INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN
ICED 03 STOCKHOLM, August 19-21, 2003

EFFECTS THAT DEFEAT RISK REDUCING MEASURES

J S Busby and E J Hughes

Abstract

An important element in the control of risk is understanding how counter-measures, or barriers, can be undermined. This paper describes a study of how barriers to accident sequences fail in practice. The objective, in particular, was to influence designers - to help them understand how designed barriers failed, and how the nature of a design impeded the operation of other barriers. Fifty accidents reported in oil drilling operations were analysed in an attempt to characterise the nature of the barriers that had been or should have been in place, and how they had been undermined. Some of the barriers had a self-limiting quality, in that there was some intrinsic quality of the barrier that limited its effectiveness. This often took effect via the operator: typically the existence of a barrier induced an operator behaviour and this behaviour then undermined the barrier. This tended to arise when the operator misunderstood the intention rather than the causation that lay behind the barrier. We have suggested two main reasons why designers fail to predict this effect, both of which are essentially structural and not to do with the qualities of designers themselves. We have also suggested how designers could be supported in 'second order' reasoning. This requires them to identify risks and provide counter-measures, and then also to examine how the counter-measures are themselves at risk.

Keywords: Risk, risk reduction, failure, barriers

1 Introduction

The idea of 'barriers' is central to much of our thinking about hazardous systems, and to some influential models of how catastrophic failures arise [1]. Rather than representing processes of successful operation or performance, these models are based on representing trajectories of failure that can be intercepted by barriers of various kinds. Even if there is an appreciable likelihood of any one barrier being penetrated, the presence of several, independent barriers makes the overall accident probability small. Barriers rely on a wide variety of strategies – ranging from redundancy and variety in the technical system [2], to 'forcing functions' [3] in the human interface. The generalised concept of a 'barrier' has also been used in some recent approaches to representing and analysing risk. Svenson, in particular, has developed an 'accident evolution and barrier model' [4][5][6]. This has been used in the analysis of complex, hazardous systems such as nuclear refuelling plant [7], and is rather similar to 'safety barrier diagrams' [8]. There are some contexts in which the term 'barrier' has been used in a more specific sense – for example in 'energy trace and barrier analysis' – and some researchers have referred only to physical mechanisms as barriers [9]. Increasingly, however,

‘barrier’ is being used in its most general sense as anything that can arrest accident sequences, as an arbitrary kind of defence mechanism [10].

Nonetheless techniques such as accident evolution and barrier analysis provide only weak support to the designer for determining whether barriers could be ineffectual or even counter-productive. There are several phenomena of which they take no obvious account. For example there is a 'risk homeostasis' effect [11] whereby people have a target level of risk, and if systems are made safer they will simply adjust their behaviour to nullify the safety improvement. There is also a 'risk migration' effect [12] whereby measures that reduce one type of risk introduce another type. And there is a so-called 'levee effect' [13] whereby measures that reduce one risk induce people to ignore related, and possibly greater, risks against which there is no protection. It is also well known that defence in depth is a fundamentally limited strategy for protecting complex systems. Multiple levels of protection simply serve to obscure progressive failure, so when – for example – routine violations of procedural barriers go uncorrected the cumulative probability of an accident increases considerably over time [14].

All of these phenomena tend to defeat barriers to failure paths put in place by designers. The aim of this study was therefore to help designers understand more systematically how barriers are undermined. Techniques like Svenson’s accident evolution and barrier analysis provide a relatively formal way of representing what someone (such as a designer) already knows about failure paths and defences: our aim was to give the designer additional knowledge of what limits the efficacy of these defences.

2 Method

The method was to analyse a secondary data source (accident investigation reports) in order to determine empirically how barriers are undermined. In contrast, previous work, such as Kecklund *et al*’s [15] study, has concentrated on assessing barriers by getting operators to judge their relative effectiveness. The data consisted of accident reports held by the International Association of Drilling Contractors, which are reported in a standardised form and then made available, anonymously, in the public domain. The sample consisted of the 50 most recent reports at the time of the study. All the accidents had occurred on or around hydrocarbons drilling operations. Evidently there are problems in relying on data of this kind – such as response bias and attribution bias, and the results have to be interpreted with this in mind.

These reports were analysed by inspecting what kind of barriers had existed, or should have existed, and what had defeated them or led them to be absent. An attempt was made to characterise the barriers themselves by categorising them according to their source (physical, human or organisational) and their effect (for example, whether they functioned by providing some kind of restraint). These categories were obtained by inspecting the data, rather than drawing on any existing framework. We then tried to determine what condition had undermined the barriers. For example, in one case a barrier to the interaction of exposed power cables and grounded equipment had been provided by physical separation. The cables were mounted much higher than the equipment. Nonetheless the equipment had to be manipulated in a narrow space by the operators, which meant they turned it on end. In this orientation it extended far enough to make contact with the power cables. Plainly the

designers had not predicted how space restriction constrained the operators to manipulate the system in such a way that the planned barrier was defeated.

An attempt was then made to develop a model that would describe in very general terms how the undermining effects took place, and to build the analysis of undermining effects into a support tool that would help designers assess the barriers they incorporated in their designs.

3 Results

There were 50 cases that were analysed, and from these 116 distinct barriers were identified. The conditions that undermined 112 of these could be inferred from the reports, and 45 of these undermining conditions were distinct. Table 1 shows the numbers of barriers categorised under each main type of source (on the horizontal axis) and effect (on the vertical axis). Thus, for example, 22 of the barriers had a physical source and had the effect of providing some kind of restraint. It can be seen that most of the barriers were either provided by the physical design or by organisational mechanisms of various kinds – although the capabilities of individual humans operating and maintaining the system accounted for a little under 20% of the identified barriers. Some care has to be taken in using these results, however, as the categorisations are only approximate: they are not entirely mutually exclusive.

Table 1. Quantities of barrier types

effect \ *source*	Physical	Human	Organis-ational	*totals*
Restraint (restricts possible translation or transition)	22	2	3	27
De-energisation (removes or denies energy that could provide a hazard)	8	2	6	16
Integrity (maintains the integrity, coherence or wholeness of a system)	2	2	4	8
Predictability (renders a specific hazard predictable, for example by tests)	2	2	3	7
Salience (makes a hazard obvious)			1	1
Separation (keeps apart two entities that together would be a hazard)	7	5	12	24
Stability (maintains a stable configuration)		1	3	4
Circumscription (sets or prescribes limits to an activity)		1	1	2
Interference (prevents passage of some hazard to contact with organs)	4	1		5
De-stressing (removes load from a structure of some kind)	1			1
Extinction (extinguishes a hazardous phenomenon such as fire)	2			2
Freeing (allows a system to find an operable state)	1			1
Avoidance (allows a task, step or activity to be avoided)			1	1
Unspecific	1	5	11	17
totals	50	21	45	116

The types of source in Table 1 should be self-explanatory, but a brief explanation has been provided for the types of effect.

Most of the barriers were very simple, reflecting the nature of drilling operations and the particular accidents that had occurred. Table 2 gives examples of some of the undermining effects associated with physical barriers – which are generally of most interest to designers.

Table 2. Examples of undermining effects with physical barriers

barrier	*barrier failure*	*undermining effect*
Protective hooping on a ladder	This was removed at particular locations to allow access	*Confounding:* barriers that impede a required activity tend to be dismantled
General purpose safety glasses provided	Harmful powder swirled and entered eye on a indirect trajectory	*Bias*: attention tends to be biased towards direct trajectory hazards
Side plate should prevent separation and fall of the object	Side plate was left open	*Learning:* Assembly would usually remain intact without side plate closed so operators learned it was unnecessary
Drain valve allowed evacuation of tank's content and avoidance of over-pressurisation during wash out	Viscous contents clogged the valve	*Replication:* Sizing of valve by designer was based on prior practice not analysis
Elevators have latches to prevent dropped casings	Latches failed without additional safety pins	*Dependency:* Design of latch failed to take account of misorientation and lateral forces inhibiting latching
Spatial separation of exposed power lines and grounded or manually handled equipment	Congested space restricted manoeuvring of large handling boom and long pipes allowing contact with power lines	*Constraint:* Spatial separation precluded in the handling of long items in narrow spaces
Securing devices provided for moving cylinders	Devices not used during a lift	*Intuition:* Operators' intuitive physics probably underestimated accelerations
Watertight door movement made slow to allow evacuation of gap	Operator opened door only partially and was trapped as it closed	*Side-effect:* Time-saving action removes latency protection
Specialised cut-off tools provided to avoid problems of cutting with general purpose tools	Grinder used for a cut-off operation instead of a cut-off tool	*Specialisation:* Tool specialisation requires more tools and makes them less likely to be available
Spatial separation between crane lines should prevent entanglement and degradation	Simultaneous use of both lines in poor visibility led to unknown entanglement	*Complexity:* Spatial separation was undermined by movement of both elements
Temporary cover installed to prevent fall through aperture	Temporary cover interpreted as additional impact cover so operator fell through after removal	*Cueing:* Replacement measures can appear to be additional measures unless they signal otherwise

4 Model

In some cases it was the designer's understanding of how the system behaved in practice that was simply deficient. For example, a crane toppled when the boom crept beyond safe limits.

Limit switches stopped the boom moving beyond these limits by cutting off power, so were ineffective when the crane crept after the power had been removed. Plainly the designer had failed to predict that 1) movement could occur without external power, 2) the barriers incorporated in the design assumed that movement only occurred under power. We can only speculate why this prediction was not made, but it seems likely that if a designer's mental model is essentially of a device that provides translation under power then it might be quite hard to think spontaneously of behaviour that does not conform to this model.

In some other cases, it was the operator's understanding of a hazard (rather than a designer's) that was deficient in a simple way. For example, in one instance operators were provided with mechanisms for physically restraining the movement of large cylinders during a lifting operation, but failed to use them. They seemed to have under-estimated the accelerations that were possible in such situations, probably because they relied on an intuitive understanding of physics that they had acquired in everyday life. This can plainly be misleading when operating specialised systems.

However there were some undermining effects that were not obviously a limitation of the designer's or operator's understanding alone. These effects had several general properties:

- The barriers had a self-limiting quality. The effects that undermined a barrier arose from the nature of the barrier itself. For example, a designer had identified a crushing risk associated with the operation of a heavy, sliding watertight door. (S)he had minimised this risk by making the door action very slow, so when the door was open there was considerable latency before the door would contact anyone still within the doorway. This slowness of action, however, led people to open the door only partially, so the expected latency was not there in practice - and there was an accident in which an operator was crushed.
- The undermining effect involved an operator's response to the barrier. In the case of the watertight door the operator's goal of getting through the door quickly was confounded by the slowness of the action, so the door was opened only partially. There was another case where a designer has provided an automatic cut-off in case an operator forgot to stop a filling operation. The operator, on seeing such a device, reasoned that (s)he could walk away and do something else, knowing that the automatic device would stop the operation. Such devices, intended only to protect against occasional operator lapses, typically do not have the reliability needed as the sole operating mechanism.
- Designers and operators appear to have similar, or at least consistent, causal models of the barrier in question. In the case of the automatic cut-off there was no discrepancy in their knowledge of what the device does. The discrepancy arises in the intention that was ascribed to the device, not the causality. Designers see redundancy as protective, as a means of reducing failure risk. Operators see redundancy as an opportunity to reduce effort or allocate effort elsewhere. In another case, a radio was used to communicate between one operator and another and an accident occurred when the first failed to receive a 'stop' signal from the second. The radio had apparently failed (if only intermittently). The protocol that the operators had adopted - to send a 'stop' message rather than continually send a 'continue' message - meant that failure of the channel could not be distinguished from the absence of a message. Both the designers and operators of radios know that failure of a channel will lead to the absence of messages, so again the failure was at the level of intentionality. The importance of understanding intentionality is one of the principles that underlies work on ecological interface design [16].

We have integrated these observations in the model of Figure 1. This suggests that designers identify risks, and then search for barriers or defences to deal with these risks. Part of this

barrier search involves an evaluation of whether the barrier is effective. A barrier is implemented and ultimately performs in practice, and there is some level of outcome risk as a result. The model suggests that knowledge of what can undermine barriers contributes to the barrier evaluation, and this knowledge can either be worked out by looking at reports of how failures have occurred in practice, or by making predictions based on the intrinsic nature of the design. In the dotted boxes, the model also suggests what detracts from the activity in the solid boxes. First, what detracts from barrier performance is 'confounding behaviour': operators doing things that stop the barriers working (for example opening isolation doors part-way). This arises because of the mismatch in intentionality understood by the designer and operator.

Also, however, two things detract from the designer's ability to predict this. First, designers sometimes reason top-down: that is, they will work out particular functions, and given these functions will work out ways of achieving them, and given these solution principles will find ways of embodying them in particular structures or mechanisms. Operators, on seeing a particular object (like a level switch) have to reason in the opposite direction, bottom-up, to find a function that the object will perform, and the requirement that the function meets. Designers' top-down reasoning blinds them, to a degree, to what operators will see when reasoning bottom up. Second, designers do not properly learn about operators from incidents or accidents because of attribution bias (for example [17]). People generally are vulnerable to emphasising other people's disposition rather than the situation when judging their performance. A designer, learning of an accident involving an operator, is biased towards explaining it in terms of operator qualities like foolishness rather than situational qualities like an unhelpful design. We are suggesting that, sometimes, knowledge about the undermining of barriers does not influence designers in their choice of barriers as much as it should.

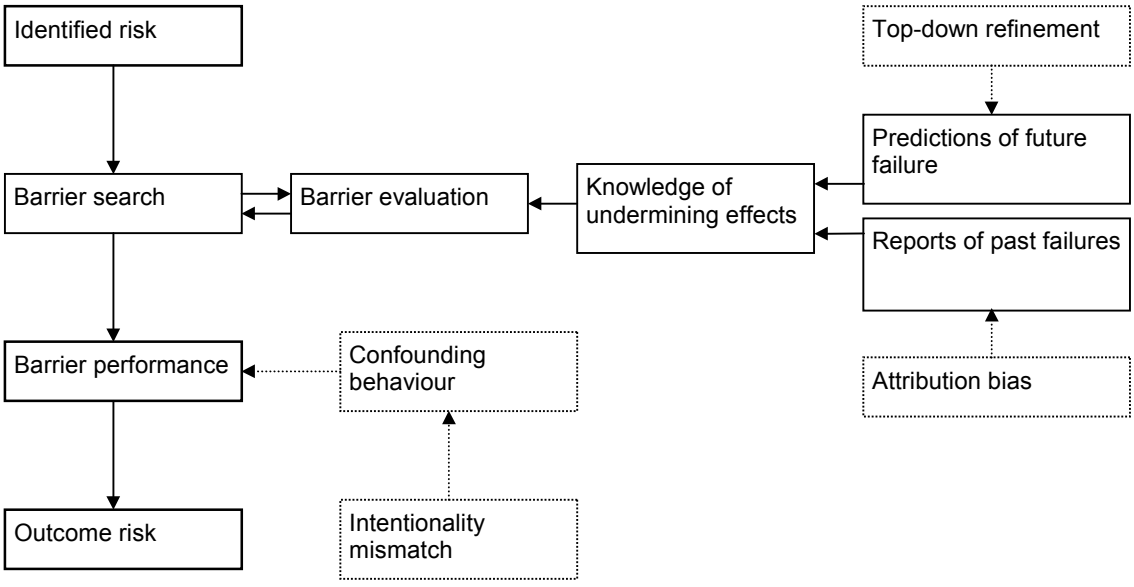

Figure 1. A model of barrier undermining

These effects will not apply to all designers and all operators on all occasions. Barriers more often than not do work. But it is important to acknowledge that it is possible to explain barrier failures in structural terms, and that it is not necessary to resort to criticising either designers or operators. There is nothing in Figure 1 that makes a person blameworthy – only vulnerable to the nature of situations, the natural pattern of work, and some psychological effects. Since

problems are explicable in terms of situations, remedies should involve people in understanding situations better, not requiring them to be better people.

5 Tool

One remedy to the barriers problem is to inform designers and operators more directly about how undermining occurs. We therefore developed a simple prompting tool that uses our analysis of how barriers fail. The tool can either be used as a look-up device or as a planning tool. For the former, the user works out how vulnerable a particular barrier is by using pick-lists to say what kind of source is closest to that of the barrier in question, and what kind of effect is closest. For example the source might be 'physical', and the effect might be 'separation'. If one separated fuel lines from hot manifolds as a barrier to an ignition hazard this would be a reasonable characterisation. The system then presents the user with the particular barriers of this kind that were found in our analyses, and says how these barriers were undermined in practice. As a planning tool, the system asks the user to write down all the barriers that are expected to be in place for a particular operation within a system. Again each barrier has to be characterised in terms of source and effect using pick lists. The system again shows users how such barriers can be undermined by referring to general phenomena and particular cases.

Thus the purpose of the tool is to support designers when they need to identify protective measures and then assess how effective the measures are likely to be. The outcome is purely qualitative, showing designers categories of protective measure and categories of undermining effect, but the identification of risks and risk reducing measures is an essential precursor to any quantitative assessment of a design and the risks to which it is vulnerable. Given that designers in the past have failed to identify some important risks and some important vulnerabilities, supporting these identification processes with this kind of tool appears worthwhile.

The tool has been evaluated informally by presenting it to staff in an engineering organisation in a different industry from the one in which the failures occurred (in aerospace), as well as presenting it to consultants and regulator in the offshore engineering industry. Their main reactions were as follows:

- It tackles a genuine problem. Designers often lack both the breadth of experience of failure, and the resources to needed to consult large numbers of failure reports. A tool that synthesises the lessons drawn from a large set of failures is an important one. Searching the accident reports used in this study alone would take far longer than using the tool.
- The notion of 'barriers' is an intuitive one, so an analysis process based on the concept is a reasonable one. The analysis needs to be appropriate to the expected hazard, however, so would only be justifiable, ordinarily, where intrinsic hazards exist in the design.
- Providing designers with knowledge of how barriers are undermined, rather than simply providing them with an analysis methodology, is important because there is a tendency to believe it is only the technical reliability of a barrier that is problematic. It is easy, for example, when providing an automatic cut-off device to consider its failure only from intrinsic loss of function – not from its interaction with other elements of the system.
- There is a difficulty in knowing how complete our analysis is, and how many cases would have to be incorporated before a reasonable level of comprehensive is achieved. The 'completeness' problem is a general one in risk analysis – and although tools that

synthesise historical experience can help designers to feel that their risk analysis is more comprehensive than not, it cannot provide any guarantees.

- Although it is possible to characterise barriers in terms of domain-independent sources and effects, these only become meaningful in particular domains. It is unrealistic, therefore, to think that a barriers analysis from one domain (such as offshore engineering) could be applied directly to another. The principle is transferable, but not the dataset. It would need an additional, parallel study to determine how generic a barriers analysis can be.
- The tool lacks a quantitative element that would help in the process of formal risk analysis. It gives no probabilistic information about the undermining effects that it describes.

6 Conclusion

The gist of the paper is that accidents occur despite the presence or possibility of barriers to them. It is possible to infer what undermines barriers from accident reports, and to characterise such barriers in terms of their source and their effect. Sometimes the failure to predict the undermining influences appears simply to be a matter of an operator or designer understanding too little about the nature of the hazard or the system. Sometimes, however, there is a more complex pattern where mismatches occur in the intentionality ascribed to barriers by designers and operators. There are some plausible, structural reasons why people do not always learn about these mismatches over time. The upshot is that barriers will not be as risk reducing as expected unless undermining phenomena are systematically considered, and it is even possible that barriers are risk amplifying. For instance, when protective redundancy is introduced in human systems the effect can be that everyone thinks someone else is performing a task and the task is completely neglected.

In a sense it is obvious that, in complex systems, barriers will fail for reasons other than intrinsic unreliability. It is obvious that they will sometimes be undermined by interactions with other parts of the system (especially human parts). Nonetheless, this undermining is apparently still not subjected to sufficient analysis. A recent example that we have been informed of is the use of high integrity protection systems (HIPS) in offshore technology. These essentially provide automated valves that interrupt flow from a well when the well pressure exceeds a certain level. This has allowed designers to specify smaller and cheaper pipes - pipes that can withstand less than the predicted maximum well pressure - and (in one case) run pipes inside a structural member. The argument is that a risk analysis shows, with the achievable level of reliability in HIPS, the effect overall is to reduce risk. Nonetheless, there have been some recent failures of these systems that appear to refute claims of very high reliability (or availability), so there must be some unpredicted phenomenon that is undermining whatever risk reducing strategies have been built into the designs. Moreover, the advocates of HIPS argued that their failure rates were much lower than conventional pressure relief valves. But this appears to have overlooked the fact that such valves often ‘failed’ by relieving at a higher than rated pressure – not by failing to relieve altogether. HIPS, in contrast, are likely to fail completely since they incorporate digital electronics and software. The implication of all this is that designers sometimes lack a sufficiently sophisticated understanding of barriers. However obvious the undermining phenomena are, they are not systematically considered during the design process

We also suggested that there was a particular difficulty to do with barriers that were undermined by mismatches in intentionality between designers and operators. One way of tackling this would be for designers to consult operators more intensively during the design process. But, typically, they are not always available when they are needed, and they often have their own, idiosyncratic preoccupations based on their personal (and not necessarily representative) experience. One design organisation we came across gave up consulting operators on control layouts because they all had different preferences, which were based primarily on what they happened to be used to. Problems of misunderstood intentionality also seem to occur in maintenance. A commonplace scenario reported to us by a regulator was that designers tended to assume that barriers would be de-activated for maintenance independently. They thus assumed that the probability that barrier X would be inoperative would be independent of the probability that barrier Y would be inoperative, so the probability of both being inoperative would be their product (a very low number). In practice, maintenance operations were often scheduled together, so that quite commonly X and Y would both be deactivated simultaneously, leaving the installation without defences. This is only one of several ways in which designers seem to overlook common cause and common mode failures. But it is an important example because it shows how the problem is not simply that the design fails, but that it fails to take account of the human responses it induces, which in turn contradict the assumptions on which the design rests. Predicting this is likely to be significantly harder than predicting direct physical failure.

Finally, it is worth pointing out some of the limitations of this study. First, the problems with relying on accident reports as a dataset are pretty obvious: people do not reconstruct the past accurately, they overestimate in hindsight what can be known from foresight, they suffer cultural and cognitive biases, and they have incentives to present the past in particular ways. This is all true *a fortiori* when dealing with failure and accidents. Second, the characterisation of barriers in terms of their source and effect provided what was essentially an engineering description, even when the barrier was provided by people. It was in other words a rationalisation, made from an external viewpoint (that is, the viewpoint of those conducting the study, not actors in the situations being studied), of how some entity or phenomenon could reduce risk through a clear causal mechanism. The idea that a barrier's effect could hinge on different interpretations of it – notably those of the designer and operator of the system in question – did not enter into the analysis. Third, the whole idea of undermining a barrier has connotations of subverting a system, of something in the operation of the system that detracted from the optimal, pristine reasoning of the system designer. Yet mostly the problem of barriers failing to arrest accidents arises from insufficient analysis in the design of the barrier. Often the designers' strategies look clumsy and blundering set against the subtlety of the ways people make these systems work, and this is particularly the case when it is some human action 'undermining' the barrier. It is a platitude to argue that designers should accommodate the qualities of human operators and users, but the platitude often implies a lack of capability on the part of operators. The reality is that it is operators' ingenuity and natural logic that is problematic in the context of poorly conceived barriers. For example, barriers sometimes confound people's reasonable intentions, like having to get access to a hazardous area to deal with a faulty or interrupted process. People sometimes then go to considerable lengths to circumvent such barriers. If they were not so ingenious in doing so the barrier would have its desired effect. It is only the operator's capacity for extemporisation that renders the designed barrier ineffective.

Fourth, the analysis removed the barriers from their context. Warning markers, to take an obvious kind of rather ineffectual barrier, are mostly ineffectual because people's attention-

directing strategies involve noticing differences in their environment, not the absence of differences. Warnings tend to become fixtures, and so, on this basis, quickly cease to attract attention. Moreover, warnings become subjects of ridicule because of their earnestness and stern-ness. It is socially acceptable and often socially laudable to make fun of them, or deface them. People are also very well aware that designers often provide warnings because they lack the imagination or resources to provide more effective ways of protecting people and systems from hazards. Such barriers are then regarded with cynicism, and once a device functions as an object of cynicism its function as a protective device is no longer provided. Another important aspect of the context that was neglected in the study was the prevailing culture, especially the culture of the hydrocarbons drilling industry which sees risk taking of a certain kind in a positive light. This is perhaps generally true of risks that are to one's own safety, that achieve productivity gains, that involve physical courage and so on. One has sympathy for a designer who is required to reduce risks when such a culture prevails, but the designer appears cynical who provides protective measures, anticipating they will be unused, simply in order to discharge his or her duties. Questions of this kind – designers cynically ignoring the culture in which their designs would be deployed, or simply being ignorant of it – did not enter into the study.

References

[1] Reason J., "Human Error", Cambridge University Press (Cambridge), 1990.

[2] Andrews J.D. and Moss T.R., "Reliability and Risk Assessment", Longman (Harlow), 1993.

[3] Norman D.A., "The Psychology of Everyday Things", Basic Books (New York), 1988.

[4] Svenson O., "The Accident Evolution and Barrier (AEB) model applied to incident analysis in the processing industries", Risk Analysis, Vol. 11, 1991, pp.499-507.

[5] Svenson O., Lekberg A. and Johansson A.E.L., "On perspective, expertise and differences in accident analyses: arguments for a multidisciplinary integrated approach", Ergonomics, Vol. 42, 1999, pp.1561-1571.

[6] Svenson O., "Accident and incident analysis based on the accident evolution and barrier function (AEB) model", Cognition, Technology and Work, Vol. 3, 2001, pp.42-52.

[7] Kecklund L.J., Edland A., Wedin P. and Svenson O., "Safety barrier function analysis in a process industry: A nuclear power application", International Journal of Industrial Ergonomics, Vol. 17, 1996, pp.275-284.

[8] Selig R., "Use of safety barrier diagrames in offshore QRA in Denmark", FABIG Newsletter of the Steel Construction Institute, Issue 31, January, 2002, pp.20-22.

[9] Kanse L. and van der Schaaf T., "Recovery of failures in the chemical process industry". In Harris D. (ed.), Engineering Psychology and Cognitive Ergonomics, Vol. 6, Ashgate (Aldershot), 2001, pp.323-332.

[11] Wilde G.J.S., "The theory of risk homeostasis: implications for safety and health", Risk Analysis, Vol. 2, 1982, pp.209-225.

[12] Grabowski M., Merrick J.R., Harrold J.R.., Mazzuchi T.A. and van Dorp J.R., "Risk modelling in distributed, large scale systems", IEEE Trans. Systems, Man, and Cybernetics, A, Vol. 30, 2000, pp.651-660.

[13] Fischhoff B., Lichtenstein S., Slovic P., Derby S.L. and Keeney R.L., "Acceptable Risk", Cambridge University Press.1981.

[14] Rasmussen J., "The role of error in organizing behaviour", Ergonomics, Vol. 33, 1990, pp.1185-1200.

[15] Kecklund L.J., Edland A., Wedin P. and Svenson O., "Safety barrier function analysis in a process industry: A nuclear power application", International Journal of Industrial Ergonomics, Vol. 17, 1996, pp.275-284.
[16] Vicente K.J. and Rasmussen J., "Ecological interface design: theoretical foundations", IEEE Trans. Systems, Man, and Cybernetics, Vol. 22, 1992, pp.589-606.
[17] Feldman, J.M., "Beyond attribution theory: cognitive processes in performance appraisal", Journal of Applied Psychology, Vol. 66, 1981, pp.127-148.
[10] Wagenaar W.A., Hudson P.T.W. and Reason J.T., "Cognitive failure and accidents", Applied Cognitive Psychology, Vol. 4, 1990, pp.272-294.

Corresponding author:
J S Busby
Department of Mechanical Engineering, University of Bath
Bath BA2 7AY
UK
Tel. +44 1225-826 588
Fax. +44 1225-826 928
Email j.s.busby@bath.ac.uk