Design for Excellence: Engineering Design Conf. pp 431, held 27-29 June 2000 at Brunel University UK.
Orgnised by IMechE. Edited by S. Sivaloganathan and P. T. J. Andrews.

Human error in the engineering design process

J S BUSBY
School of Industrial and Manufacturing Science, Cranfield University, Bedford, UK

ABSTRACT

A study was conducted of human error in the engineering process of 5 organisations that designed industrial equipment. Approximately 150 errors that had taken place were analysed individually and then coded according to the particular design activity that failed. Modes of error that were common to error in different activities were then identified. Among the primary modes of error were cases where designers failed to elicit the constraints and requirements presented by the outside world, but did so because they had fallacious beliefs that were nonetheless reasonable inferences from limited historical experience. Error was also associated 1) with the emergence of latent constraints when scaling up a design, 2) with refining designs that made them vulnerable to uncertainties in the external world, 3) with modifying existing designs whose rationale was obscure, and 4) with design tools which provided inadequate feedback for users learning by trial and error. The most promising way of reducing error may be to make designers more knowledgeable about the types of error accompanying different activities.

INTRODUCTION

Studies on the cognitions of individual designers point to a number of limitations in designers' reasoning. These include satisficing, where designers concentrate on a single and usually sub-optimal solution(1), plan deviation and abandonment(2), inflexibility in relinquishing a kernel idea once it becomes established(3), and forgetting(4). Once, however, designers become part of an organised, collective process there are more possibilities for error correction and, equally, more possibilities for failures in coordination. Various taxonomies have therefore been proposed for error in engineering design - based for example on the activities in which they occur, the objects they affect, and the ways in which communication can fail(5). There have also been some case studies of engineering design error (6)(7), and some accounts of

major engineering failure(8) which point to typically troublesome characteristics of designing, such as the ramifications of putting a well-developed design in a new environment. Error in the design process has also been tackled in civil, as well as mechanical, engineering design - again with error taxonomies, case studies and analytical models (9)(10)(11)(12). And there is, of course, research on human error generally in the psychology and systems science communities(13)(14), although this has mainly been concerned with human error in organisations that perform real-time operations such as the control of industrial plant. The purpose of the study described here was to investigate systematically a moderately large number of errors in the engineering design process specifically. A fuller account of the study can be found elsewhere(15).

METHOD

There were 2 phases of data collection. The first involved 4 design organisations supplying industrial equipment, ranging from devices through to production lines. Accounts of specific error episodes were collected via 1) semi-structured questionnaires and 2) observations of post project review meetings. In the questionnaires, informants were asked to recount particular errors, explaining their causality and their consequences. The second phase involved unstructured interviews in an organisation that designed capital plant. Informants were again asked to describe specific errors, and explain their causality. All episodes were then represented as causal trees and categorised according to the activity that failed. Comparisons were then made between the errors brought together under the same activity heading, and modes of error that extended across the different activities were identified. There are clearly problems in relying on self-reports, but this tends to be the normal way of getting data on human error since it is often impossible to know when in advance to observe a process so as to observe an error directly.

RESULTS

Of the 156 episodes, 147 allowed satisfactory analysis and Table 1 shows how they were categorised by activity. The classification was derived inductively.

Table 1 Types of design activity that failed

Activity type	*Description*	*No. cases*
Adherence to standard	Designing by employing a predetermined, standardised design in a particular application	1
Allocation of subtasks*	Decomposing the design task and allocating subtasks to other participants in the design process	8
Analysis of constraints	Analysing available information about constraints to determine design characteristics	4
Attention to information	Attending to all relevant pieces of information when embarking on or returning to a design	7
Attribution of practices*	Attribution of practices to other participants in the design process	3

Envisaging of usage	Thinking about the demands that will be made on the design	18
Formulation of assumptions	Deciding on your design premises in the absence of complete information	12
Implementation of consistency*	Making a design consistent with the artefact in its actual condition	12
Inference of behaviour	Drawing conclusions about its behaviour from a design or from data on a design	3
Integration of subdesigns*	Making parts of a design into a coherent whole when bringing them together	8
Judgment of performance	Judging whether a determined design will meet certain performance criteria	3
Modification of scale	Determining or changing the scale of a design	4
Planning of resources*	Allocation of resources to a forthcoming design task	6
Reconnaissance of needs	Seeking information about the requirements of the world at large that will be relevant to design	11
Refinement of predecessor	Improving on an existing design to make its performance better generally	8
Replication of predecessor	Reapplying an existing design without modification	11
Specialisation of function	Modifying a generalised design to make it suit a specific application	1
Statement of specification*	Stating some required characteristic of a design to others	3
Substitution of elements	Changing elements of a design for another application to suit a new application	23
Transcription of information*	Copying elements of one design to a different medium	1

A description follows of the ways these activities failed *except* (since space is limited) for the 3 activities where there was only one error, and the 6 activities - asterisked in Table 1 - that are managerial in nature. Again, a fuller analysis is given elsewhere(15).

Analysis of constraints

There were 4 cases involving failure in the analysis of constraints, but only 3 distinct modes of failure:

- Performing a wrong step in the analysis.
- Believing that steps had been taken which in fact had not.
- Forgetting to take account of all the relevant entities in the analysis.

One of the errors also illustrated how checking can fail. A designer was sizing the quench liquid need in a catalytic cracker, and took account of the vapour flow needing quenching but not the catalyst. As a result the sizing was wrong by a factor of 2.2. The checker found the discrepancy, but because it coincided with the conversion rate for kilograms to pounds he attributed it to a conversion slip on his part rather than the original designer's error. Checking thus relies not only on detecting a discrepancy but also on making the correct attribution.

Attention to information

There were 7 cases and 2 main modes of error that involved attending to information:

- Designers failing to attend to information that was present. For example, a designer failed to realise that a reboiler circuit's function was a cue to avoid pockets in the lines. He incorporated pockets in order to simplify line routeing, and later had to rework the design.
- Designers had become used to relying on information that was not on this occasion present. For example, a designer habitually relied on others to specify operating limits as a cue to incorporate a device for detecting that operation of the artefact was imperilled. When these limits were not specified, the designer forgot to incorporate such a device.

It seems to be the case that, in complex design processes which deal with complex artefacts, designers rely heavily on the environment to remind and guide them in their actions.

Envisaging of usage

There were 18 cases of this kind, with 2 main modes of error:

- Failing to envisage the problems with the design incurred by people downstream in the delivery process (such as production or installation staff);
- Failing to envisage the problems with the designed artefact incurred by people operating and maintaining it.

Some of these errors involved what were essentially second order effects. For example, in one instance, the designer had anticipated a usage problem that actually occurred (short circuiting a transformer winding to ground) by designing a frame to withstand the resulting forces. His or her error was in developing a design whose performance under short circuiting was very sensitive to precise assembly, yet made precise assembly virtually impossible.

Formulation of assumptions

There were 12 errors involving assumptions, both about the designed artefact, and about the design process. There were 4 modes of error:

- Assumptions that the future would, by default, be like the past.
- Assumptions that were apparently as good as any other, in the absence of definitive information about some constraint, but in fact were not met.
- Assumptions made while waiting for information which the designer failed to revisit when the information became available.
- Assumptions which, as point estimates, were as good as any other but were less robust. (For example, a designer assumed a crane's 2 motors would never operate simultaneously, but this assumption turned out to be unwarranted. It was of course the less robust assumption, in the absence of knowing one way or the other.)

Inference about behaviour

There were 3 cases and 2 modes of error to do with the way designers made inferences about how the designed artefact would behave in operation:

- Inferring wrongly that the satisfactory operation of a prototype implied a successful product in full production.
- Inferring wrongly the rationale of a design prepared by another designer. In one case, the original designer did not want others to reuse his design without repeating the calculations that underlay it, so he removed detailed information such as line dimensions. Unfortunately, designers often used detailed information to infer the rationale of a design element (for example, using line sizes in order to infer the line's function).

These two types of error appear to be quite different. The first, in which the designers were insensitive to sampling variability, seems to be a basic limitation of human psychology. The second, in which design rationale can be hard to infer from a design, is more a characteristic of designs themselves, and the complex mapping between functions and embodiments.

Judgment of performance

All 3 cases of error in the judgment of how a design would perform in service were of a similar type, involving a judgment of the risk of some failure. One, for example, was a design that involved a very marginal pressure balance which, in the event, fell on the unfavourable rather than the favourable side. It is perhaps significant that all the errors involved reasoning about uncertainty, margins and risk - not about average performance in average conditions.

Modification of scale

There were 4 cases and 2 distinct modes of error to do with changing the scale of a design. Both modes essentially involved failing to realise that a small, quantitative change in the performance requirement would require a disproportional degree of effort:

- Emergent constraints ruling out the known solution principle. For example, a small increase in the required performance of a cambox took its size just outside the available envelope. As a result a completely different solution principle was required.
- Discontinuities in the available sub-designs leading to large scale changes. For example, a small increase in operating pressure took the instrumentation on an existing circuit design outside its operating range. The instrumentation therefore had to be doubled up and the circuit entirely redesigned.

A lack of scalability also limits reuse because it makes unpredictable the extent to which one can use a past design in a new application where the scale is only slightly different(16).

Reconnaissance of needs

There were 11 cases and 4 modes of error involving designers determining requirements:

- Designers believing it was unnecessary to elicit a particular requirement directly. For example, a designer believed he could determine a valve size from the size of the line in which it was installed. He did not know that the line size in the immediate vicinity of a control valve could be greater in order to withstand the possible hazard of the check valves surrounding the control valve being inadvertently left closed. He had not learned this from experience because normally clients specified minimum control valve sizes explicitly.
- Designers wrongly taking a piece of information as a signal that they need not establish requirements more definitively. For example, a designer failed to find out the implications on his design of there being carcinogens in the feedstock because only trace quantities of carcinogens were specified and he assumed that trace quantities would not be harmful.
- Designers becoming habituated to a particular requirement and failing to determine in new projects whether it still held.
- Designers failing to determine who they should communicate changes in the design to, because the changes (from their perspective) were very slight.

Generally, people failed to elicit requirements because of mistaken beliefs, not forgetfulness or time pressure. These beliefs arose quite logically from unrepresentative experiences.

Refinement of predecessor

There were 8 cases and 4 modes of error made in the process of refining a preceding design:

- Failing to understand the rationale of an existing design and making misguided improvements. In one case a surface had 2 functions (one to orient the artefact, one to trigger a detecting device). A designer who attempted to modify the design identified the first function and failed to search for any further function. His modification provided the first function but failed to provide the second - which led the artefact to fail.
- Failing to anticipate the consequences of a reasonable improvement. For example a designer attempted to improve an existing design by modifying the operating principle that limited its performance, but in doing so generated intractable side-effects.
- Failing to iterate sufficiently to make the refinement satisfactory - typically because an unexpected amount of effort was needed to carry the refinement through.
- Optimising a sub-design with the result that it was not robust to changes in related sub-designs. In one organisation it was the practice to provide structures with greater than optimal material content not only to provide safety margins but also to provide some margin in the case of small design changes in the surrounding equipment. The designer, who was new to the organisation, did not know this.

Designers are often criticised for failing to refine existing designs, but plainly this refinement is a source of error and, for the design organisation, risk.

Replication of predecessor

There were 11 cases and 5 modes of error in the process of simply replicating a past design:

- The replication of existing designs in new applications in which they failed. One case involved unexpected torsional vibration in a new application where loads were different.
- The replication of designs that were flawed. In one case a design was still being developed in order to eliminate pressure pulses that were preventing satisfactory calibration: a designer replicated this design not knowing it had not been fully developed.
- The use of a generalised template that was flawed.
- The use of a 'typical' or indicative design in order to proceed with a related design as though this were a finalised design.
- The inappropriate use of a design tool during replication. There was a case where a designer was trying to replicate a sub-design in his CAD model. He had turned off the layers into which he was trying to copy the sub-design so believed the replication had failed. He re-tried the operation, but then attributed the problem to a software fault.

Substitution of elements

There were 23 cases and 6 modes of error in the process of substituting one element in a design for another:

- Lapses, where an intended design action had been planned but not executed because the designer forgot, typically after being interrupted.
- Encapsulation problems, where an unexpectedly high effort had to be made to substitute for the same element many times throughout a design. For example, in one case the same paint specification had to be modified on every one of several hundred detailed designs when the specification changed. It would have been better to put in a reference on every design to a single document which contained the specification.
- Failures to see the ramifications of substituting one element for another. For example, a designer did not predict that a new fluid type entailed changing the seal design in a pump.
- Omissions where the designer relied on external cues. For example, a designer forgot to include air dry-up connections in a design because he was reusing an existing design

whose client happened, unusually, to have a code which stipulated that such connections were not to be shown on designs.

- Failing to consult others who one does not know could tell one of problems when making a substitution.
- Errors in using design tools to substitute one element for another. One, for example, occurred when the designer did not know a CAD system had a special deletion operation. He used the operating system to delete a graphics file but was unaware that this was associated with a database entry, which led to anomalous behaviour downstream.

CONCLUSIONS

Many errors had to do with designers knowing what the world required of a design. There were problems with designers failing to envisage how others would use a design and problems to do with the process of eliciting others' requirements. Often this kind of failure is put down to designers' unwillingness to engage with others, or their desire to avoid over-constraining the design problem. The errors analysed here suggested that it arose from incorrect beliefs - but beliefs that were logical given the designers' experience. It can be hard for designers to know just how idiosyncratic their experience is, and one suspects that most people think of their experience as more representative than it actually is.

Error also arose in connection with 'scalability' - the extent to which the scale of a design that uses a given solution principle can be changed without some kind of loss. A typical error occurred when a designer reused an existing design in an application where there was a small increase in performance. This required a roughly proportionate change in spatial dimension, but this then infringed the available envelope - so a new solution principle had to be sought. The result was a grossly disproportionate amount of design effort. Planning a design activity in these circumstances becomes difficult, because the constraints that cause discontinuities like this are latent. The designer does not attend to them because he or she has become conditioned to believe they are irrelevant since, up to that point, they were.

Design rationale was connected with errors under several of the headings. Some were to do with one designer believing he understood the rationale of another's design feature when he found a function that it performed (not realising it also performed other functions). Some arose where a rationale was obscure so a designer removed a feature that turned out to be needed. Most past research on rationale is probably about good ways of recording rationale, and in some cases about making it easier to record rationale. But these errors suggest that what we need to know more about is how designers *impute* rationale when it is not explicit.

A further theme is refinement. Satisficing is typically seen as a flaw in designers' reasoning, and designers are criticised for failing to refine their designs when there are obvious opportunities for refinement. The errors that were analysed in this study suggest that refinement, in reality, can be a costly and error-prone process. It is not just the risk of extra effort on the designer's part that is hazardous in refinement activity but the effort that the designer commits the rest of the organisation to.

Finally, there were errors to do with learning how to use design tools effectively because of users' attribution bias. These errors involved users doing things that led to later problems, but

users then attributing the failure to the system rather than their own prior actions. It is not a great insight that if you attribute errors to a tool you will fail to learn how to use it effectively. And the nature of the tools encouraged such attributions: trouble can be expected when there is a specialised operation (like deletion) which operates differently from the default operation that an unknowledgeable user is likely to revert to. Thus, indirectly; design tools predispose people against learning how to use them.

REFERENCES

(1) Ball LJ, Evans JStBT, Dennis I (1994). Cognitive processes in engineering design: a longtitudinal study. *Ergonomics* **37**, 1753-1786.

(2) Colgan L and Gobel M (1993). Towards a cognitive model of circuit design. *Environment and Planning B: Planning and Design*, **20**, 321-332.

(3) Condoor SS, Shankar SR, Brock HR, Burger CP and Jansson DG (1992). A cognitive framework for the design process. *Proc. 4th Int. Conf. Design Theory and Methodology*, Scottsdale (Ariz.), 13-16 September, 277-281.

(4) Dwarakanath S and Wallace KM (1995). Decision-making in engineering design: observations from design experiments. *Journal of Engineering Design*, **6**, 191-206.

(5) McMahon CA, Cooke JA and Coleman P (1997). A classification of errors in design. *Proc. Int. Conf. Engineering Design ICED97*, Tampere, 19-21 August, 119-124.

(6) Hales C (1995). Five fatal designs. *Proc. Int. Conf. Engineering Design ICED95*, Prague, 22-24 August, 662-667.

(7) Petroski H (1991). Paconius and the pedestal for Apollo: a case study of error in conceptual design. *Research in Engineering Design*, **3**, 123-128.

(8) Whyte RR (ed.) (1975). *Engineering Progress Through Trouble*. Institution of Mechanical Engineers (London).

(9) Blockley DI (1977). Analysis of structural failures. *Proc. Inst. Civil Engineers Part 1*, **62**, 51-74.

(10) Brown CB and Yin X (1988). Errors in structural engineering. *Journal of Structural Engineering*, **114**, 2575-93.

(11) Petroski H (1994). *Design Paradigms. Case Histories of Error and Judgment in Engineering*. Cambridge University Press (Cambridge).

(12) Stewart MG (1992). Simulation of human error in reinforced concrete design. *Research in Engineering Design*, **4**, 51-60.

(13) Rasmussen J (1990). The role of error in organizing behaviour. *Ergonomics*, 1990, **33**, 1185-1200.

(14) Reason J (1990). *Human Error*. Cambridge University Press (Cambridge).

(15) Busby JS (in press). Characterising failures in the process of design.

(16) Busby JS (1999). The problem with design reuse: an investigation into outcomes and antecedents. *Journal of Engineering Design*, **10**, 277-296.