INCOSE Italian Chapter Conference on Systems Engineering (CIISE2014)
Rome, Italy, November 24 – 25, 2014

System Dependability Analysis: Main Issues and Possible Solutions

Alfredo Garro
Department of Informatics, Modeling, Electronics, and Systems Engineering (DIMES), University of Calabria
Via P. Bucci 41C, 87036, Rende (CS), Italy
alfredo.garro@unical.it

Abstract. In several application domains ranging from automotive to aerospace (Garro, Groß, Riestenpatt Gen. Richter and Tundis, 2013; Falcone, Garro and Tundis, 2014; Garro, Groß, Riestenpatt Gen. Richter and Tundis, 2012; Garro and Tundis, 2012b; Garro and Tundis, 2012c; Garro, Tundis and Chirillo, 2011), a great variety of systems are currently designed and developed by organizing and integrating existing and heterogeneous components. This design approach potentially offers many advantages in terms of time and cost reductions as promote the reusability of existing components and enable a natural parallel work organization in the system realization (Falcone, Garro, Longo and Spadafora, 2014); in fact, system components can be selected/customized/realized separately and then integrated so to obtain the overall system. However, the integration of system components is a challenging task whose criticality increases as the heterogeneity and complexity of the components increase. Thus, suitable engineering methods, tools and techniques need to be exploited to prevent and manage the risks arising from the integration of system components and, mainly, to avoid their occurrence in the late phases of the system development process which may result in a significant increase in the development cost.

To overcome these issues the adoption of the Systems Engineering approach represents a viable solution as it provides a wide set of methods and practices which allow the definition of the system architecture and behavior at different abstraction level in terms of its components and their interactions (Garro and Tundis, 2014; Tundis, Falcone and Garro, 2014; Garro and Tundis, 2012). Moreover, systems requirements are constantly traced during the different system development phases so to clearly specify how a system component concurs to the satisfaction of the requirements (Garro, Tundis, Rogovchenko-Buffoni and P. Fritzson, 2013; Rogovchenko-Buffoni, Fritzson, Garro, Tundis and Nyberg, 2013; Tundis, Rogovchenko-Buffoni, Fritzson and Garro, 2013). However, in the Systems Engineering field, even though great attention has been devoted to functional requirements analysis and traceability, there is still a lack of methods which specifically address these issues for non-functional requirements. As a consequence, the analysis concerning if and how non-functional requirements are met by the system under development is not typically executed contextually to the design of the system but still postponed to the last stages of the development process (e.g. system verification) with a high risk of having to revise even basic design choices and with a consequent increase in both completion time and development cost.

Among non-functional requirements, Reliability, which represents the ability of a system to perform its required functions under stated conditions for a specified period of time, is a key requirement to satisfy especially for mission critical systems where system failures could cause even human losses. Moreover, it is strongly related to other main system properties such as Availability, Maintainability, and Safety.

To perform quantitative and qualitative Reliability analysis, several techniques are currently available which are mainly based on statistical and probabilistic tools and on the hierarchical decomposition of the system in terms of its components. Nevertheless, the increase in both system complexity and accuracy required in the reliability analysis often goes beyond the capabilities of these techniques. Moreover, their integration in typical system development processes, and especially in the design phases, is quite difficult and then their use is often postponed to the later development stages (e.g. system verification). As a consequence, new techniques are emerging which are centered on model-based approaches so to benefit from the available modeling practices and which incorporate the use of simulation to flexibly evaluate during the design the system reliability performance and compare different design choices (Fritzson, Garro, Nyberg, Rogovchenko-Buffoni and Tundis, 2013; Garro and Tundis, 2013). Despite a general consensus on the advantages that could derive from their exploitation, the use of these model-based techniques has been traditionally unusual and has not been recommended by international standards until recently (see IEC 61508, 2010). This delay in the adoption is mainly due to the lack of methods able to integrate available modeling languages, tools and techniques in a consistent modeling framework.

In this context, the talk aims to discuss the main issues related to system dependability analysis and to present possible emerging solutions, centered on model-driven and simulation-based approaches, which will be exemplified through industrial case studies (Garro and Tundis, 2014; Garro, Groß, Riestenpatt Gen. Richter and Tundis, 2013; Garro and Tundis, 2014b).

References

A. Garro and A. Tundis, 2014. *On the Reliability Analysis of Systems and SoS: the RAMSAS method and related extensions*, IEEE Systems Journal (IJS), IN PRESS, IEEE Systems Council

A. Garro, J. Groß, M. Riestenpatt Gen. Richter, and A. Tundis, 2013. *Reliability Analysis of an Attitude Determination and Control System (ADCS) through the RAMSAS method*, Journal of Computational Science, in press, DOI, http://dx.doi.org/10.1016/j.jocs.2013.06.003, Elsevier B.V., Amsterdam (The Netherlands)

A. Falcone, A. Garro, F. Longo and F. Spadafora, 2014. *Simulation Exploration Experience: A Communication System and a 3D Real Time Visualization for a Moon base simulated scenario*, Proceedings of the 18th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (ACM/IEEE DS-RT), Toulouse (France)

A. Tundis, A. Falcone and A. Garro, 2014. *System Dependability Analysis through Platform-Independent Simulation Models*, Proceedings of the International Workshop on Applied Modeling and Simulation (WAMS), jointly held with the NATO CAX FORUM 2014, Istanbul (Turkey)

A. Falcone, A. Garro and A. Tundis, 2014. *Modeling and Simulation for the performance evaluation of the on-board communication system of a metro train*, Proceedings of the 13th International Conference on Modeling and Applied Simulation (MAS 2014), Bordeaux (France)

A. Garro and A. Tundis, 2014b. *RAMSAS4Modelica: a Simulation-driven Method for System Dependability Analysis centered on the Modelica language and related tools*, Proceedings of the Symposium On Theory of Modeling and Simulation (TMS) at SpringSim 2014, Tampa (FL, USA)

P. Fritzson, A.Garro, M. Nyberg, L. Rogovchenko-Buffoni, and A. Tundis, 2013. *Performing Fault Tree Analysis of a Modelica-based System Design through a Probability Model*, Proceedings of the Int. Workshop on Applied Modeling and Simulation (WAMS 2013), Buenos Aires (Argentina)

A. Garro, A. Tundis, L. Rogovchenko-Buffoni, and P. Fritzson, 2013. *From Safety Requirements to Simulation-driven Design of Safe Systems*, Proceedings of the 12th International Conference on Modeling and Applied Simulation (MAS 2013), Athens (Greece)

L. Rogovchenko-Buffoni, P. Fritzson, A.Garro, A. Tundis, and M. Nyberg, 2013. *Requirement Verification and Dependency Tracing During Simulation in Modelica*, Proceedings of the 8th EUROSIM Congress on Modelling and Simulation (EUROSIM 2013), Cardiff, (Wales, UK)

A. Tundis, L. Rogovchenko-Buffoni, P. Fritzson, and A. Garro, 2013. *Modeling System Requirements in Modelica: Definition and Comparison of Candidate Approaches*, Proceedings of the 5th International Workshop on Equation-Based Object-Oriented Modeling Languages and Tools (EOOLT 2013), University of Nottingham (UK)

A. Garro and A. Tundis, 2013. *Enhancing the RAMSAS method for Systems Reliability Analysis through Modelica*, Proceedings of the 7th MODPROD Workshop on Model-Based Product Development, Linköping University (Sweden)

A. Garro, J. Groß, M. Riestenpatt Gen. Richter, and A. Tundis, 2012. *Experimenting the RAMSAS method in the reliability analysis of an Attitude Determination and Control System (ADCS)*, Proceedings of the Int. Workshop on Applied Modeling and Simulation (WAMS), jointly held with the NATO CAX FORUM, Rome (Italy)

A. Garro, and A. Tundis, 2012. *Modeling and Simulation for System Reliability Analysis: The RAMSAS Method*, Proceedings of the 7th IEEE International Conference on System of Systems Engineering (IEEE SoSE), Genoa (Italy)

A. Garro, and A. Tundis, 2012b. *Enhancing the RAMSAS method for System Reliability Analysis: an exploitation in the automotive domain*, Proceedings of the 2nd International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2012), Rome (Italy)

A. Garro, and A. Tundis, 2012c. *A Model-Based method for System Reliability Analysis*, Proceedings of the Symposium On Theory of Modeling and Simulation (TMS) at SpringSim 2012, Orlando (FL, USA)

A. Garro, A. Tundis, and N. Chirillo, 2011.*System reliability analysis: a Model-Based approach and a case study in the avionics industry*, Proceedings of the 3rd Air and Space International Conference (CEAS 2011), Venice (Italy)

Biography

Alfredo Garro is an Associate Professor of Computing Systems at the Department of Computer Engineering, Modeling, Electronics and Systems Science (DIMES) of the University of Calabria.He received the Laurea Degree in Computer Engineering from the University of Calabria (Italy) on 2000. From September 1999 to September 2001, he has been a researcher at CSELT, the Telecom Italia Group R&D laboratories, where he worked on design and development of distributed systems. From October 2001, he collaborates with the Institute of High Performance Computing and Networking of the Italian National Research Council. On February 2005 he received the PhD Degree in Systems and Computer Engineering from the University of Calabria. From January 2005 to December 2011, he has been an Assistant Professor of Computing Systems at the Department of Electronics, Computer and System Sciences (DEIS) of the University of Calabria. His main research interests include: systems and software engineering, reliability engineering, modeling and simulation of complex systems. His list of publications contains about 80 papers published in international journals, books and proceedings of international and national conferences. Prof. Garro became a member of the *IEEE* and *IEEE Computer Society* in 2005; he is a member of the IEEE Reliability Society and IEEE Aerospace and Electronic Systems Society; he is member of the INCOSE Italian Chapter. Currently, he operates as a member of the *SPACE Forum Planning and Review Panel (PRP)* of the *Simulation Interoperability Standards Organization (SISO)*. He is member of the Executive Committee of the *MODRIO (Model Driven Physical Systems Operation)* ITEA2 European Project and the Technical Contact for his Institution in the *Open Source Modelica Consortium (OSMC)*.