Beyond Usability for Safety Critical Systems: How to be SURE (Safe, Usable, Reliable, and Evolvable)?

Philippe Palanque
LIIHS-IRIT,
University Toulouse 3,
31062 Toulouse, France
palanque@irit.fr

Sandra Basnyat
LIIHS-IRIT,
University Toulouse 3,
31062 Toulouse, France
basnyat@irit.fr

Regina Bernhaupt
ICT&S-Center,
Universität Salzburg
5020 Salzburg, Austria
Regina.Bernhaupt@sbg.ac.at

Ronald Boring
OECD Halden Reactor Project
N-1777 Halden, Norway
ronald.boring@hrp.no

Chris Johnson
Dept. of Computing Science,
University of Glasgow,
Glasgow, G12 8QQ, Scotland
johnson@dcs.gla.ac.uk

Peter Johnson
Dept. of Computing Science,
University of Bath,
Bath, G12 8QQ, England
p.johnson@bath.ac.uk

Abstract

While a significant effort is currently being undertaken by the CHI community in order to apply and extend current usability evaluation techniques to new kinds of interaction techniques very little has been done to improve the reliability of software offering these kinds of interaction techniques. As these new interaction techniques are currently more and more used in the field of command and control safety critical systems the potential of incident or accidents increases. Similarly, the non reliability of interactive software can jeopardize usability evaluation by showing unexpected or undesired behaviors. Lastly, iterative design processes promote multiple designs through evolvable prototypes in order to accommodate requirements changes and results from usability evaluations thus reducing reliability of the final system by lack of global and structured design. The aim of this SIG is to provide a forum for both researchers and practitioners interested in safety critical interactive systems. Our goal is to define a roadmap of activities to cross fertilize usability, reliability and safety for these kinds of systems to minimize duplicate efforts and reuse knowledge in all the communities involved.

Keywords

Usability, Reliability Safety critical systems, Human Error.

Introduction

Usability problems might appear in different forms in
the user interface, reducing the user performance with
the device, increasing the number of errors or having
users being reluctant to use the device due to
uncomfortable/unpleasant interaction. In the last
decades, the Computer-Human Interaction (CHI)
community has developed several methods to support
sound and rigorous identification of usability problems.
Many approaches have been proposed to cope with the
diversity of contexts in which evaluation has to take
place. Such methods may involve observation of users'
activity, inspection by a usability specialist, simulation
and/or prediction of usability problems sometimes
based on models describing users' expected activity
like, for instance, task models. Model-based approaches
are an example of such methods and provide better
support for the design of interactive systems, for
example by identifying usability problems in the early
phases of the development process thus reducing the
time and development costs.

Such development approaches are beneficial for the
systems the majority of the population interacts with on
an almost daily basis. However, in the field of safety-
critical interactive systems, ensuring usability, as well
as requirements such as reliability and safety is crucial.
Reliability and safety requirements are even harder to
meet when evolvability of the successive designs is a
critical aspect of iterative design processes exploited in
order to improve their usability.

A safety-critical system is one in which any failure or
design error has the potential to lead to loss of life or,
in other terms that failure outweighs the cost of
development. Safety-critical interactive systems add
the human dimension to a software system by putting
control into the hands of a human operator. Examples
of such systems include nuclear power plants, railway
systems, airplane cockpits, and military systems.

Safety, Usability, Reliability and Evolvability (SURE) can
be seen (at first glance) as convergent and always
desired properties of an interactive system. In fact they
all consider a different and orthogonal point of view on
system development. A typical example of conflicting
requirements between reliability and safety is given if
someone puts a gun on his/her head and the finger on
the trigger. The more reliable the gun the less safe it
is. Similarly the reliability of telecommunication has
decreased (for fixed line) from 99.9999% in the early
90s down to 99.9% (for mobile phones) in the late 90s.
This percentage of reliability represents an change of
unavailability of service from 52mn34s up to
36days12h per year [10]. This loss of reliability has not
prevented users to drop fixed lines and eagerly move to
mobile technologies thanks to a significant increase in
utility and usability.

The aim of this SIG is to provide a forum for both
researchers and practitioners interested in safety
critical interactive systems. Our goal is to define a
roadmap of activities to cross fertilize usability,
reliability and safety for these kinds of systems to
minimize duplicate efforts and reuse knowledge in all
the communities involved. Its aim is also to provide a
new opportunity for attendees to previous SIGs on
related topics to meet again and to provide the first

step towards community building. Finally, despite the fact that safety issues receive a growing interest at CHI conferences [11], publications related to that topic are still very limited and ways for increasing it will be discussed during the SIG.

Related Events

At CHI 98 we organized a workshop on "Designing User Interfaces for Safety Critical Systems" [7]. Even though the workshop was successful, almost no work in this area has been presented at CHI since then. At CHI 2004 we organized a SIG on "Safety-Critical Interaction: Usability in Incidents and Accidents" in order to take the opportunity of having CHI organized in Europe to attract participation from European research centers and practitioners involved in this field [8]. As a possible consequence Safety was one of the highlights of CHI 2005 conference (with the motto Technology, Safety, Community). At CHI 2006 a SIG has also been proposed on the topic "Testing Interactive Software: a Challenge for Usability and Reliability" that successfully gathered more than 60 participants [9]. We believe that this SIG will be a good opportunity to pursue in that direction of increasing the awareness and concern of CHI community to both safety and reliability aspects. At CHI 2005 we also organized a SIG on the role of HCI for the next generation of control rooms [4]. We plan to reuse this application domain [5] and other connected ones (such as aircraft cockpits [2] and air traffic control workstations [1]) and learn from other application domains where reliability and safety are less prominent (e.g., interactive TV [3]). The SIG organizers have significant experiences in these application domains, and they will discuss similarities and differences to foster participation from the audience.

Audience

One of the goals of this SIG is to identify and gather people interested in the field of human-computer interaction for safety critical systems, software engineers interested in the reliability and usability of interactive systems, as well as researchers interested in the maturation of usability evaluation methods. We foresee the following types of participants:

- Practitioners who work in the design, construction testing and certification of safety critical interactive systems. We welcome both practitioners coming from the engineering side of interactive systems as well as practitioners with a background in user interface usability testing.

- Academics working or interested in the state of the art and research activities in the field of usability, reliability and safety.

The audience would be approximately 50-100 professionals and academics interested in how to improve safety, usability, reliability and evolvability of interactive systems by integrating mainly unconnected research work within a unifying framework.

SIG Organization

The activity plan for the SIG is as follows:

- Introduction of the SIG goals and participants (10 minutes);

- Presentation by the organizers of issues in the various fields related to the topic of the SIG (5 minutes per topic) (total 20 minutes)

- Gathering from the audience (as well as presenting from the SIG organizers' experience) examples and case studies (10 minutes).

- Interactive discussion with participants to list the issues related to the integration of SURE element within interactive systems development processes. Those that seem more important will be selected, and comments on the solutions will be recorded (30 minutes).

- Interactive discussions on the issue of new interaction techniques (Post-WIMP, multimodal, …) and how exploratory work in the field of human-Computer Interaction (like focusing on User eXperience, fun or exotic input devices) may constitute divergent paths towards the 4 aspects of SURE interactive systems. How can we improve and support both reliability and safety when faced with these new interaction techniques? (10 minutes)

- Discussions on future plans and, in particular, how to increase CHI community interests in reliability and safety sides of interactive systems design. In addition, how to increase submissions to CHI conferences will be discussed. A questionnaire about participants work as well as expectations from CHI community will be distributed to the participants. Results will be passed on to the conference management committee (10 minutes)

References

[1]   Bastide R., Navarre D., Palanque P. A Model-Based Tool for Interactive Prototyping of Highly Interactive Applications. Demonstration, *Proc. CHI 2002,*ACM Press (2002), 516-517.

[2]   Bastide R., Navarre D., Palanque P., Schyn A., Dragicevic P. A Model-Based Approach for Real-Time Embedded Multimodal Systems in Military Aircrafts. Proc. ICMI 2004, ACM Press (2004), 243-250.

[3]   Bernhaupt, R., Ploderer, B., Tscheligi, M. Relevance of Prior Experience in MHP Based Interactive TV Services, *Proc. Interact 2005, Lecture Notes in Computer Science*, Springer (2005), 1149–1152.

[4]   Boring R., Hugo J., Richard C. Dudenhoeffer D. The Role of Human-Computer Interaction in Next-Generation Control Rooms. *CHI 2005 Special Interest Group. CHI 2005 Conference Companion*, ACM Press (2005), 2033-2034.

[5]   Boring, R.L., Gertman, D.I., Joe, J.C., Marble, J.L. Human reliability analysis in the US Nuclear power industry: A comparison of atomistic and holistic methods. *Procs. of the 49th Meeting of the Human Factors and Ergonomics Society*,2005, 815-1819.

[6]   M. Ould, R. Bastide, D. Navarre, P. Palanque, F. Rubio, A. Schyn. Multimodal and 3D Graphic Man-Machine Interfaces to Improve Operations. *Eighth International Conference on Space Operations*, (2004).

[7]   P. Palanque, F. Paternò, R. Fields. Designing User Interfaces for Safety Critical Systems. CHI 98 workshop report, *SIGCHI Bulletin*, October 1998, vol. 30 n°4.

[8]   Palanque P., Johnson C., Koornneef F., Szwillus G., Wright P. Safety-Critical Interaction: Usability in Incidents and Accidents. *CHI 2004 Special Interest Group. Extended Abstracts CHI 2004,* ACM Press (2004), 1600-1601.
http://liihs.irit.fr/palanque/SIGchi2004.html

[9]   Palanque P., Bernhaupt R., Boring R. Johnson C. Testing Interactive Software: a Challenge for Usability and Reliability. *CHI 2006 Special Interest Group. CHI 2006 Extended Abstracts*, ACM Press (2006), 1600-1601. http://liihs.irit.fr/palanque/SIGchi2006.html

[10] J. Gray. Dependability in the Internet Era. http://research.microsoft.com/~Gray/talks/InternetDependabilityStanford_2006.ppt

[11] Johnson C. Applying the Lessons of the Attack on the World Trade Center, 11th September 2001, to the Design and Use of Interactive, Evacuation Simulations, *ACM CHI* 2005, pp. 651-660, 2005, ACM Press.