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

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

Regina Blandford
UCLIC,
University College London
London WC1E 7DP, England
a.blandford@ucl.ac.uk

Ronald Boring
Idaho National Laboratory
Idaho Falls 83415, Idaho, USA
ronald.boring@inl.gov

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

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, BA2 7AY, England
p.johnson@bath.ac.uk

What is written in the advance programme

SPECIAL INTEREST GROUP | ROOM: C4

BEYOND USABILITY FOR SAFETY CRITICAL SYSTEMS

MODERATORS:
Philippe Palanque, Sandra Basnyat, University Toulouse, France
Regina Blandford, Universität Salzburg, Austria
Ronald Boring, Idaho National Laboratory, USA
Chris Johnson, University of Glasgow, UK
Peter Johnson, University of Bath, UK

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.
Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)

Introduction

- Beyond Usability for Safety Critical Systems
- What are SURE interactive applications?
- Safe vs Reliable vs Usable and Evolvable
  - What about usability testing of a non reliable interactive application (last year’s SIG)
  - What about reliable applications with poor usability (command line OS)
  - How to keep safety-critical applications evolvable?
- Hollistic versus reductionist (sorry it’s spoiler)
Safe, Reliable, Usable and Evolvable

- Safety
  - Will not put people’s life at stake
- Reliability
  - Defect free, one use does not interact with next uses, wear-ability (reliability over time), healing by reboot (re-install)
- Usability
  - Ease of use, Ease of learning, ...
- Evolvability
  - Wrong/incomplete user needs
  - Evolution of user needs over time (development process)

Why are they orthogonal?

- Usable & Reliable then Safer
  - Aircrafts
  - Command & Control systems
- Usable & Reliable vs safe
  - The less usable the safer
  - The less reliable the safer
Why are they orthogonal?

- Things are improving
  - Mean Time To Failure
  - MTTR

Why are they orthogonal?

- Usable vs Reliable
  - Faster to deploy
  - Easier to reconfigure
  - ...

32"
5’15”
52’34"
8h46’
3d16h
36d12h
SURE is not enough

- Trustability
- Reliability
- Availability
- Scalability
- Security
- User experience
- ...

} Dependability e.g. e-gov

Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)
Safe and Error-Tolerant

- Errors caused by…
  - Incorrect or incomplete knowledge
    - Can usually be dealt with through training or revised system design
  - Slips – cognitive or physical
    - Cannot be eliminated by training ... or even by incentivising.
    - Cognitive slips can (we believe) be accounted for by failures of attention

Ways to understand error

- Retrospective: accident reports, diaries, reflections on actions, etc.
- Concurrent: lab-based experiments
  - Devise games that provoke high error rate then manipulate features to establish how error rate changes.
Resilience

- Users mitigate against system failures
- Human error often regarded as the cause of failures
- Design challenge is to minimise human errors
  - Through staff selection, training, etc.
  - Through design
    - Need to understand likely sources of error

Evolvability

- Evolution may reduce errors
  - E.g. by removing likely causes of cognitive slips (PCEs, mode errors, errors caused by poor awareness of system state, etc.)
- Evolution may increase errors
  - E.g. habituation
- Need to understand as much as possible about the causes of error to make the best possible predictions of the effects of design changes.
Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)

Usable and Evolvable

- Usable Systems
  - User-Centered Design
    - Iterative Design
    - From ethnographic studies to usability evaluation method
  - Usability criteria and beyond
    - Usability vs user experience, ...
    - Factors like fun, pleasure, aesthetics, ...
Usable Systems

- Design for error avoidance

Usable Systems

- UEMs conducted by experts
  - Usability Inspection Methods, Guideline Reviews, ...
  - Any type of interactive systems
- UEMs involving the user
  - Empirical evaluation, observations, ...
  - Any type of interactive systems (from low-fi prototypes to deployed applications)
- Computer supported UEMs
  - Automatic testing based on guidelines, ...
  - Task models-based evaluations, metrics-based evaluation, ...
  - Applications with standardized interaction techniques (Web, WIMP)
Ensuring Usability

- Lab or field
- Method selection
- Data gathering/analysis
- Problematic Area: Testing in non-traditional environment

Ensuring Usability in Non Traditional Environments

- Combine and balance different UEMs according to usability/reliability issues
- Combine Lab and Field
- Select UEMs according to development phase
Usability & Evolvability

Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)
Reliable and evolvable

- Things went worse on many aspects
  - Interactive aspects of current software
  - Development processes
  - Evolution of research
- Things went better on other aspects
  - Users are ready to deal
  - Costs are declining
  - Gresham’s Law: “bad money drives out good”

Interactive aspect of software

- Things went worse on many aspects
  - Interactive aspects of current software
    - Reactive nature and event-loop architecture
    - Un-testable state space
  - Development processes
    - From cascading to iterative
    - Specific phases for SC systems (certification)
  - Training
Interactive Systems

Interactive System

Input

Output

System

User

Time

Event-based Functioning

At startup
- Register Event Handlers
- Call Window Manager

Finished

Application

At runtime
- Event Handler 1
- Event Handler 2
- Event Handler n

States

Window Manager

Event Queue

EH Registration

Get next event

Dispatch event

Ack received

Wait for next event
State Space

Development Processes

wish → analyse → design → implementation → test → operation

wish → new needs → analyse → operation → test → design → implementation
The Shift from Reliability to Fault-Tolerance

- Failures will occur
- Mitigate failures
- Reduce the impact of a failure
- An example: MS Word files recovery – mitigate impact
Training Costs

- Training is very expensive
  - Requires specific equipment
  - Users are not at work
- Training for bad designs is even more expensive
  - Autopilots behaviours (40% of the time spent on 20% of the behaviour of the AP corresponding to 5% of operation-HCI aero 2006)

Evolvable Systems

- The point of the conflict with safety critical industry
- Possible options
  - Simulation
    - Rôle of simulations
    - Validation of simulations
  - Tailoring
    - Worse includes everything in the system
  - Barriers
The notion of barriers

- Barrier = systems that prevent or stop an undesired consequence
- Ammunition loading problem in tanks
- Hardware easier/more independant
- Same philosophy in software (patches) does not work with certification

Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)
Roadmap for a SURE-Set-up: audience participation

- Small groups of people
  - Identifying 5 keywords (or more)
  - Identifying potential/primary application domains
  - Write down them on cards
- Position the cards on the roadmap
  - Position them in the time frame
  - Position them according to the lanes
Outline of the SIG

- Short introduction about the SIG (10 mn)
- Short presentations (20 mn)
  - Safe and error-tolerant (Ann)
  - Usable and Evolvable (Regina)
  - Reliable and Evolvable (Philippe)
- Roadmap for a SURE-Set-up: audience participation (20 mn)
- Setting up the roadmap (20 mn)
- Discussion, summary & future plans (20 mn)

Books related to the SIG? (other than HCI)

- Resilience Engineering: Concepts and Principles
  - Edited by Erik Hollnagel, David Woods, Nancy Leveson
  - 2006
- Human Error
  - James Reason
  - Cambridge University Press, UK, 1990
- Basic Concepts and Taxonomy of Dependable and Secure Computing
  - Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr
  - IEEE Transactions on Dependable and Secure Computing
  - Vol. 1, Issue 1 (January 2004) P.11 - 33
- Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting
  - http://www.dcs.gla.ac.uk/~johnson/book/
Future Plans and Announcements

Future plans
- Web site is setup and will be populated (slides, list of attendees, topics, ...)

Further work
- IFIP WG 13.5 on Human Error Safety and System Development ifipwg13-5@irit.fr
- NoE ResIST (Resilience for IST) www.resist-noe.org
- MAUSE: www.cost-294.org

Announcements
USAB 07 - Usability & HCI for Medicine and Health Care

2nd Symposium of the WG HCI&UE of the Austrian Computer Society
From data, information and knowledge to the support of medical workflows

Thursday, 22nd November 2007

OFAZ University Hospital

Important Dates:
- Monday, 4th June 2007: Preliminary deadline for submissions
- Wednesday, 24th September 2007: Camera-ready due
- Thursday, 22nd November 2007: Symposium

The proceedings will be published jointly Springer in "Lecture Notes in Computer Science (LNCS) Series".

For any questions contact: andreas.hoferer@medunigraz.at