Available online at www.sciencedirect.com
ScienceDirect
Safety Science 45 (2007) 305–327
SAFETY SCIENCE
www.elsevier.com/locate/ssci

# Safe by design: where are we now?

Andrew Hale [a,*], Barry Kirwan [b], Urban Kjellén [c]

[a] *Safety Science Group, Delft University of Technology, Postbus 5015, 2600 GA Delft, Netherlands*
[b] *EUROCONTROL – EEC BP15, Bois des bordes 91222 Bretigny Cedex, France*
[c] *Hydro Oil and Energy, N-0246 Oslo, Norway*

**Abstract**

This paper reviews and discusses the principal findings of the preceding papers in the special issue and draws out the lessons to be learned by designers, safety specialists and researchers.

It returns to the questions posed in the editorial and groups them under the headings of the case for design as an important contributor to operational safety, the general principles of the design process and whether they are universally applicable across different technologies and fields of application, the dilemmas facing designers and the help which can be offered to assist them in their vital and difficult work.

The paper ends with a summary of the gaps in our knowledge of the design process and its contribution to safety. These are large and cry out for more research to study them.


*Keywords:* Safe design; User and designer mental models; Design standards; Use situations

The papers in this special issue can only give a broad-brush impression of the state of the art of safety in design. Most of them are written from the point of view of the safety and human factors experts, working to improve the attention paid in the design stage to safety issues. Only a few are written from the point of view of the designer or design team, the people who ultimately have to carry out the difficult task of achieving that improvement. However, we believe that a clear picture nonetheless emerges, which can form the basis for designers to achieve a more systematic approach to inherently safe design. We try to summarise that approach in this paper.

* Corresponding author.
*E-mail addresses:* a.r.hale@tudelft.nl (A. Hale), barry.kirwan@eurocontrol.int (B. Kirwan), urban.kjellen@hydro.com (U. Kjellén).

0925-7535/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2006.08.007

In the subsequent sections we will develop a number of issues further under the following headings, which we derive from the questions we posed in the editorial:

1. The case for safety by design.
2. The general principles of the design process: context, nature, content, roles and responsibilities.
3. Dilemmas facing the design organisation.
4. Conclusions: what is the scope for improvements?

## 1. The case for safety by design

We started this special issue by addressing the question: How important is design in determining the level of safety during use of a system or product? Before we can answer that question, we need first to be clearer about what is covered by the design process.

### *1.1. Defining design*

An issue on which there was no clear agreement in the papers is what is covered by the design process – where does it start and when does it end? Does it include the initial choice of the high level concept for fulfilling the system objectives, or does the design process only start once this has been specified and is being worked out? If so, what is this transition point? Clearly this boundary will reflect in part what is being designed. If we consider the design of oil and gas installations, it makes no sense for the contractor responsible for detailed design to question the high level choices that led the customer (oil company) to define the need for the specified installation, rather than another type of installation or other design capacities. For the customer of consumer products, it may well be sensible to consider this choice as a design decision, as the customer has no control over it. We see this boundary question also reflected at the other end of the design process. Kinnersley and Roelen indicate that, in aviation, the operating procedures for a plane (or other parts of the system) are considered as part of the design. The European standard on safety in machinery design also considers the instruction manual as part of the design (CEN, 1991). Errors in this aspect of design, related to procedures development, should therefore be considered design errors.

As Fadier and De la Garza's paper indicates, the boundary of the design process cannot be completely sharp. In the process of installation of equipment and start-up, the system boundary shifts because the plant cannot be installed as specified, or proves not to be operable within the defined design limits. In some of the studies reviewed by Kinnersley and Roelen these sorts of shifts (use beyond the design base and change of operational context) are counted as design errors. This seems to be pushing the responsibility of the designer very far, raising as it does the issue of 'predictable misuse'. The EU Machinery regulations also include mention of this concept (European Council, 1989/98). In a paper presented to the workshop, but not included in this special issue, Blanquart (2003) indicated that the space industry has an even wider definition. Designers are asked to consider how the crew and controllers of a spacecraft can use the craft outside the planned design envelope, since this may be the only possibility to save the mission (as Apollo 13 demonstrated).

There is no simple solution to this issue of defining the boundary of design. The definition will need to depend on the context and the purpose for which it is being made. We sug-