INTERACTION IN CRITICAL SYSTEMS: CONQUESTS AND CHALLENGES

Marcos Salenko Guimarães, M. Cecília C. Baranauskas and Eliane Martins
Instituto de Computação, UNICAMP, Av. Albert Einstein, 1251, Campinas, SP, Brazil

Keywords: Critical Systems, User Interface, Software Engineering, Human-Computer Interaction.

Abstract: The need for critical systems is growing fast due to the demand on hardware and software systems for critical tasks that use to be executed exclusively by human beings. These critical systems require reliable interaction with users. Despite this fact, contributions from the interaction design field have progressed slowly. This work summarizes the main contributions from different fields to critical systems; presents some analysis based on a classification that helps to get different views and find out new possible research directions towards improving the quality of interaction with this type of system.

1 INTRODUCTION

Currently, we have experienced a growing demand on hardware and software systems to support the work on critical areas that use to be managed mostly by human beings.

The concept of a critical system has been discussed by several authors, encompassing conceptual to the technical issues. Most of the researchers define critical systems as software-based systems whose failure would provoke catastrophic or unacceptable consequences for human life.

Some authors relate the concept of criticality with dependability in systems. A method is described aiming to support dependability in interactive-safety critical systems (Marhan et. al., 2004). A "dependable system" is defined as a system which has six attributes (Knight, 2004): Reliability (to operate correctly when used); Safety (to operate with no danger); Confidentiality (no unauthorized information is used during the system execution); Integrity (no unauthorized modification of information is made during the use of the system); and Maintainability (possibility of software maintenance). Precise definitions of terms related to dependability have been developed over a period of many years (Avizienis et. al., 2001).

Literature on critical systems has shown several cases of human-system failures that resulted in people's deaths. Therac-25 is a typical case: an X-ray used to obtain bone images (through x-ray emission) or to treat tumors (through radiation emission). This error message had no meanings for the operators, who just ignored it (Mackie and Sommerville, 2000). However, for the software developer, the message intended to inform that the radiation dosage was above normal. Due to this communication problem reflected in the user interface, the consequence of this episode was disastrous leading to several deaths because of the extreme radiation injected to patients. More dramatically, as the effect of over dosage was not instantaneous, it took several years for the problem to be identified.

In aviation systems, many incidents (incidents are unexpected events that may or may not lead to accidents that may lead to deaths) have reasons originated from failures during user-system interaction. Some statistics are shown (Harrison, 2004b): from 34 total incidents, 1.100 computer-related accidental deaths (1979-1992); 4% of the deaths due to physical causes; 3% of the deaths due to software error; 92% of the deaths due to problems related to human-computer interaction. According to ATC (Air Traffic Control), 90% of the air traffic incidents were due to fault attributed to pilots or controllers.

These reports show us the role a reliable user interface (better human-computer interaction) has in enabling the correct use of critical artefacts and supporting decision making mainly during emergency situations when the users are in panic.

Salenko Guimarães M., Cecília C. Baranauskas M. and Martins E. (2007).
INTERACTION IN CRITICAL SYSTEMS: CONQUESTS AND CHALLENGES.
In *Proceedings of the Ninth International Conference on Enterprise Information Systems - HCI*, pages 170-175
DOI: 10.5220/0002350201700175

We understand that the Human-Computer Interaction (HCI)-related subjects have a role to play and responsibilities to assume in this particular domain. The objective of this work is to summarize some of the main contributions of literature to the field and identify gaps and new challenges related to interaction design in safety-critical systems.

This paper is organised as follows: the next section synthesises relevant contributions for critical systems coming from different fields. Section 3 groups the main findings, aiming to help with different views about the conquests so far and new challenges. Section 4 presents new possible directions for research and Section 5 concludes.

2 CONTRIBUTIONS OF LITERATURE FOR CRITICAL SYSTEMS

Several disciplines have historically contributed to development in the field of critical systems; the main contributions can be categorized into the following groups:

- *Human Factors and Cognitive related Theories* has contributed especially to our understanding of human errors in critical systems. The main findings in this area have been used to explain human reaction when dealing with critical situations.
- *Software Design and Usability* focuses on improvements in some parts of a software development process that can be applied to the user interface component. Some authors contribute providing some additional or modified steps in the software development process to improve the quality of the user interface regarding critical systems.
- *Socio-Technical Approaches* have many critical systems depend on the interaction among a group of people. Socio-technical approaches are necessary to understand the interaction among team members using an artefact.

Several works are proposed in literature for critical systems for improving the quality of human-computer interaction. Most of them involve the areas of human factors and cognitive theories, software design and usability, and socio-technical theories. Some studies can't be categorized only in one approach because they are multidisciplinary in nature. For example, Filipe's work (Filipe et. al., 2003) not only focuses on socio-technical but also mentions some user interface design because this work can be applicable for improvements in user interface design. Therefore, the categorization below considered the main topic of each work. The main contributions, grouped by their approaches, are summarized in Table 1.

HCI still has more to contribute for critical systems regarding interaction design issues, communications, evaluation and validation techniques. Table 1 also shows that the amount of work related to socio-technical aspects applicable to safety critical systems is significantly reduced when compared with the other categories of contributions. This finding doesn't mean that this approach is less important; quite the contrary, the most cited cases related to safety-critical systems, Air Traffic Control (ATC) systems, are socio-technical systems (Hopkin, 1995). It clearly involves social issues, human-computer interaction, human-human interaction, besides human factors, cognition, software design and usability.

Table 1 also shows that most of these works have practical contributions directed to the design phase of safety-critical system development. There is still a lack of contributions for supporting the other phases of safety-critical system development.

Methods for developing requirement analysis applicable to critical systems are still rare in literature. Are the existing requirements analysis techniques adequate for critical systems? The requirement analysis is also a known problem for developing a critical system (Johnson, 2003). One of the reasons of misunderstandings among stakeholders is the vocabulary used. In critical systems, this problem is a fundamental one. A common ground understanding among software developers, HCI experts and the domain stakeholders, regarding the ontology for the field seems to be still missing.

The impact of usability regarding emergency situations in critical applications deserves deeper analysis. The disturbance caused by emergency alarms may affect the user's mental model causing more mistakes and slips in interaction with the system. In socio-technical systems such as an Air Traffic Control system, this problem may be more complex because it involves the consideration of much more interaction factors.

To have a big picture of the contributions so far and to analyse the gaps still remaining in the field we situate them in the Semiotic Onion, which is described in the next section.

Table 1: Main contributions in interaction for critical systems.

Approach	Researcher	Contribution
Human Factors and Cognitive related Theories	(Baxter and Besnard, 2004)	The "glass cockpit" could mean that a pilot would have fewer tasks and problems but the pilot needs to know not only about aviation but also about how to use the system.
	(Hollnagel, 1993)	A model for human behaviour and cognition is presented for understanding emergencies when the operator maintains control, loses control, and/or regains control of the situation.
	(Harrison, 2004a) (Harrison, 2004b) (Smith and Harrison, 2002a) (Smith and Harrison, 2002b)	Methods for obtaining a number (or several numbers) that represents the "dimension" of the human error calculating the error probability and its impact if it occurs.
	(Galliers and Minocha, 2000)	A technique based on BBN (Bayesian Belief Network) model for calculating of probabilities of human error is executed based on this graph.
	(Daouk and Leveson, 2001)	A new approach to structuring specifications, called Intent Specifications, which captures the design rationale and assumptions made throughout the design process.
	(Vicente and Rasmussen, 1992) (Vicente et. al., 1998) (Vicente et. al., 1995) (Vicente, 2002)	A theoretical framework called Ecological Interface Design (EID) for designing user interfaces focusing on environment-human relationship analyzing the perception of the work environment that affects human behaviour.
Software Design and Usability	(Palanque et. al., 1997) (Palanque and Schyn, 2003)	A method is proposed with related tools and techniques to engineer the design and development of usable user interfaces. This method uses Petri Net to formally model the system behaviour.
	(Reeder and Maxion, 2006)	This work is not only lists several criteria for detecting the user hesitation but also defines a method that can be automated for detecting instances of user difficulty based on identifying hesitations during system use.
	(Fields et. al., 2000)	A method is presented for evaluating and comparing design options (task performance, analysis of user deviations and consequent hazards, and coordination) for allocating communication media in an interactive safety-critical system.
	(Connely et. al., 2001)	Extend and evaluate existing pattern language for safety-critical user interface development.
	(Paternò et. al., 2005)	A method to help designers to identify and derive interfaces that support users in their activities.
	(Pap and Petri, 2001)	The design patterns of user interface for safety-critical systems is presented for helping the reuse as much proven solutions and structures as possible.
Socio-technical	(Filipe et. al., 2003)	The timed knowledge approach is presented showing enhancements the ability to model, design and analyse procedures in socio-technical systems.
	(Gurr and Hardstone, 2001)	The potential of diagrammatic representations of the knowledge of system users and designers is shown during the implementation process, in order to support communication between the two groups.

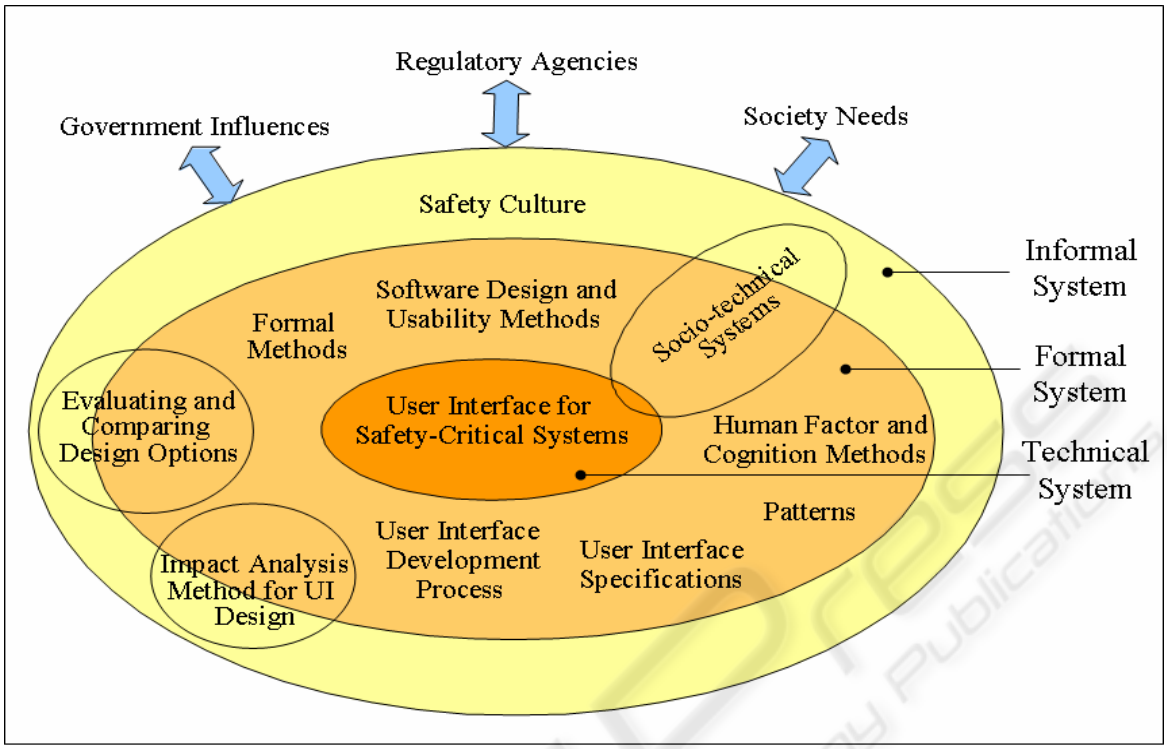

Figure 1: The "onion" model instantiated.

3 A STEP BEYOND HCI: THE SEMIOTIC ONION

The contributions listed in Table 1 can be understood from a global view of information systems by using Organizational Semiotics (Stamper, 1973) artefacts. OS (Organizational Semiotics) understands that any organized behaviour is governed by a system of social norms which are communicated through signs. The "Semiotic Onion" represents any information system including the critical ones, as situated in a Society, in which several entities cause direct or indirect influences in the automated artefact. In the informal system level, there is a sub-culture where meanings are established, intentions are understood, beliefs are formed and commitments with responsibilities are made, altered and discharged. At a formal system level (this term is more generic when compared to the same term used in Software Engineering. Formal system level includes, but is not limited to the formal methods), form and rule replace meaning and intention and finally, in technical level, part of the formal system is automated by a computer-based system. The informal level embodies the formal that, by its turn, embodies the technical level, meaning that changes in any level have impact in the other levels (Liu, 2000).

Using this model to distribute the previously discussed works, we can have another view of the impact of the contributions. Figure 1 illustrates that the contributions so far are mostly situated in the formal layer, with methods, processes and patterns related to the formal aspects of developing critical systems. Not much was found regarding the informal systems layer. The needs of a safety culture are acknowledged within an organization for contributing to safety improvement (Johnson, 2003). If people are not aware of the importance of safety, it will be difficult to apply any formal method related to safety. Studies related to informal information systems may bring important contributions for safety-critical systems in general through improvements in their interaction design.

Based on the theoretical model of OS we are now investigating the use of norms as a basis for generating a user interface in compliance with specific safety situations. Two kinds of norms are being proposed: generic and specific ones. Generic norms would be useful for generating abstract user interfaces which can be "tailored" to accommodate specific situations in concrete user interfaces.

The norms shouldn't be restricted to norms related to safety and dependability such as: availability, reliability, integrity, confidentiality and maintainability, but must encompass the informal layer of the critical system specific context.

This norm approach may contribute to norm-oriented design patterns. It can be useful for designing interfaces in conformance to norms defined by government, regulatory agencies or defined by experienced designers that usually are based on successful cases.

One of the challenges to the field of critical systems involves providing methods to construct a meaningful understanding of the organizational context of safety-critical systems. Artefacts and methods to cross the frontiers between the informal, formal and technical layers of the semiotic onion would benefit both HCI and Software Engineering specialists. The investigation domain must be wide and a framework is still necessary to deal with the influence of the organizational aspects of social nature in the definition of critical system requirements for designing a smooth user-system interaction.

4 CONCLUSION

This paper presented a literature survey regarding design for critical systems and identified three main classes of contributions: a class related to human factors and cognitive approaches, a class related to software design in general and usability in particular, and a class related to socio-technical approaches. The first class focuses on the human in isolation, especially for analyzing human cognition in critical situations that lead to error.

Considering the software design as a whole, there are some efforts towards the identification of problems in earlier steps of the software development process. The contributions mostly propose specifying formally the user interface as a way of avoiding future misunderstandings of developers.

Contributions focusing on the socio-technical aspects of critical situations focus on analyses to discover the cause of problems in the socio-technical context, in which groups of people interact with the artefact.

Summarizing, theories of interaction design still have a contribution to make regarding quality improvement of critical systems user interfaces. Further work involves analyzing the potential of other theories to capture the informal social system implications on design; methods and artefacts for sharing problem understanding in the safety-critical application domain, especially during requirement analysis.

ACKNOWLEDGEMENTS

We thank CNPq for funding (476381/2004-5).

REFERENCES

Avizienis A., Laprie, J., Randell B., 2001. Fundamental Concepts of Dependability. *Research Report N01145*. Retrieved November 16, 2006, from http://www.cert.org/research/isw/isw2000/papers/table_of_contents.html.

Baxter, G., Besnard, D., 2004. Cognitive Mismatches in the Cockpit: Will They Ever Be a Thing of the Past? In *The Fight deck of the Future: Human Factors in Data links and Free flight conference.* University of Nottingham Press.

Connelly, S., Burmeister, J., MacDonald, A., Hussey, A., 2001. Extending and Evaluating a Pattern Language for Safety-Critical User Interfaces. In *6th Australian Workshop on Safety Critical Systems and Software.* Australian Computer Society, Inc.

Daouk, M., Leveson, N. G., 2001. An Approach to Human-Centered Design. In *Workshop on Human Error and System Development*. Retrieved October 24, 2006, from http://web.mit.edu/hfes/www/Research.htm.

Fields, R., Paternò, F., Santoro, C., Tahmassebi, S., 2000. Comparing Design Options for Allocating Communication Media in Cooperative Safety-Critical Contexts: A Method and a Case Study. *ACM Transactions on Computer-Human Interaction*, 4, 370-398. ACM Press.

Filipe, J. K., Felici, M., Anderson, S., 2003. Timed Knowledge-based Modelling and Analysis: On the dependability of Socio-technical Systems. In *8th International Conference on Human Aspects of Advanced Manufacturing: Agility and Hybrid Automation*. Retrieved March 9, 2005, from http://www.dirc.org.uk/publications/inproceedings/abstract.php?id=41.

Galliers, J., Minocha S., 2000. An Impact Analysis Method for Safety-critical User Interface Design. In *ACM Transactions on Computer-Human Interaction*. ACM Press.

Gurr C., Hardstone G., 2001. Implementing Configurable Information Systems: A Combined Social Science and Cognition Science Approach. In *4th International Conference on Cognitive Technology*, 391-404. Springer-Verlag.

Harrison, M., 2004a. Human Error Analysis and Reliability Assessment. In *Workshop on Human*

Computer Interaction and Dependability. Retrieved May, 2, 2006 from http://www.laas.fr/IFIPWG/ Workshops& Meetings/46/05-Harrison.pdf.

Harrison, M., 2004b. Aspects of Human Error: A brief introduction. In *Workshop on Human Computer Interaction and Dependability*. Retrieved May, 2, 2006, from http://www.laas.fr/IFIPWG /Workshops& Meetings/46/03-Harrison.pdf.

Hopkin, V. D., 1995. *Human Factors in Air Traffic Control*, Taylor & Francis. London.

Hollnagel, E., 1993. The Modelling of Loss of Control. In *International Conference on Systems, Man and Cybernetics*, 3, 44-49. IEEE Press.

Johnson, C. W., 2003. *Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting*. Glasgow University Press.

Liu, K., 2000. *Semiotics in Information Systems Engineering*. Cambridge University Press.

Knight, J. C., 2004. An Introduction to Computing System Dependability. In *26th International Conference on Software Engineering*. IEEE Press.

Mackie, J., Sommerville, I., 2000. Failures of Healthcare Systems. In *First Dependability IRC Workshop*, 79-85. Edinburg University Press.

Marhan, A., Paternò, F., Santoro, C., 2004. Improving Dependability through a Deviation Analysis on Distributed Tasks in Safety Critical Systems. In *Workshop on Interdisciplinary Approaches to Achieving and Analysing System Dependability.* Retrieved September 14, 2006, from http://hom epages.cs.ncl.ac.uk/michael.harrison/dsn/index.html.

Palanque, P., Schyn, A., 2003. A Model-Based Approach for Engineering Multimodal Interactive System. In *INTERACT'03*. IFIP.

Palanque, P., Bastide, R., Paternò, F., 1997. Formal Specification as a Tool for Objective Assessment of Safety-Critical Interactive Systems. In *INTERACT'97,* 323-330. ACM Press.

Paternò, F., Santoro, C., Touzet, D., 2005. Adapting Interface Representations for Mobile Support in Interactive Safety Critical Contexts. In *Workshop on Complexity in Design and Engineering*. Glasgow University Press.

Reeder, R. W., Maxion, R. A., 2006. User Interface Defect Detection by Hesitation Analysis. In *International Conference on Dependable Systems & Networks*. IEEE Press.

Smith, S. P., Harrison, M. D., 2002a. Blending Descriptive and Numeric Analysis in Human Reliability Design. In *9th International Workshop on Interactive Systems: Design, Specification and Verification,* 2545, 223-237. Springer.

Smith, S. P., Harrison, M. D., 2002b. Augmenting Descriptive Scenario Analysis for Improvements in Human Reliability Design. In *Symposium on Applied Computing*. ACM Press.

Stamper, R. K., 1973. *Information in Business and Administrative Systems*, John Wiley and Sons. New York.

Vicente K. J., 2002. Ecological Interface Design: Progress and Challenges. In *Human Factors,* 44, 62-78. Human Factors and Ergonomics Society Press.

Vicente K. J., 1991. Representation Aiding for Problem Solving in Process Control System. In *Systems, Man, and Cybernetics,* 2, 1189-1194, IEEE Press.

Vicente K. J., Christoffersen K., Pereklita A., 1995. Supporting Operator Problem Solving Through Ecological Interface Design. In *Systems, Man, and Cybernetics*, 25, 529-545. IEEE Press.

Vicente K. J., Torenvliet G. L., Jamieson G. A., 1998. Making the Most of Ecological Interface Design: The Role of Cognitive Style. In *4th Symposium on Human Interaction with Complex Systems*. IEEE Press.

Vicente, K. J., Rasmussen, J., 1992. Ecological Interface Design: Theoretical Foundations. In *Systems, Man, and Cybernetics*, 22, 589-606. IEEE Press.

Pap Z., Petri, D.,2001. A Design Pattern of the User Interface of Safety Critical Systems. In *International Workshop on Control and Information Technology*. Retrieved October 24, 2006, from http://citeseer.ist.psu.edu/pap01design.html.