# Analysing Human Aspects of Safety-Critical Software

by Michael D. Harrison and José Creissac Campos

***In focusing on human system interactions, the challenge for software engineers is to build systems that allow users to carry out activities and achieve objectives effectively and safely. A well-designed system should also provide a better experience of use, reducing stress and frustration. Many methods aim to help designers to produce systems that have these characteristics. Our research is concerned with the use of formal techniques to help construct such interactive systems.***

We have a number of goals in treating our subject formally. The first is to make both the identification and solution of usability problems clearly traceable and systematic. We wish to use models of interactive behaviour that make usability assumptions precise and to use tools that enable a systematic and thorough exploration of how these usability assumptions are captured in the system. An important issue in this respect is whether the models capture the relevant properties of the system without biasing the analysis inappropriately. We want to avoid focusing on problems that do not connect well with the actual use of the system. This is an ongoing topic of research and one that involves engagement with human/computer interaction specialists. We have been researching the applicability of model checking to reasoning about interaction design. This has included the development of a set of standard property templates that can be used systematically to analyse these systems. Different models can be used to characterize different features of the system. An important concern is to determine how these analyses can be performed in a complementary way.

Two modelling perspectives are important to the approach we take. The first is the interactive device. The device could be a control panel, a desktop computer, a mobile phone or a table-top interface. The important characteristic from the perspective of the analysis is that the user can be thought of as being in a dyadic relationship with it. The second is the interactive system. Here the focus of analysis is the whole system. While this might be an interactive system where the main players are the device and the user, we may also be concerned with several users immersed within a smart environment involving sensors, public devices and small handheld devices that move around as the user moves from place to place. The important characteristic here is that users are seen not as exogenous entities but rather as part of the system.

Two recent examples of analyses relate to these two levels. At the device level we have used the IVY tool (see link below) to analyse the user interfaces of a car air-conditioning system and a flight management system, and we are currently working to build a substantial repository of useful specifications. The control panels of the devices are specified in Modal Action Logic (MAL).

Standard usability properties of the device are analysed systematically by creating instances of standard templates. An important feature of this analysis is to provide representations of counter-examples that would enable a human factors specialist to use the information as a basis for constructing and analysing scenarios in which the desirable properties failed. This has enabled us to explore interactions between the different modes of the system and to explore potential inconsistencies in the design. Examples of design issues detected include the system reaching unsafe states due to user interface mode problems, or inconsistencies in the behaviour of user interface controls.

At the interactive system level we have explored smart environments. For example, we have developed models using Promela, UPPAAL and PEPA to explore the characteristics of a building containing situated displays, designed to guide people unfamiliar with the environment to their destinations. Properties of the information that flows to mobile users are explored as users change their context in such smart environments. Here formal models have been designed to help engineers to visualize usability issues in relation to the consequences of different designs. In the case of Promela we explore alternative designs in which the displays in each space can show one or a number of directions (where the directions are tagged with appropriate destinations). We have also explored different assumptions about the capacities of the different rooms and properties related to the ease with which visitors can reach their destinations. As well as exploring the information that flows to the individual, we are concerned with exploring the impact of a potential design on collective behaviours using stochastic models.

Traditional usability analysis methods based on testing and expert reviewing are challenged by the increasing complexity of new systems being built. This is particularly true in the case of safety-critical systems. We believe formal approaches provide answers by delivering rigorous and repeatable analysis in an automated manner. Tools are needed that streamline the modelling and analysis process. At the moment we are moving towards researching support for the interpretation of the analysis results by developers.

**Link:**
IVY tool:
http://www.di.uminho.pt/ivy

**Please contact:**
Michael D. Harrison
Newcastle University, UK
E-mail: Michael.Harrison@ncl.ac.uk
http://www.cs.ncl.ac.uk/people/michael.harrison

José Creissac Campos
Universidade do Minho, Braga, Portugal
E-mail: Jose.Campos@di.uminho.pt
http://www.di.uminho.pt/~jfc