Failure modes analysis of organizational artefacts that protect systems

J S Busby[1], **R E Hibberd**[2]*, **A R Mileham**[2] and **G Mullineux**[2]
[1]Department of Management Science, Lancaster University, Lancaster, UK
[2]Department of Mechanical Engineering, University of Bath, Bath, UK

Abstract: Designed systems inevitably rely to some degree for their protection on organizational artefacts. These are rules, procedures, instructions, authority structures and so on that are designed, like physical devices, but have organizational rather than physical functions. An analysis was conducted of maritime accidents to investigate how these organizational artefacts were implicated in failure, and a method was then developed to help system designers to perform a failure modes analysis of these artefacts. The proposal is that analyses of failure modes in physical devices should be accompanied by parallel analysis of failure modes in organizational artefacts.

Keywords: failure, failure modes and effects analysis (FMEA), accidents, risk, organizational factors

1 INTRODUCTION

It is almost never appropriate to concentrate solely on the failure of the technical elements of a designed system. The phenomena of risk compensation and risk homeostasis [**1**, **2**], for example, mean that there is a tendency for safety improvements to be nullified by adjustments in behaviour. Organizations routinely convert such safety gains into production gains [**3**], and their activities migrate towards the boundaries of safe operation under competitive pressures [**4**]. As the role of technical failures in the causation of accidents has fallen, the role of human and organizational factors has become more apparent [**5**]. Modern high-hazard low-risk systems are now primarily prey to organizational accidents [**6**]. Where attempts have been made to remove people from the system with increasing automation, the potential for failure has not been removed or even reduced; it has simply created new error pathway, and delayed opportunities for error detection and recovery [**7**]. Some commentators have suggested that risk is *always* underestimated because the methods used to estimate technical risk fail to acknowledge the organizational contribution to technical failures [**8**].

The purpose of the study described here is to extend the analysis of failure to the domain of human and organisational elements. A large amount of work has been done on human reliability assessment (HRA) [**9**] and its contribution to risk analysis. HRA is concerned primarily with the behaviour of individuals and their errors. However, our interest was in the organizational aspects of failure and, in particular, organizational artefacts. These are entities that are designed, in the same way that technical devices are designed, but have organizational rather than physical functions. They are typically used to protect systems when it is not feasible or cost effective to use technical measures. For example, operating procedures, codes of practice, rules of engagement and authority structures that define who has responsibility in particular situations are all organizational artefacts. Since they are often as important as technical devices in maintaining safety, they need to be analysed in parallel with the technical devices whenever a designer is conducting a risk assessment or failure analysis.

An obvious candidate approach is to extend the use of failure modes and effects analysis (FMEA). FMEA is essentially a decompositional process, breaking a system down into its parts, asking how the parts can fail and what the causes, consequences and criticality of the failures are. It has been criticized on various grounds, such as its neglect of interactions between parts [**10**], but continues to be widely used. The difficulty in applying FMEA to organizational artefacts lies in the fact that such artefacts do not fail in a way that is analogous to technical artefacts. They are not physically destroyed or degraded in a way that intrinsically undermines their function. Instead, they fail because their actions are undermined in the larger system of which they are a part.

The MS was received on 23 February 2004 and was accepted after revision for publication on 6 May 2004.
**Corresponding author: Department of Mechanical Engineering, Faculty of Engineering and Design, University of Bath, Bath BA2 7AY, UK.*

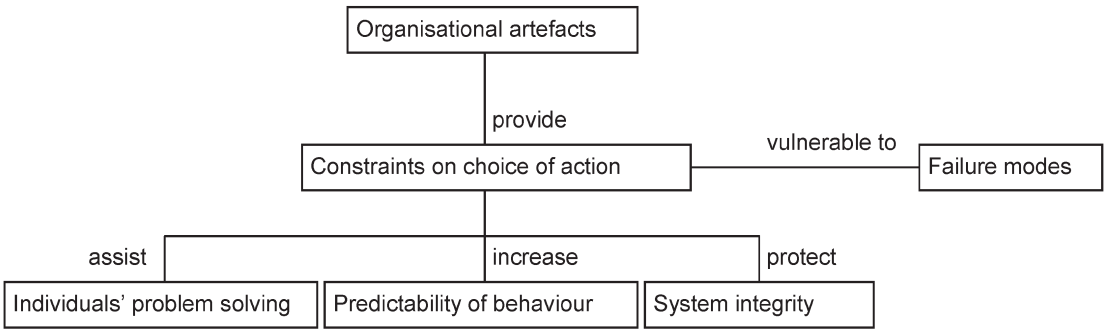

Fig. 1 Model used in the analysis

What has been attempted in this study is, firstly, to analyse just how this failure with organizational artefacts occurs in practice and, secondly, to develop a process that is as close as possible to FMEA but takes account of the intrinsic differences between technical and organizational artefacts. This has been undertaken in the particular context of the maritime industry.

2 ANALYSIS OF FAILURE IN PRACTICE

The first stage of the work involved an analysis of accidents in the maritime industry, to identify how organizational artefacts that protect systems fail in practice. This was based on analysing a secondary data set, consisting of accident reports published by the UK Marine Accident Investigation Branch (MAIB). The model that underlies the analysis is shown in Fig. 1. It is based on the principle that organizational artefacts provide constraints on people's actions. For instance, traffic rules constrain manoeuvres to be of particular kinds, operating instructions constrain operations to take place in a particular sequence and so on. These constraints help the people in the system by narrowing down the choices that they have to make, by making people's actions more predictable to other people in the system and by protecting the integrity of the system by constraining activity to just that of non-hazardous kinds. For example, it can be very helpful on the high seas to provide traffic rules that mean a master does not have to make complicated calculations of what another master in the vicinity is going to do. He or she can simply adhere to the rules but, when also constrained by a schedule and operating in crowded seas with various topographical constraints, the situation can become overconstrained and the rules can become a source of problems rather than benefits.

The accident reports published by the MAIB over the past 3 years were each assessed to determine whether an organizational artefact of some kind had been implicated

Table 1 Types of artefact identified in the analysis

Type of artefact	Example of constraint	Example of failure mode
Rules and requirements	Constraining other peoples behaviour to predictable kinds	Being laid aside when people are faced with more pressing constraints or reduced resources
Rights and precedences	Constraining the need to negotiate with others	Having weak moral authority means the constraints lack force
Marks, warrants, warnings, notices and indicators	Constraining behaviour to avoid hazardous actions	Giving people unwarranted confidence when mark of assurance mistakenly applied
Checking and verification systems	Constraining the consequences of error	Providing insufficient information to the checker about intentions
Operating procedures, codes and instructions	Constraining actions to take place in a necessary sequence	Failing to specify whether sequences are arbitrary or necessary and so encouraging people to rearrange sequences to minimize effort
Communication channels, devices and protocols	Constraining uninformed activity	Giving the misleading appearance of being heeded
Authority structures, roles and jobs	Constraining the boundaries of what people have to think about	Being arbitrary, so providing an insufficient basis for prediction
Maps, charts, radar and other representations of the physical world	Constraining movement in hazardous regions	Being over-relied on—because it involves less effort or because it allows operators to blame the representation or device
Plans, schedules and intentions	Constraining actions to those agreed upon and consented to	Becoming an excessive constraint on people in situations where improvization is needed
Records and traces	Constraining remembered states or conditions to those that occurred	Being neglected where there is no expectation of any future need
Cultural and moral conventions and assumptions	Constraining people to making similar assumptions	Not being shared by the complete constituency of the organization

and whether the manner of the failure was clear from the report. This was the case in 35 of the 216 reports collected. Each report was then analysed by identifying the artefact in question, the constraints that it was meant to have provided and the manner in which these were undermined. The artefacts were grouped into a set of basic types. Table 1 shows the types of artefact that were identified in this analysis, together with examples of the failure modes associated with each type.

It is important to say that, because the sample is limited, the results are not comprehensive. Moreover, some of the failure modes shown against certain types of artefact are not exclusive to those types. For example, the failure mode in which a rule or regulation is set aside when the situation becomes overconstrained could apply to any organizational artefact and not just rules and regulations.

3 PROPOSED METHOD OF FAILURE ANALYSIS

The previous analysis gives certain clues as to what an FMEA, or similar method, applied to organizational artefacts should look like:

1. It should be concerned with identifying system failure, and not component failure, although specific components can be used as a point of entry to the analysis.
2. It should be based on understanding the constraints that artefacts provide, and the manner in which these constraints can be rendered ineffective.
3. It should be systematic because people need to have some confidence that the analysis is comprehensive—that when the analysis finishes there is not a large number of failure modes that have gone undetected.
4. The results shown in Table 1, although incomplete, provide prompts and reminders when trying to identify failure modes. It may not be obvious, when looking at a particular organizational artefact, how its constraints can fail. The knowledge of these failure modes, distilled from past failures, can help to support the process.

Two versions of a method for analysing failure modes arising from the use of organizational artefacts have been proposed. The first of these employs a typical FMEA methodology to the assessment of the failure modes of individual organizational artefacts. The second method, which arose as a result of perceived weaknesses in the first, focuses on the analysis of specific tasks and the manner in which organizational artefacts can fail to support the completion of these tasks.

3.1 First version of the method

In the initial version of our organizational artefact FMEA, an attempt was made to modify the FMEA methodology as little as possible, but enough to take account of the essential qualities of organizational artefacts:

1. The first step is to bound the system being analysed. This is inevitably artificial but seems inevitable. For example, in the maritime case the system could consist of a specific vessel.
2. The second step is to decompose the system into its components. In this case, these are organizational artefacts of the kinds shown in Table 1. As with FMEAs of technical systems this can be done gradually, over successive hierarchical levels. Thus, for example, the collection of organizational artefacts could be divided according to categories such as those indicated in Table 1. They could be further subdivided according to the main physical subsystems of the system in question.
3. The third step is to identify the constraints that these artefacts provide.
4. The fourth step is then to identify ways in which the constraints could become inoperative.
5. Further steps can be similar to those of standard FMEAs, tracing the causes and consequences of failure, and perhaps adding a numerical index such as a 'risk priority number'.

This approach is similar to conventional FMEA in that the way into the problem of analysing risk is by decomposing the system into elements. However, FMEA is essentially about looking at how those elements fail intrinsically, and then asking about the causes and consequences of this failure. An organizational FMEA has to look at how the constraints provided by the elements lose their effectiveness and not how the elements degrade or disintegrate in themselves. Thus the idea of 'seeding' the risk analysis by starting at a component level is similar, but the identification of failure modes has a different basis.

3.2 Second version of the method

The main problem with the first method is how the system is broken down into components. A physical or technical system has a basic integrity that makes this relatively straightforward. A vehicle typically has a drive-train, a containment structure, a control system and so on. A drive-train might have an engine, a transmission and so on. On the other hand, a system's organizational artefacts are often afterthoughts and do not themselves have a complete consistent logic. The physical parts of a vehicle belong together in a complete assembly, but the rules for driving the vehicle, the procedures for maintaining it, the authority structure for the command of the vehicle and so on are often just accumulated as additions to the technical system. This means that simply writing down organizational artefacts as components of a system is

harder and more prone to omission. An alternative 'way in' to the problem is, instead of starting with a structural view and breaking it down into components, to look at the activity or process performed by the system. This leads to a second method:

1. Again the first step is to bound the system, e.g. a specific vessel.
2. The second step is to identify the principal processes performed by the system, including, for instance, entry into a port.
3. The third step is to identify the preconditions for the processes to be functional and safe. This might need to be done successively over several levels. Plainly, preconditions of entry into port are that the vessel does not capsize, does not collide with other vessels, does not collide with land and so on. A precondition of avoiding collision with other vessels is that its intentions are known to these other vessels, that the other vessel's intentions are known to it, that their respective positions and paths are observable and so on.
4. At some point these preconditions become constraints that are provided by artefacts. The fourth step is to identify these constraints and artefacts.
5. The fifth step is again to identify potential failure modes, i.e. ways in which the constraints provided by the artefacts can be made ineffective.

3.3 Brief case application

Space precludes a detailed case study, but the following brief application illustrates the principle of the first method (which suits the simple nature of the system in question). Table 2 shows the example, namely a small piece of equipment that is added to an existing vessel, with two associated organizational artefacts (an operating procedure and a tag). It excludes, for each failure mode, the more detailed analysis of cause, consequence and so forth that would be normal in an FMEA.

The example is very limited but shows that the principle of analysing organizational artefacts in terms of the constraints that they provide is potentially a helpful way of being systematic about thinking through potential failures. It also shows how ineffectual social or organizational constraints can be, in contrast with physical constraints. They are easily undermined when they do not make sense, when they obstruct people in normal tasks and when they are essentially afterthoughts in the design process.

4 DISCUSSION

It seems clear from the analysis of historical failures, that organizational elements, and organizational artefacts in particular, contribute to risk and yet are almost universally relied on to some extent to protect designed systems from failure. This means that any technical risk analysis needs to be accompanied by an organizational risk analysis. Applying a technique such as FMEA directly, however, does not work well because organizational artefacts do not fail in an analogous way to physical devices. A more appropriate form of analysis is to identify the constraints that these organizational artefacts provide, and then to identify ways in which the constraints can become ineffective during the operation of the system.

It became evident that there were different ways of modifying the FMEA methodology to deal with organizational artefacts. One approach was based on the principle of simply enumerating all the artefacts there were in a system, examining their constraints and then identifying the failure modes. An alternative approach was based on decomposing the processes performed by a system, rather than decomposing the structure of a system. The preconditions required for these processes are then identified, and the constraints and artefacts required to maintain these preconditions are generated. At this point, the failure modes can again be considered.

Table 2 Example

Description	Additional equipment consisting of a hydraulic ramp. This requires the manual insertion of a locking pin when the ramp is raised. This pin is one of several, but the other pins are semipermanently installed as they hold the ramp assembly. The locking pin is not visible from the ramp controls and so a tag is provided to enable the person inserting or removing the pin to show the pin's status	
Organizational artefact	Intended constraint	Failure mode
Procedure stipulating use of locking pin after raising ramp	Constrain operation to correct operating sequence; constrain device to safe states	Modifying the stipulated sequence if it appears to be arbitrary Lacking the knowledge needed to execute the sequence properly; not distinguishing the locking pin from the other pins could lead an operator to believe the pin was engaged Failing to provide specific cues; the operator may simply forget to insert the pin since there are no direct cues and insertion of the pin requires an additional step to the necessary operating sequence
Tag repeating status of locking pin	Constrain operator's knowledge of pin status to actual status	Giving undue confidence when the indication is incorrect; the operator inserting or removing the pin may set the tag first and be interrupted before dealing with the pin itself

It is difficult to say which of these alternatives is a better method, since it depends on circumstances how well all the organisational artefacts deployed in a system can be simply enumerated without thinking about processes and preconditions.

ACKNOWLEDGEMENTS

This work has been funded in part by the Engineering and Physical Sciences Research Grant GR/R 7507. Many thanks are due to Edmund Hughes and Keith Tatman of the MCA and to Debbie Lucas of HMRI, for their insight and comments on the work. Thanks are also due to the anonymous reviewers for their helpful comments.

REFERENCES

1 **Adams, J.** *Risk*, 1995 (UCL Press, London).
2 **Wilde, G. J. S.** The theory of risk homeostasis: implications for safety and health. *Risk Analysis*, 1982, **2**, 209–225.
3 **Reason, J.** *Managing the Risks of Organizational Accidents*, 1997 (Ashgate, Aldershot, Hampshire).
4 **Rasmussen, J.** Risk management in a dynamic society: a modelling problem. *Safety Sci.*, 1997, **27**, 183–213.
5 **Evan, W. M.** and **Manion, M.** *Minding the Machines. Preventing Technological Disasters*, 2002 (Prentice-Hall, Upper Saddle River, New Jersey).
6 **Reason, J.** The identification of latent organisational failures in complex systems. In *Verification and Validation of Complex Systems: Human Factor Issues* (Eds J. A. Wise, V. D. Hopkin and P. Stager), 1992 (Springer-Verlag, Berlin).
7 **Lutzhoft, M. H.** and **Dekker, S. W. A.** On your watch: automation on the bridge. *J. Navig.*, 2002, **55**, 83–96.
8 **Vaughan, D.** Autonomy, interdependence, and social control: NASA and the Space Shuttle Challenger. *Admve Sci. Q.*, 1990, **35**, 225–257.
9 **Kirwan, B.** The validation of three human reliability quantification techniques—THERP, HEART and JEDI. Part 1: technique descriptions and validation issues. *Appl. Ergonomics*, 1996, **27**, 359–373.
10 **Ansell, J.** Reliability: industrial risk assessment. In *Risk: Analysis, Assessment and Management* (Eds J. Ansell and F. Wharton), 1992 (John Wiley, Chichester, West Sussex).