

The Psychology of Errors in the Engineering Process

"Sed quis custodiet ipsos Custodes?"

Robert Collins
Sentient Systems Limited
1 Church Street, Wimborne,
Dorset, BH21 1JH

Bridget Leathley
Four Elements Limited
Greencoat House,
Francis Street,
London, SW1P 1DH

ABSTRACT

This paper is about errors in the engineering process. In particular it considers the psychological mechanisms that may cause engineers to make mistakes, or at least make them more susceptible to error. The paper is particularly concerned with the safety of systems and hence the manner in which errors in the engineering process can lead to incidents, accidents and disasters.

A number of case studies highlighting errors in analysis are presented and these are evaluated with respect to cognitive and social-psychological error mechanisms. An overview of the field of cognitive and social psychology as it relates to errors in the engineering process is provided.

The final section of this paper introduces a variety of techniques from other fields of study, aimed at overcoming the problems associated with the aforementioned predispositions to error.

An annotated bibliography of works on psychology suitable for engineers new to this field and case study material of engineering errors is included.

1 Why Should Engineers Study Psychology?

This paper is about errors in the engineering process. In particular, it considers the psychological mechanisms that may cause engineers to make mistakes, or at least make them more susceptible to error. The paper is particularly concerned with the safety of systems and hence the manner in which errors in the engineering process can lead to incidents, accidents and disasters.

The ideas presented here have much in common with those ideas concerning the errors made by operators of complex systems, the subject area of 'Human Factors', or 'Man-Machine Interface' (MMI) design. But this paper considers a different set of activities to those of system operation. This paper deals with the activities of engineers and designers as they go about developing the equipment and systems that others will use. It is not too surprising that many of the explanations of human behaviour provided by psychologists and human factors experts can be applied to

understanding errors in the engineering process, since engineering is a uniquely human activity.

Although we may rely on complex mathematical models, computer simulations, experimental tests of mechanical parts and our understanding of physical laws to explain the behaviour of systems or processes, nevertheless we suffer from human fallibility in our efforts. Mathematical models have to be created and then applied by humans. Computer simulations must be produced, populated with data, operated and observed by humans. Experimental results have to be processed and interpreted by humans. Physical laws must be understood and applied correctly. And for each of these, results must be communicated and understood, and on the assembly of evidence, decisions must be made by fallible humans.

At each stage of this human process is an opportunity for error. With each error comes an opportunity for failure, and with each failure comes the possibility of disaster. This paper considers the mechanisms of human error as they may occur in the engineering processes with the intended purpose of trying to improve those processes.

We think that this is an important task considering the comments of one of the most eminent authorities on human errors. Reason has compared the relative importance of system design compared with 'operator error' as a cause of accidents:

"Rather than being the main instigators of an accident, operators tend to be the inheritors of the resident 'pathogens' created by poor design, incorrect installation, faulty maintenance and bad management decisions"

(Reason 1988)

Our contention is that the field of psychology has much to offer the engineering profession in this respect. Although we include in this the type of specific design input that human factors experts and ergonomists may provide, we are particularly concerned with contributions to the process of engineering. We believe that a great deal of information already exists within the psychology literature that could be used to improve the way in which we conduct our business, and yet that this information seems to be acted upon only seldomly.

If, as it has been suggested, there is some psychological predisposition to errors in engineering processes then we must understand those predispositions (Collins and Leathley 1994). If such predispositions can be characterised then there may be an opportunity to avoid them, or to contain the damage that may arise from them. In the parlance of traditional reliability and safety analysis, if the failure mode is known, then there is an opportunity to employ error detection and recovery.

As well as considering the implications of cognitive errors (those associated within individual 'thinking') we shall also consider the social psychological factors (those associated with people interacting in groups) that may lead to errors. The study of cognitive psychology seems to make the most prominent contribution to engineering within the domain of man-machine interface design. Analogously, the field of social psychology can contribute knowledge on the behaviour of engineers working in 'social' groups, that is assemblies of cooperative individuals with a common set of aims and objectives. With respect to safety, the social characteristic of the engineering processes might be most closely associated with the notion of 'Safety Culture'. There are a large number of social processes and procedures entailed in the general operation of any medium to large-scale engineering development. Amongst these we would include meetings, reviews, inspections, casual discussion, generation and response of memoranda and reports.

A large corpus of literature exists that describes cognitive processes and social behaviour of humans. The literature is well founded in experiment, and the explanatory models are widely accepted. It is known that the behaviour of individuals and groups is often 'counter-intuitive' and seemingly 'irrational'. People make mistakes when we feel that they should not. People make choices that seem to contradict all evidence to the contrary. People build mental models of the world that have little relationship to reality. Much knowledge of this type exists and yet little of it seems to inform the engineering process. We have been unable to find an engineering procedures document written in response to the types of human error described in the literature of psychology.

We will consider errors that arise from 'slips', 'mistakes' and 'lapses' of engineers as well as errors that may effect groups or individuals within groups such as 'compliance' and 'group-think'.

The first section of this paper considers a set of case studies of major engineering errors and disasters. Our intention is to make a three-fold contribution. Firstly, to juxtapose psychological theory with case-studies of engineering errors in order to argue for the development of engineering procedures based on psychological theory. Secondly, we hope to widen the audience for the psychological literature to the general community of engineers. Finally, we aim

to propose practical approaches to overcoming some of the basic predispositions to errors as well as some avenues for further research and study in this area.

Ours is a practical and pragmatic approach to these issues. We accept that it is difficult to substantiate a complete and formal argument that 'psychological predispositions' are responsible for errors in the engineering process. However, we believe it to be so and believe also that there is enough evidence from case study material to present an argument convincing enough to warrant action.

Some of the material in this paper has been reproduced from our earlier paper (Collins and Leathley 1995). We have omitted from this discussion our review of the general analytical process and our argument that we must accept as fact a lack of 'completeness' in all engineering, safety and reliability analysis. To this discussion we have added more details to some of the case- study material and further suggestions for avoiding errors in the engineering process.

2 INCIDENTS AND ERROR

2.1 Challenger

In early 1986 the space-shuttle Challenger exploded, killing all of the crew and bringing NASA's manned-flight programme to a complete halt. The specific cause of the disaster was eventually traced to the failure of seals in the vehicle's Solid Rocket Motors (SRM).

The space-shuttle is without doubt a hugely complex system and it might be considered possible that some important failure modes would inevitably be missed in design-analysis. However, one might also expect that if catastrophic failure modes were identified within systems then they would be subject to design review and improvement.

A fact not widely publicised at the time of the Challenger disaster was that the seal failure was not a 'unique event'. A 'calendar of events' running from 1977 until the destruction of Challenger has been documented by Reason (1990). The first seed of a design error came in 1977 when it was discovered that casing joints expanded instead of tightening as they were designed to do. NASA was, however, persuaded that this was "not desirable but acceptable". Scorching around seals was first noticed in November 1981 and occurred repeatedly until Challenger was destroyed.

On the second occasion that the seal failure was observed it was the subject of an 'Action Item' that called for a complete review of all of the SRM joints and seals. The manager who signed off the 'Action Item' left NASA shortly afterwards and *the planned review was never conducted* (Berry 1989).

Many revealing comments on the sequence of events and the attitudes and beliefs of the engineers working on the shuttle project have been recounted by Richard P. Feynman. Feynman, winner of a Nobel prize for physics, was appointed as one of the twelve members of the presidential commission investigating the Challenger disaster (Leighton 1993). We could quote many sections of this text that indicate a dissonance between what was known by individuals and the subsequent decisions made by 'the organisation'; consider the following:

"..engineers [from the company making the seals] had come to the conclusion that low temperatures had something to do with the seals problem, and they were very, very worried about it. On the night before the launch..they told NASA that the shuttle shouldn't fly if the temperature was below 53 degrees.. and on that morning it was 29...

..NASA was 'appalled' by that statement. The man in charge of the meeting.. argued that the evidence was 'incomplete'"

"Mr Ullian [the range safety officer] told us that 5 out of 127 rockets that he had looked at had failed - a rate of about 4 percent...because he assumed a manned flight would be safer than an unmanned one he came out with a 1% chance of failure.

But NASA told Mr Ullian that the probability of failure was more like 1 in 10^5 .

I tried to make sense out of that number. 'Did you say '1 in 10^5 '?"

'That's right; 1 in 100,000'

That means that you could fly the shuttle every day for an average of 300 years between accidents - which is obviously crazy!"

To find out how well the NASA engineers were communicating, Feynman gave a small group of them a test. He asked them to write down the probability that a flight would be uncompleted due to a failure in an engine.

"One guy wrote '99-44/100% pure'... meaning about 1 in 200. Another guy wrote something very technical and highly quantitative ..which also meant about 1 in 200. The third guy wrote, simply, '1 in 300'.

[Their manager's] paper however, said: 'Cannot quantify. Reliability is judged from past experience..and engineering judgment'.

I turned to [the manager] 'I think you weaseled. ... You told me how you determined it. What I want to know is: after you determined it, what was it?'

...He says, 10^{-5} "

In a footnote, Feynman makes another comment that may strike a chord with many reliability and safety engineers:

"As far as I can tell, "engineering judgment" means they're just going to make up numbers!"

Immediately after the accident, NASA reconsidered its judgment on the likely catastrophic failure rate of the shuttle and gave it as about 1 in 78. A recent probabilistic risk assessment carried out by the Science Applications International Corporation suggested that a figure of 1 in 248 was more likely. Given the proposed flight programme this gives a 50% chance of another catastrophic failure before the year 2015 (Kiernan 1995).

It has been suggested that this incident was a result of a failure to communicate. Should not the engineers have reported their concerns to senior management? As Berry has pointed out:

"[More reports] would merely guarantee that more would be written than read! No, to correct these problems, people at the top must ask the right questions"

(Berry 1989)

2.2 Three Mile Island, Chernobyl and Wylfa

The explosion at Chernobyl was the worst accident in the history of nuclear power and there is evidence that it was due solely to human action rather than any mechanical failure¹.

The accident happened as a result of a series of experiments that went disastrously wrong. As Reason has reported, the test plan for the experiments was wholly inadequate and "... the section on safety measures was drafted in a purely formal way". The operators involved had "...lost any feeling for the hazards involved".

The Chernobyl accident eclipsed the nuclear industry's previously most controversial incident. The one that occurred at the Three Mile Island nuclear plant near Harrisburg, Pennsylvania. Perrow has pointed out:

¹ For a full discussion of the psychological factors involved in the Chernobyl disaster, the reader is referred to the comprehensive paper by Reason (1987).

"The subsequent investigations and law suits disclosed a seemingly endless story of incompetence, dishonesty, and cover-ups before, during and after the event"

(Perrow 1984)

The commission set up to investigate the incident decided that:

"the major cause of the accident was due to inappropriate actions by those who were operating the plant"

(Perrow 1984).

But Perrow has argued that it may be unreasonable to blame operators for errors if those operators have to be 'super-men' to make the right decision at the right time. If a person is swamped with confusing, contradictory information that partially fits their previous experience, but in fact represents a situation that is quite different, then it is not unreasonable to expect them to make 'mistakes'. If one operator misreads a dial then it is deemed to be the operator's fault. If many operators misread a dial then it is deemed to be a fault in the design of the dial. Presumably between these extremes lies a spectrum of attribution. Where we apportion blame is dependent on the expectations we have of human performance in the areas of design and of operation. We tend to the view that whilst there may be operator error this is only a symptom of the properties of the system being controlled. In other words, a view can be adopted that says that there is no such thing as operator error, only errors in design that allow operators to make mistakes.

Reporting on the £250,000 fine placed on Nuclear Electric for a failure to shut down Wylfa after an accident 'The Times' on 14th September of this year said:

"Hugh Carlisle, QC, for the Nuclear Installations Inspectorate told Mold Crown Court it was a 'classic example of brains in neutral'."

This is perhaps a disingenuous comment. There is no obvious evidence that the system operators were not aware of the situation, only that they chose to allow the system to operate, rather than shutting it down when they should have. This may have been as a result of individual cognitive errors or errors due to social interactions of the group, but it seems most likely that the decision to keep the reactor operating was in response to a 'pathology' of the organisation as a whole. That is, economic pressures to keep operating forced the operators to make decisions that, in retrospect, are judged inappropriate.

In these examples we are attempting to highlight a hierarchy of error types that range from the individual cognitive error (such as misreading a dial), through errors arising from group interactions (eg. communication errors) and ultimately to 'cultural' failures, and failures arising from the broader economic and operational environment (time and cost pressures).

2.3 Hubble Space telescope

The launch of the famously short-sighted Hubble Telescope does not strictly rank with other safety-related catastrophes. However, the failed processes of quality control and of system-analysis carried out during its production are similar enough to those involved in safety and reliability analysis to draw important analogues.

Analysis and testing was conducted on the mirror of the Hubble Telescope, and information that suggested it was in error was available before it's launch. The most damning indictment of the errors in the analytical and experimental verifications of the systems comes from those who investigated the development after the error was discovered:

"..so [the small lens used to check the main mirror] was moved down by a millimetre, and that could have been discovered just by checking with a ruler, and that was evidently never done. But even more than that, optical tests were made later which clearly, in their data, showed the mistakes. Its not a subtle effect, it's completely obvious, and that data which showed the mistake was discounted simply because they could not believe that the original manufacturer was incorrect. So one's jaw still drops at how many opportunities there were for this error to have been seen, that were missed."

(Angel)

"One of the most unfortunate aspects was that the data was so easy to discover, because that meant that it was near the surface. It existed in the technicians' notebooks but it had been overlooked and discounted at the time. In this particular case there was significant inhibitions [sic] to communication from the technicians that were involved to other parts of the organisation. "

(Allen)

So the error was known about, but "there was significant inhibitions to communications". The factor that lead to the failure of the system to act in the required manner was not fundamentally related to the technology but to the interactions of the developers. The problem with the Hubble Telescope was one of human organisation and of human communication; in short, it was a psychological problem.

2.4 Tacoma Narrows Bridge

The news-reel film of the catastrophic failure of the Tacoma Narrows Bridge has become familiar to many engineers. The violent, wind-induced motion of the bridge platform provides a graphic example of resonance effects in mechanical structures. Casual observation of the film suggests that the wind speeds that caused the failure were somehow exceptional, but that is not true. The bridge was designed to withstand a wind-speed of 200mph and collapsed when the winds were gusting to 70mph, a not uncommon occurrence.

Levy and Salvadori (1992) have reported that the bridge was nicknamed 'Gallopig Gertie' from the day it was opened on July 1, 1940 because of the way it undulated in the wind.

"..from the time of its construction [the design engineers] repeatedly tried to take the up-and-down sway out of the bridge. To this purpose 1.5in (38mm) tie-down steel cables were attached to the bridge near each end and anchored to fifty-ton concrete blocks, but when these cables were installed..they snapped like cotton threads during the first windstorm. These tie-down cables had neither significantly reduced the swaying and bucking of the bridge... and yet they were reinstalled three days later with renewed optimism about their effectiveness." (emphasis added)

Levy and Salvadori (1992)

But perhaps the designers could be exonerated on the basis that the mechanics of suspension bridges were not well understood in the 1940s. Perhaps there was not enough previous information or experience to enable any better design decisions to be taken.

In fact, the converse is the case. Cawkell has catalogued a long history of wind damage to bridges (including suspension bridges) that occurred before 1940 and which should have provided information to enable better design decisions to be made on the Tacoma Narrows (Cawkell 1991). For example, a paper published in 1933 by Moisseif discussed the problems associated with lateral wind forces on long, narrow bridges based on practical experience of the

George Washington Bridge completed in 1931 (Moisseiff 1939).

Cawkell provides a table of comparative statistics from bridges built before the Tacoma Narrows and which would have been available to the designers had they looked for them. The statistics are so markedly anomalous for the Tacoma Narrows that, as Cawkell has pointed out:

"Unless accompanied by an explanation about how it was possible to justify such a light, flexible structure totally different from any contemporary bridge, the only possible reaction would have been frank disbelief"

Cawkell catalogues a list of possible reasons why information from previous disasters might have been ignored by those responsible for the design of the bridge. His analysis leads him to the conclusion that:

"Boldness, design novelty, and economic considerations overrode caution and experience."

An astounding coda to the story of the collapse of the Tacoma Narrows Bridge is the report of the subsequent investigation:

"Both the Public Works Administration and the Reconstruction Finance Corporation were entirely justified in assuming that, because of the experience and reputation of the consultants employed, there could be no possible question as to the adequacies of the design" (emphasis added)

2.5 The Clapham Junction Railway Accident

At 8:10 on the 12th December 1988 two trains full of passengers collided at Clapham Junction. Thirty-five people died as a result of the accident and 69 more were seriously injured. 415 people received minor injuries.

The accident resulted from a signalling failure. The signalling failure occurred as a result of alterations to the system - a wire that should have been removed from the signal had been left in place. Current from the wire that should have been removed prevented a crucial signal from showing 'red'.

The report of the investigation into the Clapham Junction railway accident provides a detailed analysis of the accident itself, the response of the emergency services and, of particular interest here, the factors that contributed to the error in wiring of the signal (Coates 1989).

The Senior Technician responsible for the error in the wiring was promoted into his position not as a result of passing any examinations, as his job description might have suggested, but rather as a result of changes in staffing arrangements. When performing his work he "just made a plan out himself in his head and then went and did the job."

When changing the wiring of the signal involved in the accident the technician failed to cut back the old wire (which remained live) and to tape it off with insulating tape. He had never been told to cut back the wire and had never observed others doing so. His belief was that pushing the 'redundant' wire away from the terminal to which it was previously connected was sufficient and that it was not necessary to cut the wire back. More-over he believed that pushing the old wire to the side left the wire in a safe state.

The error that occurred might thus be attributed to lack of training or due to the fact that an inappropriately skilled person was tasked with performing a safety-critical procedure. But what of the supervisors and managers who were an important part of the environment where the technician worked? There had never been any complaints about the technician's skills or quality of his work in the 16 years he had been employed by British Rail. During the investigation it was made clear that the blame for the continual bad practice did not lie with the technician but with British Rail because:

"Either it should never have been allowed in the first place or once it had happened and the practice had become your practice and indeed was commonplace, it should have been stopped because the matter should have been monitored" (emphasis added)

Mr Roger Henderson Q.C. for BR.

It was part of documented procedure within British Rail that a safety check should be done by an independent person because:

"The installer who makes an error may, when he looks at the work, may miss the error he has made. He may see what he thought he had done, and meant to do, not what he has in fact done."

In psychological terms this is referred to as 'Mental Set', a subject we shall return to in the last section of this paper. However, no such independent check of the work was ever done. The supervisor explained his failure to independently check the work on the basis that he was expecting the technician to check his own work, which had been the general practice for many years, and the requirement to perform an independent check had never been mentioned to him. The supervisor had not been made aware of the requirements of the written procedure to which he and his staff should have been working.

Thus the trail of blame leads directly up through the chain of command, with procedural errors being made at each level.

As well as the continual errors in practice that might be attributed to lack of training or skill there was evidence of another category of error. The report of the investigation suggested that the specific wiring fault may have arisen as a result of:

1. The process of combining two jobs, and,
2. the technician's concentration was broken by an interruption of some sort;

Both of these mechanisms for error are treated fully in the literature of cognitive psychology and again are matters to which we shall return.

2.6 Some Comments on Case Study Material

At this point we should consider the basic problem of case study material. When reviewing a case study we can never be absolutely sure that we have the whole story. Case studies often appear convincing because the story is told, emphasising only those salient points that highlight the writer's interpretation of 'what is really happening'. Accepting this caveat, the interpretations we place on the events we record appear to be well supported by experiment and by other commentators (Reason 1990). What we see in 'real life' seems to follow closely what we would predict from experiments in cognitive and social psychology. It is our contention that, as pragmatic engineers, we should accept the best psychological theories available and incorporate their results into our work practices.

3 PSYCHOLOGICAL PREDISPOSITIONS TO ERROR

3.1 Introduction

This section deals with two major branches of psychology that have a bearing on errors in safety and reliability analysis: social psychology and cognitive psychology. It is impossible within the confines of a paper such as this to do justice to the full range of published research in these fields, and our aim is thus to draw attention to major research results only. This section is aimed at an audience that we assume to be predominantly composed of engineers and technologists rather than graduate or professional psychologists.

Social Psychology (Section 3.2) treats behaviour in terms of a "black box" model. That is, it considers 'inputs' and

'outputs' to the way people behave, and how this behaviour is effected by other people or by organisations. The processes that exist inside the individual, that is the reasons why people or groups behave in particular ways, is considered to be the province of Cognitive Psychology (Section 3.3). Cognitive psychology, can be seen as considering the "white box", where we try to establish what is going on inside the mind. Cognitive psychology is concerned with the manner that information is represented and manipulated inside the "box".

In section 3.2 we will look at some social mechanisms of error. In 3.3, cognitive explanations will be given for some of these, as well as other error types.

3.2 Social Psychology

3.2.1 Conformance

One potential obstacle to the successful completion of a safety analysis is a social pressure to conform, - 'not to rock the boat'. Rules of professional conduct maintain that we should never compromise judgement due to pressure from organisations or individuals and yet evidence exists that suggests that human beings are prone to do just that.

Experimental evidence for the power of conformity is available from the work carried out by Asch in the 1950s (Asch 1956). Asch actually set out to prove that people were not influenced by a group when the correctness of their own decision could not be in doubt.

He arranged for 5 'subjects' to sit together, and be asked to judge the length of lines drawn onto a card. They were told that it was an experiment in perception. However, only one person was really the subject - the others were confederates of the experimenter, 'planted' in order to exert social pressure on the genuine subject.

A line was shown, next to three other lines of different lengths. The task set was to judge which of the three lines was closest in length to the first and to call out the judgement so that everybody could hear. The task was designed to be an easy judgement, and for a few rounds, all of the 'subjects' made the correct choice.

However, after a few goes, the 'subjects' who were in league with the experimenter all gave an answer that was obviously wrong! The real subject was the last to call out his decision and was thus confronted with a string of answers that did not match his own judgement. Although the correct answer was clear, around 75% of the subjects chose to conform, rather than to follow their own judgement, at least once.

From interviews carried out after the study, it appears that this was because their actual perception of the lengths of the lines changed, rather than arising from a conscious desire to 'fit in'.

The situation in terms of a typical safety and reliability analysis task may not be entirely analogous since the consequences of conformity against better judgement may be very much greater than in the experiment conducted by Asch. However, the consequences of a failure to conform are also great. We can at least conceive that a person could alter their judgement about a system rather than point out difficulties that may cause serious delays to a project, as with Challenger, or require expensive resources to correct, as with the Hubble telescope.

3.2.2 Group Behaviour.

Another aspect of social psychology relevant here, is the way people behave in groups. While groups can be used to remove some of the errors that individuals may make, by checking each other's work, a number of biases have been observed in groups of people working together:

Group think - where, because of shared experiences, members of the group make the same mistakes, and are unable to spot mistakes in each other's work. Another explanation is that group loyalties can lead to an avoidance of criticism (Janis 1972). The feeling of immunity from harm at Chernobyl, and the fact that no one challenged the test plan, might be partly explained by 'group think'.

Group polarisation - where the position taken by the group is more extreme (more polarised) than the decision that would be taken by any one person. There are two extremes of this:

Risky shift - where the decision taken by a group is more risky than would be taken by any one member of the group alone. This phenomenon could go some way to explaining some of the risks taken in the Challenger project, and boldness of the Tacoma Narrows bridge design.

Cautious shift - where the decision taken by a group is safer than would have been taken by any one member of the group alone. This is sometimes witnessed amongst juries for serious crimes.

False consensus - Where a group believes a decision has been made that everyone agrees with, but actually this is not the case.

Pluralistic ignorance - Where an individual has the mistaken belief that they are the only person with a different point of view, and therefore say nothing.

To avoid group think, the team need to be able to accept that errors occur naturally, and that checking for them and removing them is a natural part of the analysis activity. Bringing in outsiders, or a "devil's advocate" is another way of avoiding group-think. Someone who is prepared to challenge accepted values and norms may be considered a trouble-maker, but they can at least encourage the group to re-consider their decision.

We will return to some of these in the next section and seek a cognitive explanation for them.

3.3 Cognitive Psychology

3.3.1 Cognitive Bias.

Tuler (1988) lists a number of contributors to faulty decision-making. He described these as "cognitive biases and heuristics". Of these, the following may be considered relevant to the current topic:

- overconfidence in estimations and plans;
- previous experiences often used as bases for future choices;
- accepting confirmatory evidence and ignoring or forgetting contradictory evidence;
- options that are not readily observable may not be considered;
- tendency towards conservatism;
- thinking in causal series rather than causal nets;
- anchored by previous experience.

In most situations, these biases assist to make decision-making a more efficient activity. For example, when removing an apple pie from the oven when it is cooked, we use the heuristic:

"oven is hot, therefore, plate being removed from oven is probably hot".

This saves us having to collect further information (eg obtaining a thermometer and checking the temperature of the plate). Instead, we can quickly make the decision to use an oven glove. In the same way, over a period of time it is likely that analysts develop rules to improve the speed and efficiency with which an analysis can be carried out. In some cases, these rules may enhance the accuracy, enabling better decisions to be made. However, there are circumstances under which these heuristics bias us incorrectly.

Tuler suggests that we build "mental models" of how a given system works:

"..these 'mental models' are based on previous experiences and information and they are derived from various representations of the system ... collection of beliefs about a system, including functions, structure, and internal processes and relationships"

(Tuler 1988)

'Overconfidence in estimations and plans' can result from overconfidence in this mental model. If the rules work most of the time, then naturally we expect them to work all of the time. However, this may lead to the application of a rule incorrectly, without the full picture. This relates to the second bias listed, 'previous experiences often used as basis for future choices'. This may apply within a single analysis as well as between analyses. Once part of an analysis has been completed, a picture of the system starts to emerge. This picture effectively influences future choices in the analysis.

The third bias, 'accepting confirmatory evidence and ignoring or forgetting contradictory evidence', is an explanation of the concept of "mental set" mentioned in Section 3.5.

Mental models can become fixed. Rather than adapting the mental model according to new observations, we may continue to apply a rule even if it is no longer valid. To defend this application, there is a tendency to concentrate on the evidence in favour of the rule, and perhaps not notice the evidence that disputes the rule, or challenges the mental model. A particular view of the system is held, and therefore all evidence is seen in that light.

The evidence suggests that a 'mental model' prevalent at the Chernobyl nuclear reactor was that it was safe to carry out tests. Readings which should have indicated problems, were ignored or discounted.

The irony of the fourth bias, ('options which are not readily observable may not be considered'), is that "not readily observable" may actually refer to things which would have been quite easy to see. For example, measuring the position of the test mirror in the quality assurance checks for the Hubble Telescope, or looking at the data in the technicians' notebooks. These would have been easy, if they had been considered. But these errors were not expected. If the particular mistakes had been considered possible, they would have been observed.

We can relate the 'tendency towards conservatism' back to the social pressures outlined in Section 4.2. Halting an expensive development project, or space programme, can be considered quite radical, and therefore there is likely to be a tendency to try to dismiss problems.

'Thinking in causal series' - Reason (1987) explains that the Chernobyl operators, while sensitive to the main effects of their immediate actions, remained unaware of any consequences of their actions on other parts of the system.

The above list of heuristics and biases may be considered as meta-cognitive skills - they represent ways of thinking. They survive because they are generally useful to us. However, there are situations where it is necessary to break out from the normal serial processing of options. "Mental set", or fixedness of the mental model may play a role here in preventing alternative ways of thinking. The normally efficient mechanism can predispose us to error

3.3.2 Cognitive Dissonance.

Cognitive dissonance is a theory presented first by Leon Festinger (Festinger 1957). Cognitive dissonance is a state of tension created by the occurrence of two conflicting 'cognitions' (ideas or opinions) at the same time. Theory suggests that this tension is uncomfortable, and so individuals tend to attempt to reduce it.

The theory of cognitive dissonance can be used to explain behaviour in situations which otherwise would seem contradictory. For example, if a designer considers herself competent, conscientious, and proficient at the design task then there is a dissonance between this view and the view that "my design is flawed, will be unreliable and in it's present state is likely to be the cause of death and injury". Experimental evidence shows that people tend to reduce this type of dissonance by changing their cognitions with respect to one of the two notions. But we know that the two notions may not be contradictory *in fact*. It is perfectly possible that an otherwise competent designer can make a mistake. It is perfectly possible for a system to fail for reasons that were truly outside of the scope of human knowledge at that time.

The true danger here lies in the cognitive dissonance reduction process because this is the route that leads to the altogether more tragic event, the catastrophe resulting from a failure that was known about or easily within our ability to predict, and yet that was never investigated.

Dissonance is also important in looking at the way we behave once we have made a decision. An analyst may look at all the information before establishing a fact crucial to the analysis and making a decision. Once made however, any further information which confirms this decision will tend to be welcomed, any information which suggests a change should be made is likely to be thought of as less relevant (Aronson 1980). Hence, by making a decision, we start to screen out information which does not fit in with our original picture of the activity.

Knox & Inkster (1968) asked people about their certainty that horses they were betting on would win. Those asked *after* they had placed their bets were more certain in their judgements than those asked *before* they had placed their bets. People are more certain they are right after there is nothing they can do about it.

Once a design has been reviewed and no error has been found, we are very much more likely to

believe that no error exists, in a manner disproportionate to the amount of investigation done.

An additional problem occurs when checking the work of a superior, or of a respected colleague. The belief that the other person is good at their work, perhaps better than oneself, does not resolve with the notion that one can have found a mistake with their work. This provides a context within which we can understand the reticence of engineers on the Challenger or Hubble Telescope projects, to dispute the plans of more senior people.

Although we have no details of the wider 'political' motivation that lead to the comment concerning the destruction of the Tacoma Narrows bridge quoted in section 3.4 above, there is certainly a suggestion of dissonance between 'trust in experts' and the evident results of that unquestioning trust.

3.3.3 Information-Processing and Schemas

There are a number of theories relating errors to failures in the way we process information. For example, Reason (1990) categorises errors in terms of the different phases involved in thinking about, and then performing, an action. He describes three types:

- 1) error in planning - mistake
- 2) error in storage - lapse
- 3) error in execution - slip

Norman (1981) defines different types of slips. First, he defines sequences of behaviour (or "action sequences") in terms of "schemas". Norman describes these schemas as "sensory-motor knowledge structures". That is, a schema is triggered by some stimulus to our sensory system (eg a noise, the sight of a particular friend or colleague, the arrival of a particular piece of work). The information about how to behave (the motor part) is contained in memory, as a knowledge structure. Schemas can be hierarchical, with one schema (the "parent") calling any number of other schemas (the "child" schemas), and several schemas may be active at any given time. Slips can then be defined in terms of faults in the execution of these schemas. Norman defines three categories:

- 1) error in formation of an intention
- 2) error in activation of a schema
- 3) faulty triggering of a schema

Error in formation of an intention may result from incorrect, incomplete or ambiguous classification of the situation. For example, if the goal is not clear, or if insufficient attention is given to a situation, an inappropriate schema for the current situation may be chosen. An example of incomplete specification is pouring coffee onto one's breakfast cereal, and milk into one's coffee cup.

Faulty activation includes unintentional activation of a schema at the wrong time, unexpected termination of the schema, leaving it incomplete, and missing or repeating steps. The former may happen when one gets 'too close' to a familiar schema. For example, getting into the car to put it into the garage, and instead driving to work.

Incomplete activation of schemas is illustrated by all those occasions when you go into a room to get something, only to discover that, on arriving you can't remember what you went in for.

The likelihood of missing or repeating steps in a schema is increased when a schema is interrupted. Hence, it may be that the interruption of the technician looking at the wiring in the Clapham Junction disaster, may have resulted in a step being missed from the action sequence.

The final category of slip occurs when components within a schema become confused or reversed. Spoonerisms are an example of this. Attempts to form new schemas by combining old schemas can lead to this type of slip.

An insight into the Clapham Junction disaster can be provided by looking at the difficulties of combining schemas. Combining two jobs involved the combination of two parent schemas, and their resulting child schemas. It could be that the combination was difficult to resolve, and again, could have resulted in missed and repeated steps, and premature completion.

4 SOME TECHNIQUES FOR OVERCOMING PSYCHOLOGICAL PREDISPOSITIONS TO ERROR

4.1 Introduction

Before making some specific comments about the methods that may be available to overcome our predispositions to error it is important to make some general points. Most of the items detailed below are already part of the accepted practice of safety and reliability analysis. We are attempting here to place these practices within a frame-work and also to highlight those areas that might admit to specific research.

Our most general point is that the study of psychology has a great deal to offer to the process of engineering development, and of analysis. We are hoping firstly, to generate greater interest in psychology amongst safety and reliability engineers from a traditional engineering background, and secondly, to encourage those analysts with expertise in the field of psychology to share their skills and knowledge with a wider community of engineers.

4.2 Automation of Analysis

Automation is the extreme manifestation of procedurisation. Many of our analytical techniques are highly repetitive and prone to the types of human error described above. The automation of analysis must be a prime candidate for research effort in the fields of safety and reliability.

It is important to distinguish here between:

- i. automation of analysis: the processing of raw data is performed by machine and new knowledge is thus obtained; and,
- ii. automation of administration: the use of data-base tools and so on to store analytical results (Collins 1995).

The latter should contribute to the reduction of errors, but the goal must be the former - analysis by machine.

4.3 Inspection vs Review

It has been pointed out that 'design reviews' (as opposed to 'inspections') can be less powerful than they may at first appear (Fagan 1976, 1986). The familiar scenario of a group of engineers sitting in a meeting and 'walking through' the design suffers from exposure to a number of the problems outlined above, not least of all, conformity to group norms.

We question the notion of engineering reviews as a group activity. To paraphrase Douglas slightly:

"There is only one sufficient reason for using group techniques in a .. situation, which is that in the considered opinion of the group convenor it is by all available data the best possible means of coping with the .. situation"

(Douglas 1976)

To be valid as a group activity there must be some demonstratable benefit arising from group rather than individual activity. Creative activities, for example 'brain-storming' sessions, may show greater productivity when performed as a group; however, we are not convinced that the same may be said of 'analytical' processes such as design reviews.

We can also imagine a series of protocols for allowing group members to express their doubts before they know the opinions of others. It has been suggested that group members should review written material and present a short written response before important decision-making meetings (Douglas 1976). The purpose of the meeting would then be partly to discuss the written responses, and to highlight any significant differences between written responses. Such a protocol would however have to be well managed. One could imagine a series of written answers that were ambiguous and did not put the writer at risk. An alternative protocol might feature a short series of 'multiple choice' options forcing

prior declaration of judgements on important issues.

We propose further research to identify protocols for group reviews of designs and processes. We would expect these to adopt 'Fagan Inspection' style check-lists for group reviews, but more importantly, to identify the exact circumstances under which group reviews are preferable to individual inspection.

4.4 Devil's Advocates

The Asch experiment, while presenting us with a problem, also provides us with a partial solution. If 4 other people gave the wrong answer, the 5th person (the subject) was likely to conform. However, if only one other person gave the correct answer, the subject was much more likely to give their true judgement - the correct answer. The 'right' answer could still be the minority choice, but having even one person agree was enough for people to be prepared to be wrong. For this reason the institutionalised role of a 'devil's advocate' in technical reviews can be seen to be a valuable one.

4.5 Independence Provided by Consultants

Conformity to group norms is less likely if the critical judgement arises from staff who are outside of the organisation effected by the decision, and who are motivated towards different goals. But what does 'independent' mean in this context? Has not an organisation who hires external and independent consultants the option of repeatedly 'hiring and firing' until it gets the required and expected answer?

We would like to see research that addresses the sociological, psychological and professional issues associated with 'independent analysis'. The questions must include an adequate definition of 'independence', a metric for judging it, and the mechanisms and protocols for preserving it.

4.6 Repertory Grid Technique

One technique developed to overcome some of the problems involved when groups work together is an application of repertory grid technique (RGT). RGT was first applied in clinical psychology settings, to "map" the way people thought about people around them (Kelly 1969). Similar techniques have been used to produce job descriptions, and map candidates with job requirements. This technique has now been developed and applied to teams of people controlling safety-related processes (Four Elements 1993).

Members of the team provide details of the tasks they carry out, and bi-polar constructs of these tasks are drawn out. For example, "difficult-easy", "dangerous-safe". A grid is drawn up showing these constructs as the extreme points on a linear scale. Each individual in the team completes the grid by rating tasks against this scale. Comparisons can then be made between the mental model each team member has of the process they control, and any differences noted. In this way, some of the dangers of pluralistic ignorance, false consensus and group-think can be avoided.

4.7 'Egoless' Safety and Reliability Analysis

Weinberg (1971) introduced the concept of "Egoless programming". His suggestion was that if a programmer is personally responsible for a programme, they will tend to defend the programme against criticism, even if it has obvious failings. If a programme is considered 'group property', criticism will be better accepted. One could imagine a similar system of ownership applying to other engineering tasks and analyses.

A major criticism of Weinberg's suggestion must however be that it was not substantiated experimentally. We would again propose a research topic that addressed attitudinal issues of 'ownership', 'protectionism', and 'competitiveness' within engineering development and analysis teams.

4.8 An Error Tolerant Engineering Process

In the field of human factors design, Rouse has proposed that 'error tolerant' systems should be designed (Rouse

1990). His argument is that:

"..the total elimination of human error is a futile pursuit. Instead, systems should be designed so that they are error tolerant in the sense that errors can occur without leading to unacceptable consequences"

Rouse provides a classification scheme for human errors. Items include, for example:

- ...
- 2. Choice of hypothesis
 - 2d. Functionally irrelevant
 - Does not relate to state variables observed
- 3. Testing of Hypothesis
 - 3b. false acceptance of wrong hypothesis
 - reached wrong conclusion

As well as classifying the types of errors that may occur when an operator controls a system it may also be used to classify the types of human errors that occur in the engineering process. For example, the above categories might apply to the error of changing the wrong part of a system design as a result of a design defect report (i.e. adding tie-down cables to a bridge that is simply too light, long and thin) or concluding that if a seal is partially destroyed but a spaceship survives then partial seal failure is safe in the future.

Rouse describes an error remediation process that acts in response to different types of errors. The engineering process often includes such mechanisms in the form of quality assurance, reliability analysis and safety assurance. We notice however that these remediation processes have not arisen as a result of a formal analysis of human error types but rather they have evolved in response to historical errors.

We propose research that considers the existing models of human error modes and mechanisms with respect to the engineering process. Particularly, we should formally compare the activities undertaken as part of quality assurance, reliability analysis and safety assurance with the a set of remediation processes developed directly from models of human error.

5 CONCLUSION

Catastrophic events do happen, and we have shown that the origin of these events can often be traced back to specific human errors in design, analysis or the application of procedures. As our general analytical procedures improve and develop, some effort must be dedicated to ensure that they can be applied and used correctly. A perfect analytical tool, that revealed all problems with a design, would be of theoretical interest only if it was too complicated to be applied correctly, in practice. A technique is only truly valuable if it is used and can be applied correctly (Collins 1989). It might be more problematic to apply a theoretically perfect method than to use a more simple, but less powerful, technique since powerful techniques can attain an authority, and carry with their use a conviction that is not warranted. It is better to know that we are ignorant of certain parameters of a system than to be certain of some of them and yet believe we know them all!

In the fields of safety and reliability analysis it is often incumbent upon us to address the 'weak link in the chain'. In the future our weak link may not be the power of our analytical techniques, but our ability to apply them correctly. In parallel to developing new techniques we must address the issue of their application.

Our principle and overriding suggestion is that there be greater input from the field of psychology into the domain of safety and reliability analysis and into engineering in general. We need psychologists to review the application of the techniques we employ and to propose strategies to improve their effectiveness.

As professional safety and reliability analysts we must make all efforts to ensure that we can never be the 'weak link' in the chain.

Considering the quote from Juvenal that heads this paper:

"Sed quis custodiet ipsos Custodes?"

(But who is to guard the guards themselves?)

(Juvenal c.60-c.130)

If we are the ultimate custodians of the safety and reliability of systems, equipment and processes then who will ensure that we do not err?

We must ensure to the greatest extent possible that never again will catastrophe strike because something that was thought, was never voiced. Because something that was voiced, was never written down. Because something that was written down, was never read.

A APPENDIX: ANNOTATED BIBLIOGRAPHY

A.1 Case Studies

Leighton, R (1993)

"What do you care what other people think?: Further adventures of a curious character"

Harper Collins : London

ISBN 0 586 21855 6

We would recommend this as a 'must buy' text. Part 2 of the book contains a very readable, 126 page report of Feynman's part in the review of the Challenger disaster. Feynman is blunt and to the point and brought to his review the clear, incisive thinking of a Nobel prize winning physicist.

Perrow, C. (1984)

"Normal Accidents: Living with High-Risk Technologies"

Basic Books Inc: New York

ISBN 0 465 05144 8

This book is a large collection of case studies that would make thought provoking reading for any engineer. Perrow's basic thesis is, however, different to our own, attributing many disasters to the innate characteristics of systems as a whole.

Read, P.P (1993)

"Ablaze: The story of Chernobyl"

Mandarin Paperbacks : London

ISBN 0 7493 1633 0

An exhaustive, (and exhausting) 450 page account of the Chernobyl disaster.

A.2 General Psychology

Gleitman, H (1981)

"Psychology"

W.W. Norton and Company, Inc. : New York

ISBN 0 393 95102 2

Hilgard, E.R., Atkinson, R.L., and Atkinson, R.C. (1979)

"Introduction to Psychology"

Harcourt Brace Jovanovich Inc : New York

ISBN 0 15 543668 6

These are the two 'standard' undergraduate text-books on psychology. They are suitable for anybody new to the subject of psychology and would provide a good foundation for any engineer who would like to develop their understanding of this subject for incorporation into their working practices.

Cooper, C.L. and Makin, P. (1984)

"Psychology for Managers"

The British Psychological Society : London

ISBN 0 333 36523 2

A very useful guide for those working in management. Couched in accessible language and covering such topics as

motivation, social behaviour and stress.

A.3 Social Psychology

Aronson, E. (1980)
"The Social Animal"
W.H.Freeman and Company: San Francisco
ISBN 0-7167-1229-6

A very readable and interesting introduction to social psychology. Again, the 'standard' undergraduate text-book on social psychology.

A.4 Cognitive Psychology

Reason, J. and Mycielska (1982)
"Absent Minded: The Psychology of Mental Lapses and Everyday Errors"
Prentice-Hall, Inc. : Englewood Cliffs, N.J.
ISBN 0 13 001735 3

This is a more readable text for those new to psychology than the Reasons "Human Error". However, it may be difficult to obtain in the UK.

REFERENCES

- Asch, S. (1956)
"Effects of group pressure upon the modification and distortion of judgment"
in M.H. Guetzkow (ed) *Groups, Leadership and Men*
Carnegie : Pittsburgh
- Allen, L.
Chairman of the Board of Investigation for the Hubble Space Telescope Project
Quoted from "Horizon: Small Problem with the Telescope", BBC Television
- Angel, R.
Member of the Board of Investigation for the Hubble Space Telescope Project
Quoted from "Horizon: Small Problem with the Telescope", BBC Television
- Aronson, E. (1980)
"The Social Animal"
W.H.Freeman and Company: San Francisco
ISBN 0-7167-1229-6
- Berry, A. (1989)
"Harrap's book of Scientific Anecdotes"
Harrap Books Ltd.: London
ISBN 0 245-54597-2
- Cawkell, A.E. (1991)
"The Tacoma Bridge Disaster: A Lesson in Disregarding Information"
in F.W. Horton and D. Lewis (Eds) *Great Information Disasters*
Aslib : London

- Coates, J.R. (1989)
 "Investigation into the Clapham Junction Railway Accident"
 Her Majesty's Stationary Office: London
- Collins, M.A. (*In 1995*)
 "Automated Abstraction of Failure Effects using a Formal, Hierarchical, Hardware Specification Language"
 M.Sc Thesis : Cranfield University
- Collins, R.J. (1989)
 "The Psychologist as an Agent for Change: Computers and Special Education for Adults"
 in *The Applied Psychologist* J.Hartley and A.Branthwaite (eds)
 Open University Press: Milton Keynes
 ISBN 0-335-09844-4
- Collins, R.J. and Leathley, B. (1995)
 "Psychological Predispositions in Safety, Reliability and Failure Analysis"
 Journal of the Safety and Reliability Society
 Spring 1995
- Douglas, T. (1976)
 "Groupwork Practice"
 Tavistock Publications Limited: London
 ISBN 0 422 74730 0
- Fagan, M.E. (1976)
 "Design and Code Inspections to Reduce Errors in Program Development"
 IBM Systems Journal, 15, 3, 182-211
- Fagan, M.E. (1986)
 "Advances in Software Inspections"
 IEEE Transactions on Software Engineering, SE-12, 7, 744-751
- Festinger, L. (1957)
 "AAS Theory of Cognitive Dissonance"
 Stanford University : Stanford
- Four Elements (1993)
 Private Communication
- Janis, (1972)
 "Victims of Groupthink"
 Houghton Mifflin : Boston
- Kelly, G.A. (1969)
 "The role of classification in personality theory"
 in B.Mahler (ed) *Clinical Psychology and Personality: the selected papers of George Kelly*
 Wiley : New York
- Kiernan, V. (1995)
 "Safer shuttle still risks catastrophe"
 New Scientist, 2nd September 1995, pp. 6
- Knox, R. and Inkster, J. (1968)
 "Postdecision Dissonance at Post Time"
 Journal of Personality and Social Psychology, 8, 319-323

- Leighton, R (1993)
 "What do you care what other people think?: Further adventures of a curious character"
 Harper Collins : London
 ISBN 0 586 21855 6
- Levy, M. and Salvadori, M. (1992)
 "Why Buildings Fall Down"
 W.W.Norton and Co. : New York
 ISBN 0 393 31152 X
- Moisseiff, L.S. (1939)
 "Growth in suspension bridge knowledge"
 Engineering News Record, August 17th, 46-49
 (Referenced in Cawkell 1991)
- Norman, D.A. (1981)
 "Categorization of Action Slips"
 Psychological Review, vol 88, no 1, January 1981.
- Perrow, C. (1984)
 "Normal Accidents: Living with High-Risk Technologies"
 Basic Books Inc: New York
 ISBN 0 465 05144 8
- Reason, J. (1987)
 "The Chernobyl Errors"
 Bulletin of the British Psychological Society
 40, 201-206
- Reason, J. (1988)
 "Chernobyl: A Reply to Baker and Marshall"
 The Psychologist: Bulletin of the British Psychological Society, 7, 255-256
- Reason, J (1990) "Human Error" CUP
 "Human Error"
 Cambridge University Press: Cambridge
- Rouse, W.B. (1990)
 "Designing for Human Error: Concepts for Error Tolerant Systems"
 In H.R.Boher (Ed) "Manprint: An Approach to Systems Integration"
 Van Nostrand Reinhold : New York
 ISBN 0 442 00383 8
- Tuler, S. (1988)
 "Individual, Group and Organizational Decision-Making in Technological Emergencies: A Review of Research" Industrial Crisis Quarterly 2.
- Weinberg, G.M. (1971)
 "The Psychology of Computer Programming"
 Van Nostrand Reinhold Company: New York
 ISBN 0-442-20764-6