Efficient Modelling and Analysis of User Interfaces in High-Assurance Systems

Saulo Silva
saulo.r.silva@inesctec.pt

HASLab/INESC TEC & Universidade do Minho
Braga, Portugal
Overview of Agenda

Introduction
• Introduction.
• Focus of the research.
• Definitions.
• Motivation.

Context
• Approaches to formal modelling and analysis of human machine interaction.
  – Analysis of usability and safety properties of user interface design.
  – Analysis of user interface design against task models.
  – Analysis of user interface design against human behaviour.

Research
• Objective.
• Tools to support the research.
  – PVSio-web.
  – CIRCUS.
• Ongoing work.
• Future work.
Agenda

Introduction
- Introduction.
- Focus of the research.
- Definitions
- Motivation
  - Approaches to formal modelling and analysis of human machine interaction.
    - Analysis of usability and safety properties of user interface design.
    - Analysis of user interface design against task models.
    - Analysis of user interface design against human behaviour.
- Objective.
- Tools to support the research.
  - PVSio-web.
  - CIRCUS.
- Ongoing work.
- Future work.

Context

Research
Introduction

• Early user interface in injection pump

Mechanical injection pump (1951).
Focus of the research

Formal Modelling and Analysis of Human-Machine Systems

Infusion Pump.  

Airplane cockpit
Definitions

Interactive human-machine systems
Represent systems that interact with humans.

Interactive system model
 Defines how the system responds to user actions.
Motivation

Unpredicted situations can happen due to problems in user interfaces

- Mode confusion;
- Lack of visibility of system state;
- Lack of consistency of controls;
- …
Motivation

Aircraft ran out of fuel (1985)

– Mode confusion when refuelling the aircraft

Boeing 767-233 after forced landing.

¹Lockwood. Investigating the Circumstances of an Accident Involving the Air Canada Boeing 767 Aircraft. 1985.
Motivation

Overdose of radiation accidentally given to patients (1985)

– High energy dosage given due to user Interface bug

Motivation

Superheating misdiagnosed (1979)

– Design flaw in the control room

Three Mile Island control room.

1United States. President's Commission on the Accident at Three Mile Island. The need for change, the legacy of TMI: report of the President's Commission on the Accident at Three Mile Island. The Commission, 1979.
Agenda

- Introduction.
- Focus of the research.
- Definitions
- Motivation.

- **Approaches to formal modelling and analysis of human machine interaction.**
  - Analysis of usability and safety properties of user interface design.
  - Analysis of user interface design against task models.
  - Analysis of user interface design against human behaviour.

- Objective.

- Tools to support the research.
  - PVSio-web.
  - CIRCUS.

- Ongoing work.

- Future work.
Approaches to formal modelling and analysis of human machine interaction

1) Analysis of usability and safety properties.

2) Analysis against task models.

3) Analysis against cognitive models.
I) Analysis of usability and safety properties

Example: Visibility of operational modes of an infusion pump.
1) Analysis of usability and safety properties

Ex.: visibility of data-entry mode in the Flight Control Unit (FCU).
I) **Analysis of usability and safety properties**

Challenges:

- the scalability of the analysis;
- the relevance of counter-examples produced by the analysis.
2) Analysis against task models.
2) Analysis against task models.

- Ex.: approaches based on
- Verification of system models and the task model
- Co-execution, simulation and test and the task model
Analysis: Verification

• Bolton et al (2013)\textsuperscript{1}

Analysis: Verification

• Campos (2003)\(^1\)
  – Task model and system model: described as interactors
    • Expressed in Modal Action Logic (MAL)
  – Analysis: using IVY tool
    • Automatic translation of the interactors models in NuSMV models and properties.

Analysis: Simulation/Co-execution

• Palanque et al (2010)$^1$

2) Analysis against task models.

Challenges:

• how to analyse systematically non-normative behaviours?
• how to take into account strategies to optimise task operations?
• Simulation and test are not as exhaustive as verification!
3) Analysis against cognitive models.
3) Analysis against cognitive models.

Example:
Rushby (2002)\(^1\) work on mental models for tackling automation surprises.

3) Analysis against cognitive models.

Challenges:
how to validate the cognitive assumptions incorporated in the user model.
Agenda

Introduction
- Introduction.
- Focus of the research.
- Definitions
- Motivation.
- Approaches to formal modelling and analysis of human machine interaction.
  - Analysis of usability and safety properties of user interface design.
  - Analysis of user interface design against task models.
  - Analysis of user interface design against human behaviour.

Context
- Objective.
- Tools to support the research.
  - PVSio-web.
  - CIRCUS.
- Ongoing work.
- Future work.
Objective of this research

Explore how to combine two analysis methods:
- verification of usability and safety properties;
- verification against task models.

Expected outcome:
- Set of design patterns presenting efficient solutions to combine these two approaches.
Tools for analysis of system and task models

• PVSio-web

• CIRCUS
PVSSio-web

• Ex.: modelling a push button
PVSio-web

- Description of the system model in emucharts (FCU Software)\(^1\)

CIRCUS toolset

- Ex.: task model (FCU software)

Ex: Abstract tasks – task that involves tasks of different types

Ex: Enable operator (>>)
Tasks can be executed one after another (left to right)

HAMSTERS task model

Reach button
Change pressure unit
Click on button
Change units
Display units
Check units

CIRCUS co-execution of system and task models
Specific reasons to justify the tools

- **PVSio-web**
  - can represent system models in the notation of statecharts;
  - analysis is made using theorem proving;
  - does not support explicit task modelling;
  - does not suffer with incompleteness of the analysis.

- **CIRCUS**
  - can translate task models into a notation compatible with that used for modelling the system.
Ongoing work

• Early stage of this research;
• Two formal tools are currently being used;
• Allows to investigate the definition of efficient modelling patterns (combining task models and system models).
Future work

• Moving to a realistic case study
  – Medical domain
  – Avionics domain
Thanks for listening!

saulo.r.silva@inesctec.pt

Acknowledgements

This project is partially supported by Project "NORTE-01-0145-FEDER-000016", financed by the North Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, and through the European Regional Development Fund (ERDF).

Conselho Nacional de Desenvolvimento Científico e Tecnológico