxx Proceedings of IEEE Annual Symposium Reliability, Maintainability, Security, 1992-2005.
[BSD6] xxx Proceedings of IEEE Symposium on Fault Tolerant Computers, 1990-2004.
[BSD7] xxx Proceedings of European Safety & Reliability Conference ESREL, 1996-2005.
[BSD8] I. Bacivarov, Fiabilitatea sistemelor de telecomunicaţii, Ed. Militară, Bucureşti, 1995.
[BSD9] D. Stoichitoiu, I. Bacivarov, A. Kobi (eds), Quality and Dependability, Proceedings of the 10th IEEE - CCF Conference, 2006.
[BSD10] C. Gacek, a.o., Architecting Dependable Systems III, Vol. 3549 of LNCS, Springer, 2005.