An Holistic Approach to Dependability ?

Alberto Pasquinin, W. Goerke, Karama Kanoun, A Rizzo

An Holistic Approach to Dependability ?

Moderator: A. Pasquini, ENEA, Rome, ITALY
Participants: W. Goerke, Karlsruhe University, GERMANY
K. Kanoun, LIS-LAAS, Toulouse, FRANCE
A. Rizzo, University of Siena, ITALY

Abstract

This panel will address the problem of methods for dependability analysis and evaluation of computer system, where the human, hardware and software components are considered by an integrated approach. The state of the art consists of well developed methods in particular domains, but dependability is a total system concept. However practitioners have come to accept that their approaches address only some aspects of this total system view. This panel will move from the point of view of the specific participant competencies to discuss: the extent to which the individual approaches synergise (and the state of the art in doing that) or are antagonistic; the difficulties hindering an integrated approach to dependability.

Introduction

Alberto PASQUINI - ENEA
Email: pasquini_a@casaccia.enea.it

Safety-critical systems require an assessment activity to verify that they are able to perform their functions in specified use environments. This activity would benefit from evaluation methodologies that consider these systems as a whole and not as the simple sum of their parts. Indeed, analysis of accidents involving such systems as shown that they are rarely due to the simple failure of one of their components. Accidents are the outcome of a composite causal scenario where human, software and hardware failures combine in a complex pattern.

Well known examples include: space applications such as when the Phobos I flight control system and the ground control caused the failure of the space mission; medicine when a combination of an architectural flaw with a software fault and operator misbehaviour in the Therac 25 radiation therapy machine caused the over radiation and death of some cancer patients; nuclear power when a failure of the Crystal River process control system and the operator caused a radioactive water release. These examples are all drawn from large scale, low volume systems. The same kind of problem will also surface in increasingly volume produced items that will incorporate programmable components involving hardware, software and interaction with operators. An obvious area is in the automotive industry whenever

there are strong pressures to decrease costs and increase functionality through the use of programmable elements.

On the contrary, dependability analysis and evaluation of safety critical systems involving computers are based on techniques and methodologies that concern human, software and hardware components separately. Most integration efforts are limited to hardware and software components with the questionable assumption that their evaluation can be performed independently and then combined, for example using the traditional reliability graphs when evaluating reliability. Therefore the assessors of these systems have the difficult task of integrating the results of completely different and not compatible methodologies at different stages of advancement.

Furthermore, the research activity of experts and scientists usually addresses only one among the hardware, software and human components. There is an evident lack of communication between the researchers of these disciplines that have separate conferences, scientific journals and research networks.

An innovative approach is needed for the dependability analysis and evaluation of safety-critical systems. Instead of regarding the human, hardware and software components as effectively independent, this approach must take a holistic view seeking to identify the component inter-dependencies and incorporate the evaluation within a common framework. This aim requires the joint effort of experts and scientists from different disciplines: engineers, computer scientists, mathematicians, psychologists, and cognitive scientists.

Human as a Back-up for System Safety

Winfried GOERKE - Karlsruhe University
Email: goerke@ira.uka.de

Simplified the development of system dependability can be characterised in the following way: The classic view addresses functional limits of equipment, especially if reliability is concerned, hence back-up procedures in case of failure are required, originally by human operator or fail-safe design. More recent developments take increased levels of automation everywhere into account, such that a substitution of human functions also with respect to intelligent decisions can be observed, hence computer control of complex systems forms a basic solution approach.

As a consequence also dependability has shifted to systems as a whole: the user does not care for the reason for the denial of service, he simply requires an organisation masking all the detailed effects which might lead to failures of certain sub-components. He requires a design incorporating all possible deficiencies of functional details, being able to deliver the specified service in spite of possibly detailed malfunctions. Society has become used to the availability of sophisticated technical systems and depends upon them to a very large degree. But occasionally their limits in capability can be noticed: supply systems break down and disrupt service (power systems, telephone systems, railways), but service can be restored

after more or less short times. Limited safety, however, may lead to loss of human lives or cause damage to health or property which cannot be accepted, even if they seem to be unavoidable.

How can we increase safety or better decrease risk? From a hardware point of view fault tolerance and redundancy indicate possible solutions, but only to the limited extent of the physical device behaviour. A component breakdown can be masked to tolerate its occurrence as far as the system is concerned. But there are system aspects where this approach cannot be used, in particular the overall system design. As we have learned by bitter experience from the limited dependability achieved so far in e.g. air transportation and space flight, it is overwhelmingly the human part which will finally be blamed if an accident has occurred. This leads to the following questions:

- Has the hardware system design been sufficient as far as fault tolerance is concerned?
- Are there software components demonstrating design flaws or bugs robust to removal?
- Was there an operator mistake as far as back-up by human control is concerned? How was training organised, in particular with respect to the system state calling for back-up?
- What about system integration? Should not the influence of human errors be excluded from possibly causing a fatal system state because it is well known how error prone humans will react? How can this be achieved?
- Are our methods insufficient as far as human interaction is concerned?

Software Reliability Evaluation

Karama KANOUN
E-mail: kanoun@laas.fr

Software faults are design faults in the broad sense of the term, including faults injected from the requirements to operation and maintenance. Usually, software reliability evaluation consists in applying reliability growth models to the failure data collected on the software under consideration. This means that the field of software reliability evaluation addresses systems that are not life critical but that could be "money" critical. Since the obtained results are not accurate for all systems under any circumstances, several methods have been developed to improve the estimations obtained from these models. However, even for accurate estimations, the relevance of the measures estimated varies with the considered life-cycle phase. For instance, the most relevant estimations are obtained for software systems in operation, on multiple installations, since we have usually a sample of failures that are representative of system behaviour.

In the software reliability evaluation field, emphasis has mainly been placed on the development of a) reliability growth models and their related staff (such as model validation criteria) considering the software as a black box, b) methods to improve

the estimation accuracy, c) some structural models, taking into account the structure of the software and the transfer of control between the various components, mainly in stable reliability, and d) more recently and still in an infancy phase, methods incorporating past experience on previous similar software systems.

Most of these methods are applicable to hardware field; one of the questions to be addressed is: could they be used or, at least, adapted to human error collection and/or data processing ? Indeed, data collection for quantification of human behaviour is a growing concern now. Could the human reliability field benefit from the software reliability field ? Does the human behaviour exhibit a trend during system operation (more experience can improve the knowledge about the systems and their environment and hence the number of human errors can be reduced). Is the notion of reliability growth meaningful when dealing with human behaviour ?

Indeed, a first step towards a holistic approach has been jumped: a few models for system dependability evaluation, considering hardware and software faults together with their interactions (but excluding human errors) have been developed since several years (based on Petri Nets and Markov Chains). But how could the human behaviour be incorporated into these models ? More precisely, how could models integrating from the beginning the three aspects can be derived ? Is such an aim realistic ? These questions are of prime importance for those systems in which the safety depends heavily on the cooperation between the "technical system" and the human operator. An example of such systems is the Air Traffic Control System where the role of the technical system is only to process and provide information to the controller who has to take the final decisions (the technical system has not direct impact on the controlled environment).

Human Error and Distributed Cognition

Antonio RIZZO - University of Siena
Email: rizzo@unisi.it

System Reliability Analysis has made noticeable progress in assessing technical component reliability, but the introduction of Human Reliability Analysis is still a very difficult task.

Human interaction with objects and artefacts in both physical and social systems is frequently characterised by errors. However, "errors" are very often best attempts at accomplishing desired and sensible goals, and should not be necessarily attributed to incompetence. People may not have any way of foreseeing the unintended and deleterious consequences of their decisions and actions, and when negative modifications occur in the world, they might regret having taken a certain action or made a particular decision.

The recent user-centred design approach of man-machine systems considers the error as the product of breakdowns in communication between the humans and the physical artefacts. These breakdowns may play a fundamental role in the design process by revealing and creating space for problems and opportunities. Moreover,

as these authors have observed, a structured analysis of the processes that cause breakdowns and of the processes that allow to handle breakdowns should be useful to the designers. The inevitability of human error have led system designers to make a great effort to minimise the incidence of errors, to maximise their discovery, and to make easier their recovery or the repair of their consequences. However, despite the claims for user-centred systems, most of the available guidelines and design principles for error recovery are concerned with errors occurring at the syntactic level of the human-computer interaction. That is, error concerning users performances that violate rules in the grammar of the interaction. Guidelines and principles are not concerned with higher semantic and pragmatic levels of the interaction. How can a more general approach based on distributed cognition be identified and can it represent a sound support for a global analysis of system dependability ?

About the Panel Participants

Alberto Pasquini - He is with the Italian Agency for New Technology, Energy and the Environment (ENEA) where he works in European research projects in the area of software engineering and, more specifically, software quality and reliability. He was member of the Italian licensing authority for nuclear power plant where he was involved in the dependability evaluation of computer systems used to control nuclear power plants. His current interest are in software reliability and reliability evaluation of systems involving human components. He is the scientific coordinator of the OLOS network.

Winfried Goerke - He received his diploma in electrical engineering and graduated as Dr.-Ing. at the University of Karlsruhe, Germany. Being a full professor in the computer science department of this university his main research interests are related to fault-tolerant computing systems. Among his scientific publications there are textbooks on reliability engineering, fault diagnosis of switching circuits, microcomputers and fault-tolerant computing systems. He is a member of GI (German Computer Society) and ITG/VDE (society of information techniques within the association of German electronic engineers).

Karama Kanoun - She is currently Charge de Recherche at LAAS-CNRS. She joined LAAS in 1977 as a member of the "Fault-Tolerance and Dependable Computing" group. Her current research interests include modeling and evaluation of computer system dependability considering hardware as well as software. She has authored and co-authored more than eighty papers. She has conducted several research contracts and she has been a consultant for some French companies and for the International Union of Telecommunications. Dr Kanoun is a member of the working group of the European Workshop on Industrial Computer Systems (EWICS): "Technical Committee 7 - Reliability, Safety and Security", a member of the AFCET working group "Dependability of Computing Systems". She acts as a referee for several international conferences and journals. Besides serving on program committees of international conferences, she served as a program committee co-

chair of the international Symposium on Software Reliability Engineering (ISSRE'94) and she served as general chair of ISSRE'95.

Antonio Rizzo - He teaches Human-Computer Interaction at the Communication Science Department of the University of Siena. He worked at the Human Factors Unit of the National Research Council - Institute of Psychology in Rome. He has been involved in research on cognitive ergonomics since mid-eighties by working in several European founded projects and as consultant of national industries. His current interest are in the field of Multimedia Design and Distributed Cognition. In particular, he is concerned with the design of a Multimedia System for supporting disabled people involved in tourism activity; and with the development of an integrated approach for designing safety critical applications. He is the University of Siena co-ordinator for the Apple Design Project '96.

About the OLOS Network

OLOS is a network funded by the European Community under the programme Human Capital and Mobility, Contract: ERBCHRXCT 940577. Partners of the network are European Universities, Research Centres and Industries active in the dependability analysis and evaluation of computer systems. The interdisciplinary competencies that are present in the network ensure the resources needed for a holistic approach to dependability. Goals of the network are:

- To develop interdisciplinary competencies, especially among young researchers, concerning "global system dependability";
- To define and develop the concept of "global system dependability" in order that various dependability and reliability notions and methodologies can be seen to make a contribution to overall dependability;
- To promote the development of an integrated set of methodologies to be used for the dependability analysis and evaluation of those critical systems that require the combination of hardware, software and human resources.

More detailed information concerning the OLOS network can be obtained through the authors or visiting the World Wide Web site: http://rep1.iei.pi.cnr.it/OLOS.