Introduction to the Special Issue on Interface Issues and Designs for Safety-Critical Interactive Systems: When There Is No Room for User Error

Software is increasingly being used to control safety-critical systems. Much research since Leveson's fundamental article "Software Safety: Why, What, and How" (*ACM Computing Surveys* 18, 2 (1986), pp. 125–163) has focused on ways to reduce or avoid software failures. However, the reliability of even the best-engineered software can be undermined by its user interface. Indeed, interface design for safety-critical interactive systems poses special challenges to the human-computer interaction community.

This special issue addresses the challenge of analyzing, designing, and building reliable and usable safety-critical interactive systems. From a pragmatic point of view a safety-critical system is a system for which the cost of a failure is more important than the cost of developing the system. Safety-critical interactive systems add the human dimension to a software system by putting control into the hands of a human operator. Prominent examples of such control systems include nuclear power plants, railways systems, airplane cockpits, and military systems. Recent years have seen much effort put into the reengineering of the control system that is well represented in this special issue—air traffic control.

When compared to office automation systems, human-computer interaction for safety-critical interactive systems is both familiar and different. For instance, the management of a functionality like "undo," that can be seen as a usability issue in an office automation system, can become a critical functionality when the user interacts with a safety-critical system.

The three articles in this special issue provide three snapshots for how human-computer interaction issues play out in the broader field of safety-critical interactive systems. In the first article, **"Is Paper Safer? The Role of Flight Strips in Air Traffic Control,"** Wendy Mackay provides a detailed ethnographic study on how air traffic controllers work. The article promotes an interesting perspective on the use of multidisciplinary approaches for the analysis of safety-critical interactive systems. Based on this study the author cautions against the illusive quick fix of replacing existing work practices with new technology. The article may be considered controversial: it does not accept the idea that all safety features can be articulated and easily re-created in a radically new system. It suggests a third route, namely, to embed new technology into the existing, known, mostly safe work practices.

Galliers, Sutcliffe, and Minocha in their article **"An Impact Analysis Method for Safety-Critical User Interface Design"** focus on the analysis of human error and its implications for the design of safety-critical interactive systems. System design is examined from the perspective of

system failure resulting from the user or the system environment. The analysis method can be used to examine the consequences of errors for the purpose of influencing interface design. A reengineered interface would seek to avoid occurrence of errors or to reduce their effect. The analysis is supported by a probabilistic model that uses Bayesian Belief Nets. A case study of a laser spectrophotometer is fully treated according to the proposed method.

In **"Comparing Design Options for Allocating Communication Media in Cooperative Safety-Critical Contexts: A Method and a Case Study,** Fields, Paternò, Santoro, and Tahmassebi propose a method for comparing design options for safety-critical interactive systems. As in Mackay's article, the case study entails en-route air traffic control. An important contribution of this article is a method for an integrated analysis of three important methods of this field: task performance, analysis of user deviation and consequent hazard, and cooperation among users.

Each of the three articles deals with the analysis and design phases of safety-critical interactive systems. If changes are to be made to large, complex, safety-critical control systems, the changes must be made early in the development lifecycle, where redesign in response to identified problems is feasible.

This special issue arose from a CHI'98 Workshop organized by Palanque and Paternò ("Designing User Interfaces for Safety-Critical Systems," *SIGCHI Bulletin* 30, 4). The three articles included in this special issue were selected from more than a score of papers received. The editors thank and acknowledge their debt to the many qualified external reviewers from several countries who have helped select and improve (through their comments) the contributions in this special issue.

WAYNE D. GRAY
George Mason University

PHILIPPE PALANQUE
University of Toulouse 1

FABIO PATERNÒ
CNUCE—C.N.R.