EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL EXPERIMENTAL CENTRE

REVIEW OF ROOT CAUSES OF ACCIDENTS DUE TO DESIGN

EEC Note No. 14/04

Project Safbuild

Issued: October 2004
# REVIEW OF ROOT CAUSES OF ACCIDENTS DUE TO DESIGN

## Authors
- Alfred Roelen, (NLR)
- Steve Kinnersly, (AEA)
- Fabrice Drogoul

## Date
10/04

## Pages
viii+41

## Figures
1

## Tables
1

## Appendix
3

## References
43

## EEC Contact
Fabrice Drogoul

## Project
Safbuild

## Task No. Sponsor
120000-SRD-3-E1-0000

## Period
2003

## Distribution Statement:
(a) Controlled by: Head of SRT
(b) Special Limitations: None

## Descriptors (keywords):
Design, root causes of accidents, ATM, nuclear, rail, aviation

## Abstract:
This document gives the results of a study of the proportion of accidents that have their root causes in design. In particular, it investigates the validity of the claim that 60% of the root causes of accidents arise in the design stages.
This document gives the results of a review study from different industry databases of the proportion of accidents that have their root causes in design.

The review has been carried out as part of the Eurocontrol SafBuild project. SafBuild aims to establish, within the context of EEC strong designs that are resistant to failure the first place, or else tolerant to it. SAFBUILD aims to support designers in their safety role, to develop a process and supporting tools for integrating safety into the design throughout the design life cycle, leading to a safer and more resilient ATM system.

A necessary part of SafBuild is to determine the extent to which accidents are caused by design in order to provide a foundation for building safety into design.

The study reviewed accident and incident data and reports from the aviation, railway and nuclear industries. Where the data or reports indicated that design was a root cause, this was taken as adequate evidence. In cases where the data or reports did not give root causes, or where the root causes were investigated or categorised in a way that precluded the possibility of identifying design as a root cause, a judgement was made according to the available evidence.

Overall, the results show 50% of all accidents or incidents having a root cause in design. The proportions for the aviation and nuclear industries (51% and 46% respectively) are remarkably similar. In most cases, causes other than design also contributed to the accident or incident.

Typical types of design-related oversight that are root causes of accidents are:

- Use outside of the design envelope,
- Changes of operational context,
- Failure of defence in depth,
- Misconceptions between designers and operators,
- Unexpected failure mechanisms.
- Incorrect functioning leading to mistrust of safety system by operator.

Barry Kirwan
Head of SRT
Page intentionally left blank
# CONTENTS

**FOREWORD** ................................................................................................................................. v

1. Introduction ........................................................................................................................................ 1

2. Purpose of the Study .......................................................................................................................... 1

3. DESIGN stage .................................................................................................................................. 1

4. OTHER Definitions ........................................................................................................................... 2

5. Scope and Content of the Review ...................................................................................................... 3
   5.1 Overall research approach ............................................................................................................... 3
   5.2 Existing reviews ................................................................................................................................. 3
   5.3 Aviation ....................................................................................................................................... 5
   5.4 Nuclear ...................................................................................................................................... 6
   5.5 Railways ................................................................................................................................... 6

6. Findings of the Review ....................................................................................................................... 7
   6.1 Aviation ....................................................................................................................................... 7
   6.2 Nuclear ...................................................................................................................................... 7
   6.3 Railways ................................................................................................................................... 8
   6.4 Discussion ...................................................................................................................................... 8

7. Conclusions ....................................................................................................................................... 11

8. Abbreviations and acronyms ............................................................................................................ 12

9. References ....................................................................................................................................... 13

Appendix A: List of aviation accidents .................................................................................................. 17

Appendix B: List of Nuclear incidents .................................................................................................. 31

Appendix C : Railway Accidents and Incidents .................................................................................. 39
Page intentionally left blank
1. INTRODUCTION

The Eurocontrol Experimental Centre (EEC) works to improve safety in Air Traffic Management (ATM) by better integration of safety in EEC projects, by provision of better safety methods for internal and external use, and by the development and implementation of safety learning processes in the ATM industry. An important element of these safety learning processes is an awareness of the potential impact of EEC projects on aviation safety.

The aviation industry has been concentrating a lot of effort on the technical improvement of systems, but despite this, technical failures and failures that are contributed by the design still occur. While the Eurocontrol Experimental Centre is involved in many ATM system design projects, typically a lot of these projects do not lead directly to operational systems. Many are research projects that lead to prototypes for future development. Because of the specific role of EEC in the ATM system design process, it may not be clear how these research activities have an impact on aviation safety. It is essential that EEC be aware of these potential impacts to be able to build safety into the design process.

Design is complex, so is safety - what looks easy on paper may not be so in practice. One of the tasks of SAFBUILD is to determine what role design plays in accidents, and the results of this task are described in the underlying report.

2. PURPOSE OF THE STUDY

The purpose of this study is to determine how the root causes of accidents can arise from the design stages of a project and to determine the implications for EEC projects that include design. There is a lack of clarity on the precise meaning or scope of the term ‘design’. After a clarification on this topic the study reviews the root causes of accidents from databases and expert experience from a range of relevant industries.

3. DESIGN STAGE

‘Design’ is the process by which detailed specifications sufficient for unambiguous production of an entity (e.g. software item; hardware; visual display; subsystem; system) are developed to satisfy the concepts, requirements, assumptions and constraints for that entity.

It could be difficult to know who the designers really are. The design work is a diffuse distributed process. A lot of people involved in the design might not consider themselves as designer even if they are part of the activity. To clarify the position it has been decided to refer to design activity rather than designers.

Another point that needs to be clarified is the coverage given to the term design. For engineers design is often considered as one stage after requirement capture. In our safety point of view we consider design to range from concept development and requirement capture to the point of fabrication/construction.
For the sake of the study Design does not include the generation of top-level concepts, requirements, assumptions and constraints for an entity. However, the design process may:

- Generate lower level concepts, requirements, assumptions and constraints;
- Cause top-level concepts, requirements, assumptions and constraints to be questioned and modified.

Design does not include the production of the entity (e.g. software coding; production of hardware; etc.).

4. OTHER DEFINITIONS

For the purpose of this study, a definition of safety will be used that has been adopted by international organisations such as the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC). It is included in ISO/IEC Guide 51 (second edition) and is the definition of safety used by IEC 61508, the cross-industry international standard for the functional safety of electrical/electronic/programmable electronic systems.

The specific definition used in ISO/IEC Guide 51 and IEC 61508 is given below.

‘Safety’ is freedom from unacceptable risk.

‘Risk’ is a combination of the probability of occurrence of harm and the severity of the harm.

‘Harm’ is physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or the environment.

The definition of accident that is used in this research project is the following:

‘Accident’ is defined as any incident that caused harm or is likely to have caused harm in closely related circumstances.

According to this definition, events such as a train passing a signal at danger are classified as accidents, regardless of whether this event led to damage and/or injury. The root cause of such an event is not influenced by the result of the event. The use of this definition allows a comparison with e.g. the nuclear industry, where damage and injury is extremely rare.

‘Root cause in design’

Accidents typically involve a combination of errors and faults. It is in many cases not possible to assign a single, unambiguous root cause. A root cause is a condition which is necessary for an accident. Whereas each root cause is necessary, only together they are sufficient for the accident to occur.

The approach used in this study is inclusive: if at least one credible root cause of an accident lies in the design stages then the accident is considered to have had a root cause in the design stages.
5. SCOPE AND CONTENT OF THE REVIEW

5.1 Overall research approach

The issue of building safety into design has been important for regulators and industry for many years. Studies into the causes of accidents have been carried out both by regulators and the more highly regulated industries such as aviation, rail, and the nuclear industry.

The research approach for determining the ratio for root causes of accident that are in the design stages was to start with these studies and then to investigate specific domains in more detail if (a) data were available and (b) they were relevant to the EEC context.

Detailed investigations were carried out for aviation, nuclear and railways by analysing accident and incident reports.

5.2 Existing reviews

Eurocontrol in their introduction to the EATMP Safety Management Guidelines has provided data on design relation with accident/incident causes. These cite:

- 44% during specification
- 15% during design and development
- 6% installation and commissioning
- 15% in maintenance
- 20% changes after commissioning

(See figure 1)

From this it can be seen that 59% are claimed to arise during the specification and design and development phases. This slightly richer picture is in keeping with the finding in other areas\(^1\), e.g. root causes of failure in project management identifies that the largest single area of problems is in the requirements identification and documentation phases.

This view of 44% in requirements and specification and 15% in design and development significantly changes the perception of the actions which may be required to ensure improvement placing some emphasis on the specification processes.

---

\(^1\) The first interim report from the AEA Technology study also supports a similar view.
5.2.1 UK Health and Safety Executive

HSE’s publication ‘Out of Control’ publicised the details of 34 incidents from a wide range of industries that had been reported to the Heath and Safety Executive. The main purpose of the study was to raise awareness of the technical causes of control system failures. A simple classification scheme, based on a safety life cycle, was devised for analysing the causes of the incidents. The scheme includes the following phases:

1. Safety requirements specification
2. Design and implementation
3. Installation and commissioning
4. Operation and maintenance
5. Changes after commissioning

In the HSE publication, a judgement is made as to which project phase was predominant in the cause of the incident. The analysis concludes that 44% of incidents were caused by inadequate specification, and a further 15% were caused by inadequate design and implementation. This means that according to the definition of design provided in chapter 3, a total of 59% of the cases has inadequate design as a causal factor.
5.2.2 Boeing Commercial Aircraft

Boeing has examined 232 commercial jet aircraft accidents over a 10-year period (1982-1991) to develop recommendations for accident prevention strategies. The accident data base excluded events involving sabotage, suicide, terrorism, experimental testing, or direct military action. Accidents to aircraft built in the former USSR were not included. Non-flying accidents (e.g. pushback accidents) were also not included. The sequence of events was established for each accident, and events were grouped using 37 categories for accident prevention strategies. An accident prevention strategy was defined as an action which, had it been utilised, would have broken the chain of events and prevented the accident. One of the accident prevention strategies is ‘design improvement’. If a currently practicable design improvement could be envisioned that might reasonably or significantly reduce the likelihood of a future similar accident, then ‘design improvement’ was assigned as an accident prevention strategy.

The Boeing study concluded that design improvement was an accident prevention strategy in 20% of all cases.

5.3 Aviation

5.3.1 Accident inclusion criteria.

Several criteria were used to establish the final accident sample analysed in this investigation. The basic inclusion criteria were as follows:

(a) The accident resulted in 1 or more fatalities. Fatal accidents usually result in a thorough and detailed investigation and ditto investigation report.

(b) The accident involved aircraft with the following characteristics:
   • Fixed wing aircraft – helicopters are not considered
   • Aircraft heavier than 5,700 kg.

(c) The accident flight had the following characteristics:
   • Engaged in public transport
   • World-wide – no restriction on geographical location
   • Both scheduled and unscheduled flights
   • Cargo-, passenger-, positioning- and functional test flights
   • Both international and domestic flights.

(d) The accidents occurred during the time frame 1994 through 2002. This time frame is considered large enough to provide an acceptable number of accidents for this study, while at the same time the data is applicable to present day aviation.

(e) Comprehensive accident investigation information is available. The amount of detail that is needed for this analysis requires comprehensive accident investigation information. In practice, the required level of detail is only
found in (preliminary) accident investigation reports from the official accident investigation boards.

Application of the above criteria resulted in a sample of 35 accidents presented in Appendix A.

Note: While this study was limited to analysing fatal accidents, this does not mean that design does not play a role in non-fatal accidents or incidents. As a matter of fact, it can be expected that design problems play an equally important role in accidents and incidents.

5.3.2 Accident analysis protocol

The general procedure for analysing each accident included a review of the accident investigation report. The information was then interpreted on the presence of design issues as contributing or causal to the accident, using the definition of ‘design’ provided above. In determining whether an issue was causal or contributing to an accident, the findings of the accident investigation report were strictly adhered to, no ‘own’ interpretation of the cause of the accident was made.

5.4 Nuclear

A statement on incidents at nuclear installations in Britain which meet Ministerial reporting criteria, is reported to the Secretary of State for Trade and Industry and the Secretary of State for Scotland and is published every quarter by the Nuclear Safety Directorate of the Health and Safety Executive (HSE). The statement includes summary incident reports. All published incident reports covering the period September 2001 – June 2003 were included in the analysis. This resulted in a sample of 13 incidents presented in Appendix B.

5.5 Railways

Extensive and detailed data for accidents and incidents are available for railways. Accidents are the subject of detailed investigations into (among other things) root causes, including aspects of equipment and track design that may have contributed to the accident. There are, however, few accidents so meaningful statistics on the contribution due to design cannot be obtained.

There are many more incidents than accidents. Among incidents, the most important for passenger safety are signals passed at danger (SPADs). In the UK alone there are over 100 SPADs per year that either cause harm or damage or where the train goes outside the area protected by the signalling system and there is therefore the possibility of harm or damage if circumstances had been different (e.g. another train approaching). In principle, the number of SPADs would permit meaningful statistics to be derived. However, SPADs are usually investigated and analysed mainly in terms of immediate operational causes such as ‘failure to locate signal’, which can be addressed by operational measures such as procedures or training. The deeper reasons for the operational cause, for instance design features that make it difficult for a driver to respond quickly to a signal at danger, are not investigated - unless, of
course, the SPAD leads to an accident. Thus, it is not possible to assess quantitatively the contribution of design to SPADs.

Insights into how design contributes to railway accidents and incidents can, however, be obtained from investigations into accidents and from the introduction in the UK of a new safety system (Train Protection and Warning System – TPWS) to reduce the risk from SPADs. Appendix C gives relevant details of three recent fatal railway accidents and experience of the introduction of TPWS into the UK. Note that Appendix C only covers accidents in which design contributed either to the cause or severity.

6. FINDINGS OF THE REVIEW

6.1 Aviation

Of the 35 accident investigation reports investigated in this analysis, 18 reports (51%) mention design of the aircraft, design of ATM systems or design of the airport as causal or contributing to the accident.

- In 15 cases (43% of the sample), aircraft design was a causal or contributing factor.
- In 2 cases (6% of the sample), Airport design was a causal or contributing factor.
- In 1 case (3% of the sample), ATM systems design was a causal or contributing factor.

In most cases, aircraft accidents cannot be attributed to a single cause. The observation that design issues were causal or contributing to the accident does not mean that other factors (such as human factors, operational procedures, maintenance issues, etc) did not play a role in the chain of events that resulted in the accident.

6.2 Nuclear

Of the 13 incidents investigated in this analysis, 6 reports (46%) are design related. In 2 cases (15%) the Regulator required design changes to be made to the nuclear installation, In 4 cases (30%) alternative measures to prevent similar incidents have been proposed.

Similar to aviation, in most cases nuclear incidents cannot be attributed to a single cause.
6.3 Railways

The available data does not permit statistically valid conclusions to be drawn regarding the proportion of accidents or incidents due to design. However, examination of the cases given in Appendix C shows that design was a significant factor in some recent major accidents, both as a cause of the accident and its severity (e.g. passenger survivability). Data from the introduction of a new safety system (TPWS) in the UK shows that design is a contributory factor to this safety system being ineffective on 15% of the occasions it was invoked in a hazardous situation. This is because previous incorrect functioning has lead to driver mistrust.

As with aviation and nuclear, accidents and incidents cannot usually be attributed to a single cause.

6.4 Discussion

The results of the analysis of accidents and incidents in the air transport and nuclear industry carried out in this investigation show that design contributes to approximately 50% of accidents and incidents. This figure correlates well with HSE’s report ‘out of control’ which concludes that 59% of incidents from a wide range of industries has inadequate design as a causal factor. The fact that the figures correlate so well despite the variety in the types of activities is remarkable. The slightly higher percentage from the HSE study may be explained from the fact that this study focussed on failures of technical systems rather than accidents in general.

The results of the Boeing study seem to correlate less well with the findings (20% vs 50%). This may be due to the fact that the Boeing interpretation of a design related cause focuses on the design of the aircraft. Potential improvements in the design of ATC systems, design of airports and design of weather information systems are not included in the accident prevention strategy ‘design improvement. The Boeing study does however list the following separate accident prevention strategies:

- ATC system performance 13 %
- Weather information availability and accuracy 10%
- Eliminate runway hazards 7%
- Other airport 6%

This suggests that if the Boeing interpretation of a design related factor would have been expanded to include design of all elements of the aviation system, and not only design of the aircraft, a figure close to 50% would have been obtained.

For EEC it is important to have an understanding of what design practices and safety considerations are most beneficial to assuring a safe design. This requires an identification of the specific design stages where oversight happened and the types of oversights that caused accidents. Typical types of oversight are

- Design did not use accepted Standard
- Operator misunderstands or misinterprets
- Used outside design envelope
- Failure of ‘defence in depth’
- Unrevealed failures and errors
• Addition to existing system without considering whole-system design issues
• System used for unintended application
• Backup measures inadequate after equipment failure
• Failure of safety function (interlock) not revealed
• Component failure (cracking) due to poorly understood operating regime
• Infrastructure system (ventilation) made incident worse
• Infrastructure system (fire protection) fails to guarantee operation of front-line safety system

In many complex, engineered systems - such as those found in production and transportation - technical failure is relatively rare, regulatory oversight is strong, and the engineering of protective devices is highly developed. The primary source of hazards that remain now seems to lie in people's misconceptions about such systems. This includes the misconceptions of designers about operators, operators' intentions and the operating environment; and it includes the misconceptions of operators about the design, its rationale and boundaries of safe operation. These misconceptions are, moreover, related. A designer can have a misconception, for instance, about an operator's misconception about a design. It is therefore important that in the future both designers and operators can look at the historical misconceptions both of other designers and of other operators when reasoning about the risks that a system presents. Below are safety insights from other industry 'misconception' problems are relevant for ATM drawn from the complete listing shown in table 1.

- The belief that operators will seek information about the system condition – whereas they are often passive recipients
- The belief that operators will update their knowledge when they use new artifacts – whereas they sometimes rely on knowledge acquired when using old ones.
- The belief that operating conditions are benign or have little effect on the use of an artifact – whereas operators use artifacts differently in difficult conditions.
- The belief that operators have good experiential knowledge about a system's limit states – whereas operators cannot explore limit states because of the risks.
- The belief that design practices towards operating environments are general – whereas operating environments are more varied than the practices recognize.
- The belief that operating procedures can avoid a harm that is inherent in the design – whereas procedures may be too general and are often violated.
- The belief that precautionary aids will increase system reliability – whereas operators will not routinely check and operate aids not in routine use.
- The belief that emergency conditions will only be of particular kinds – whereas emergency conditions are highly unpredictable by their nature.
- The belief that operators will sustain high attention levels – whereas attention is degraded in a variety of conditions.
**Table 1:** Misconceptions of operators about the design or design intentions (HSE - Design & Ops Misconceptions - r054)

<table>
<thead>
<tr>
<th>Expectation</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms contradicting other indicators can be ignored</td>
<td>Belief that false alarms are more likely than failed indicators</td>
<td>Indicator showed pump stopped so over-temperature alarm ignored</td>
</tr>
<tr>
<td>All that needs to be known is contained in procedures</td>
<td>Belief that knowledge contained in sequential instructions is adequate</td>
<td>Followed rule that CI engines tolerable inappropriate after vapour leak</td>
</tr>
<tr>
<td>Automated systems can be substituted by manual ones</td>
<td>Belief that manual strategies can replace normally automated system</td>
<td>Failed to confirm action following instruction in manual filling operation</td>
</tr>
<tr>
<td>Everyday intuition is a good guide to hazards</td>
<td>Belief that intuitive science can predict the effect of one's actions</td>
<td>Ignored possibility of rapid corrosion generating unbreathable atmosphere</td>
</tr>
<tr>
<td>If a test for X is positive then X is true</td>
<td>Belief that positive test inevitably means hypothesis confirmed</td>
<td>Believed blockage test implicated valve when it was a relief that was blocked</td>
</tr>
<tr>
<td>The design of the system is consistently protective</td>
<td>Belief that design will be protective to a consistent degree</td>
<td>Expected that a detector that would not fully engage would still be operational</td>
</tr>
<tr>
<td>Equipment to be worked on is identifiable unambiguously</td>
<td>Belief that heuristics for identifying components will work dependably</td>
<td>Believed that label order followed order of objects that labels referred to</td>
</tr>
<tr>
<td>The past is a good guide to the future</td>
<td>Belief that past strategies can be reused if no contrary indication</td>
<td>Treated substance as though it were one normally transported by this means</td>
</tr>
<tr>
<td>The system and its safety devices work perfectly</td>
<td>Belief that precautionary systems perform perfectly, perfectly reliably</td>
<td>Expected closed isolation valves to obviate need for slip plate</td>
</tr>
<tr>
<td>There is only one indicator for every parameter</td>
<td>Belief that can rely on one indicator to monitor a performance variable</td>
<td>Failed to scan chart recorder to verify failed main instrument reading</td>
</tr>
<tr>
<td>What is available is what is needed</td>
<td>Belief that artefacts provided are for that reason suitable for the task</td>
<td>Ignored high substance concentration when used hose available to hand</td>
</tr>
<tr>
<td>When equipment stops someone carrying out their required task it is faulty</td>
<td>Belief that an object that confounds the performance of a reasonable task must have failed</td>
<td>Defeated interlock which had forgotten to activate</td>
</tr>
<tr>
<td>When the rationale for something is not obvious it does not matter</td>
<td>Belief that objects that have no obvious rationale have arbitrary functions</td>
<td>Deviated from mandated operating sequence in order to avoid effort of repeated climb</td>
</tr>
<tr>
<td>Work or attention can be offloaded onto safety systems</td>
<td>Belief that redundant precautionary systems can be used routinely</td>
<td>Used safety trip with finite reliability to routinely turn off heater when flow stopped</td>
</tr>
</tbody>
</table>
7. CONCLUSIONS

An investigation across aviation and nuclear industries confirms that approximately 50% of all accidents have a root cause in design. Data for the different types of industry are remarkably similar.

The overall detail of the information used on this study allowed identification of a number of different ways in which design can contribute to accidents. However, it did not allow classification of the failure according to the design stage or the type of safety oversight. People’s misconceptions about systems includes the misconceptions of designers about operators, operators’ intentions and the operating environment; and misconceptions of operators about the design, its rationale and boundaries of safe operation.

While safety studies and assessments are conducted with the aim of preventing similar accidents in the future, practical solutions to identified problems are usually operational, training etc, rather than redesign, so the importance of design is not always highlighted in the investigation reports. Aircraft, nuclear plants and railways are immensely complex and expensive systems, which take years to develop. Only in rare cases is a redesign of an aircraft required following an accident, the most recent example being the Concorde supersonic aircraft which underwent modifications after a crash at Paris in 2002.

The implications of this study are significant for ATM. There must be significant efforts to assure safety during the design process. This will require both traditional safety assessment methods, as well as use of best practice material and guidance on Human Factors (in particular the Human Machine Interface and working methods of controllers). The focus on Human Factors can compensate for designer and operator (controller) misconceptions. Additionally consideration needs to be given to tackling these misconceptions at the design stage, via the designers/developers themselves. This may be subject to future Safbuild research.

<table>
<thead>
<tr>
<th>Expectation</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work or attention can be</td>
<td>Belief that redundant precautionary systems can be</td>
<td>Used safety trip with finite reliability to routinely turn off</td>
</tr>
<tr>
<td>offloaded onto safety systems</td>
<td>used routinely</td>
<td>heater when flow stopped</td>
</tr>
<tr>
<td>It is reasonable to</td>
<td>Belief that under pressure the most appropriate response is</td>
<td>Removed protective mask when task required large physical</td>
</tr>
<tr>
<td>concentrate completely on a hard task</td>
<td>concentration on primary task</td>
<td>effort</td>
</tr>
<tr>
<td>The function of an object</td>
<td>Belief that function indicated by appearance is intended</td>
<td>Mistook valve for a distance piece and wrongly loosened off</td>
</tr>
<tr>
<td>can be inferred from its form</td>
<td>function</td>
<td></td>
</tr>
<tr>
<td>Operators have the knowledge to</td>
<td>Belief that risks are well enough known to permit risk taking</td>
<td>Entered swept vessel knowingly incurring risk of residual</td>
</tr>
<tr>
<td>gamble wisely</td>
<td></td>
<td>fumes</td>
</tr>
<tr>
<td>The working environment</td>
<td>Belief that the characteristics of the environment reveal the</td>
<td>Inferred from use of gas detectors prior to welding that</td>
</tr>
<tr>
<td>tells operators what hazards</td>
<td>types of hazard that are present</td>
<td>only risk from residual gas, not gas generated after welding</td>
</tr>
<tr>
<td>they face</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11
### 8. ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAB</td>
<td>Aircraft Accident Investigation Branch</td>
</tr>
<tr>
<td>AOM</td>
<td>Aircraft Operating Manual</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>BE</td>
<td>British Energy</td>
</tr>
<tr>
<td>BEGL</td>
<td>British Energy Generation Limited</td>
</tr>
<tr>
<td>BNF</td>
<td>British Nuclear Fuels</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>DME</td>
<td>Distance Measuring Equipment</td>
</tr>
<tr>
<td>EEC</td>
<td>Eurocontrol Experimental Centre</td>
</tr>
<tr>
<td>EICAS</td>
<td>Engine Indication and Crew Alerting System</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FL</td>
<td>Flight Level</td>
</tr>
<tr>
<td>HSE</td>
<td>Health and Safety Executive</td>
</tr>
<tr>
<td>ILS</td>
<td>Instrument Landing System</td>
</tr>
<tr>
<td>INES</td>
<td>International Nuclear Event Scale</td>
</tr>
<tr>
<td>IRR</td>
<td>Ionising Radiations Regulation</td>
</tr>
<tr>
<td>NII</td>
<td>Nuclear Installations Inspectorate</td>
</tr>
<tr>
<td>NTSB</td>
<td>National Transportation Safety Board</td>
</tr>
<tr>
<td>SEPA</td>
<td>Scottish Environment Protection Agency</td>
</tr>
<tr>
<td>SPAD</td>
<td>Signal Passed at Danger</td>
</tr>
<tr>
<td>TCAS</td>
<td>Traffic Alert and Collision Avoidance System</td>
</tr>
<tr>
<td>TPWS</td>
<td>Train Protection and Warning System</td>
</tr>
<tr>
<td>UKAEA</td>
<td>United Kingdom Atomic Energy Authority</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>VOR</td>
<td>VHF Omni-Directional range</td>
</tr>
</tbody>
</table>
9. REFERENCES

General


2. Health and Safety Executive, Mutual misconceptions between designers and operators of hazardous installations, J S Busby, University of Bath 2003


Aviation accident reports


8. NTSB AAR-03/02, Loss of Pitch Control on Takeoff, Emery Worldwide Airlines, Flight 17


20. Bureau Enquêtes-Accidents, Accident on 25 July 2000 at La Patte d’Oie in Gonesse (95) to the Concorde registered F-BTSC operated by Air France, report number F-SC000725A.


29. Final Aviation Accident Report, Birginair flight ALW-301, Puerto Plata, Dominican Republic, February 6, 1996, Original report published by the Junta Investigadora de Accidentes Aéreos (JIAA), Director General of Civil Aeronautics, Dominican Republic, Translated copy distributed by the Air Line Pilots Association.


35. Bundesstelle für Flugunfalluntersuchung, Status Report, AX001-1/-2/02, August 2002.


**Nuclear Incident Reports**

37. Brief reports of UK nuclear incidents reported to Government are posted on the UK Health and Safety Executive website at [http://www.hse.gov.uk/nsd/quarterly-stat/index.htm](http://www.hse.gov.uk/nsd/quarterly-stat/index.htm)
Railway Accident and Incident Reports


41. Inquiry into the Southall East Derailment. Latest information on this inquiry can be found at http://www.hse.gov.uk/railways/southalleast/index.htm


APPENDIX A: LIST OF AVIATION ACCIDENTS


   **Accident synopsis**
   
   KLM flight KL433, operated by KLM Cityhopper with a SAAB 340 B, departed Amsterdam Airport at 12:20 for a scheduled flight to Cardiff. During climb, passing flight level 165, the Master warning was triggered by the right engine oil pressure Central Warning panel light. The Captain slowly retarded the right hand power lever to flight idle and called for the emergency checklist. After completion of the emergency checklist procedure, the right hand oil pressure Central Warning panel light was still on and the Captain decided to return to Amsterdam. The right hand engine remained in flight idle during the remainder of the flight. While returning to Amsterdam, the flight was radar vectored by ATC for an ILS approach on runway 06. After passing approximately 200 ft height, the aircraft became displaced to the right of the runway and a go-around was initiated. During the go-around, control of the aircraft was lost and; at 12:26 UTC, the aircraft hit the ground, in a slight noselow attitude with approximately 80° bank to the right, approximately 560 meters to the right from the runway 06 centerline, just outside the airport. Two passengers and the Captain died in the accident, eight passengers and the First Officer were seriously injured.

   **Design related factors**
   
   A contributing factor to this accident was a lack of awareness of the consequences of an aircraft configuration with one engine in flight idle. The manufacture’s Aircraft Operating Manual (AOM) does not contain guidance material concerning the consequences of an engine in flight idle. From a certification point of view, the manufacturers AOM is part of the design of the aircraft.

2. **China Airlines, Airbus A300, B1816, Nagoya Airport, Japan, April 26, 1994.**

   **Accident synopsis**
   
   China Airlines Flight 140 took off from Taipei International Airport at 0853 UTC on April 26, 1994 for a flight to Nagoya Airport, Japan. The aircraft carried a total of 271 persons, consisting of 2 flight crew members, 13 cabin crew members and 156 passengers. While the aircraft was making an ILS approach to runway 34 of Nagoya Airport, under manual control by the First Officer (F/O), the F/O inadvertently activated the GO lever, which changed the Flight Director to GO AROUND mode and caused a thrust increase. This made the aircraft deviate above its normal glide path. The autopilots were subsequently engaged, with GO AROUND mode still engaged. Under these conditions the F/O continued pushing the control wheel in accordance with the Captain’s instructions. As a result of this, the horizontal stabilizer moved to its full nose-up position and caused an abnormal out-of-trim situation. The crew continued the approach, unaware of the abnormal situation. The angle of attack increased and the Alpha Floor function was activated and the pitch angle increased. The captain had now taken controls and initiated a go-around. The aircraft began to climb steeply with a high pitch angle attitude. The aircraft stalled and crashed. 264 persons (249 passengers and 15 crew members) were killed and 7 passengers were seriously injured.

   **Design related factors**
   
   One of the causes of the accident was the inadvertent triggering of the GO lever by the First Officer. The design of the GO lever contributed to this: normal operation of the thrust levers allows the possibility of an inadvertent operation of the GO lever.

**Accident synopsis**

On September 8, 1994, about 1903 eastern daylight time, the aircraft crashed while manoeuvring to land at Pittsburgh International Airport. The probable cause of the accident was a loss of control of the aircraft resulting from the movement of the rudder surface to its blowdown limit. The rudder surface most likely deflected in a direction opposite to that commanded by the pilots as a result of a technical malfunction of the main rudder power control unit. All 132 people on-board were killed, and the aircraft was completely destroyed.

**Design related factors**

The Boeing 737 rudder system design is not reliably redundant. As a result of this and other accidents, the NTSB has asked the FAA to require the Boeing Commercial Aircraft Group to develop design changes for the 737 series aircraft to preclude the potential for loss of control from an inadvertent rudder hardover.


**Accident synopsis**

On October 31, 1994, at 1559 Central Standard Time, an Avions de Transport Regional, model 72-212 (ATR 72), registration number N401AM, leased to and operated by Simmons Airlines, Incorporated, and doing business as American Eagle flight 4184, crashed during a rapid descent after an uncommanded roll excursion. The airplane was in a holding pattern and was descending to a newly assigned altitude of 8,000 feet when the initial roll excursion occurred. The airplane was destroyed by impact forces; and the captain, first officer, 2 flight attendants and 64 passengers received fatal injuries.

**Design related factors**

ATR failed to disseminate adequate warnings and guidance to operators about the adverse characteristics of, and techniques to recover from, ice-induced aileron hinge moment reversal events; and ATR failed to develop additional airplane modifications, which led directly to this accident.

5. **Trans World Airlines Flight 427, McDonnell-Douglas MD-82, N954U and Superior Aviation Cessna 441, N441KM, Bridgeton, Missouri, USA, November 22, 1994.**

**Accident synopsis**

On November 22, 1994, at 2203 central standard time, Trans World Airlines flight 427, a McDonnell Douglas MD-82, collided with a Cessna 441 at the intersection of runway 30R and taxiway Romeo, at the Lambert – St. Lois International Airport (STL) in Bridgeton, Missouri. The MD-82 was operating as a regularly scheduled passenger flight from STL to Denver, Colorado. There were 132 passengers, 5 flight attendants and 3 flight crew members aboard the airplane. The MD-82 sustained substantial damage during the collision. The Cessna 441, operated by Superior Aviation as a positioning flight, was destroyed. The commercial pilot and a passenger were the sole occupants on board the Cessna and were killed. Of the 140 persons on board the MD-82, eight passengers sustained minor injuries during the evacuation.

**Design related factors**

Design was not a factor.

Accident synopsis
At approximately 0922 hours on Friday 9 June 1995 a de Havilland DHC-8 aircraft, ZK-NEY, collided with the terrain some 16 km east of Palmerston North Aerodrome while carrying out an instrument approach. During the approach, the landing gear did not come down properly and the flight crew was trying to follow the alternate gear extension procedure while continuing the approach. One crew member and three passengers lost their lives and two crew members and twelve passengers were seriously injured in the accident.

Design related factors
Design was not a factor.


Accident synopsis
On August 21, 1995, about 1253 eastern daylight time, an Embraer EMB-120RT, N256AS, airplane operated by Atlantic Southeast Airlines Inc., (ASA) as ASE flight 529, experienced the loss of a propeller blade from the left engine propeller while climbing through 18,100 feet. The airplane then crashed during an emergency landing near Carrollton, Georgia, about 31 minutes after departing the Atlanta Hartsfield International Airport, Atlanta, Georgia. The flight was a scheduled passenger flight from Atlanta to Gulfport, Mississippi, carrying 26 passengers and a crew of 3, operating according to instrument flight rules, under the provisions of Title 14 Code of Federal Regulations Part 135. The flightcrew declared an emergency and initially attempted to return to Atlanta. The flightcrew then advised that they were unable to maintain altitude and were vectored by air traffic control toward the West Georgia Regional Airport, Carrollton, Georgia, for an emergency landing. The airplane continued its descent and was destroyed by ground impact forces and postcrash fire. The captain and four passengers sustained fatal injuries. Three other passengers died of injuries in the following 30 days. The first officer, the flight attendant, and 11 passengers sustained serious injuries, and the remaining 8 passengers sustained minor injuries.

Design related factors
Design was not a factor.


Accident synopsis
At 2142 eastern standard time, on December 20, 1995, American Airlines Flight 965, a Boeing 757-223, N651AA, on a regularly scheduled passenger flight from Miami International Airport, Florida, U.S.A., to Alfonso Bonilla Aragon International Airport, in Cali, Colombia, operating under instrument flight rules, crashed into mountainous terrain during a descent from cruise altitude in visual meteorological conditions. The accident site was near the town of Buga, 33 miles northeast of the Cali. The airplane impacted at about 8,900 feet mean sea level, near the summit of El Deluvio and approximately 10 miles east of Airway W3. Of the 155 passengers, 2 flightcrew members, and 6 cabincrew members on board, 4 passengers survived the accident.
Design related factor
Contributing to the cause of the accident was the aircraft’s Flight Management System logic that dropped all intermediate fixes from the display(s) in the event of execution of a direct routing.

Accident synopsis
On February 6, 1996, at approximately 03:45 UTC, a Boeing 757 operated by Birginair as a charter flight crashed minutes after take-off from Gregario Luperón Airport, Puerto Plata, Dominican Republic. The crew lost control over the aircraft after confusion due to an erroneous airspeed indication that was caused by a blocked pitot tube. The aircraft was destroyed and 176 passengers and 13 crewmembers were killed.

Design related factors
Additional factor to the accident: The EICAS system of the Boeing 757/767 aircraft does not include an alert of ‘caution’ or ‘warning’ when a signal of erroneous airspeed is detected. Additional factor to the accident: The Operations Manual of the Boeing 757/767 did not contain detailed information to provide the flight crew with a list of appropriate verifications, to signal a discrepancy in the indications of airspeed, simultaneous activation of rudder/mach trim and other EICAS warnings, and a flight with an airspeed indicator that might not be trustworthy.

Accident synopsis
On May 11, 1996, at 14:13:42 eastern daylight time, a Douglas DC-9-32 crashed into the Everglades about 10 minutes after takeoff from Miami International Airport, Miami, Florida. The crash resulted from a fire in the airplane’s class D cargo compartment that was initiated by the actuation of one or more oxygen generators being improperly carried as cargo. by The airplane, N904VJ, was being operated by ValuJet Airlines, Inc., as flight 592. Both pilots, the three flight attendants, and all 105 passengers were killed. Visual meteorological conditions existed in the Miami area at the time of the takeoff. Flight 592, operating under the provisions of 14 CFR Part 121, was on an instrument flight rules flight plan destined for the William B. Hartsfield International Airport, Atlanta, Georgia.

Design related factors
One of the causes of the accident was the failure of the FAA to require smoke detection and fire suppression systems in class D cargo compartments.

Accident Synopsis
On July 17, 1996, at about 2031 eastern daylight time and 12 minutes after take-off from New York’s JFK airport the aircraft’s center wing fuel tank exploded. The aircraft broke-up in mid air and subsequently crashed in the Atlantic Ocean. All 230 people on board were killed, and the aircraft was destroyed.

Design related factors
Contributing to the accident was the design concept that fuel tank explosions could be prevented solely by precluding all ignition sources and the design of the Boeing 747 with
heat sources located beneath the center wing tank with no means to reduce the heat transferred into the centre wing tank or to render the fuel vapour in the tank non-flammable.

11. TAM Flight 402, Fokker-100, PT-MRK, São Paulo, Brazil, October 31, 1996.

Accident synopsis
On October 31, 1996, TAM flight 402 was performing a regular passenger flight from São Paulo to Rio de Janeiro. During take-off, immediately after leaving the ground, a series of uncommented thrust reverser deployments of the right hand engine started. During the next 24 seconds of flight, the aircraft drifted towards the right, maintaining itself at low height and speed, reaching an attitude of pronounced tilting to the right and eventually colliding with the ground. All 89 passengers and 6 crewmembers died in the accident, in addition to four people on the ground.

Design related factors
Contributing to the accident were design deficiencies to the Fokker 100 thrust reverser system.


Accident synopsis
On December 22, 1996, at 1810 eastern standard time, a Douglas DC-8-63, N827AX, operated by ABX Air Inc. (Airborne Express) impacted mountainous terrain in the vicinity of Narrows, Virginia, while on a post-modification functional evaluation flight. Control was lost during a stall recovery attempt. The three flightcrew members and three maintenance/avionics technicians on board were fatally injured. The airplane was destroyed by the impact and a postcrash fire.

Design related factors
Design was not a factor.


Accident synopsis
About 1554 eastern standard time, on January 9, 1997, an Embraer EMB-120RT, N265CA, operated by COMAIR Airlines, Inc., as flight 3272, crashed during a rapid descent after an uncommanded roll excursion near Monroe, Michigan. Flight 3272 was being operated under the provisions of Title 14 Code of Federal Regulations Part 135 as a scheduled, domestic passenger flight from the Cincinnati/Northern Kentucky International Airport, Covington, Kentucky, to the Detroit Metropolitan/Wayne County Airport, Detroit, Michigan. The flight departed Covington, Kentucky, about 1508, with 2 flightcrew members, 1 flight attendant, and 26 passengers on board. There were no survivors. The airplane was destroyed by ground impact forces and a postaccident fire.

Design related factors
One of the causes of this accident was the FAA’s failure to establish adequate aircraft certification standards for flight in icing conditions.


Accident synopsis
On August 6, 1997, about 0142:26 Guam local time, Korean Air flight 801, a Boeing 747-3B5B (747-300), Korean registration HL7468, operated by Korean Air Company, Ltd.,
crashed at Nimitz Hill, Guam. Flight 801 departed from Kimpo International Airport, Seoul, Korea, with 2 pilots, 1 flight engineer, 14 flight attendants, and 237 passengers on board. The airplane had been cleared to land on runway 6 Left at A.B. Won Guam International Airport, Agana, Guam, and crashed into high terrain about 3 miles southwest of the airport. Of the 254 persons on board, 228 were killed, and 23 passengers and 3 flight attendants survived the accident with serious injuries. The airplane was destroyed by impact forces and a postcrash fire.

Design related factors
Design was not a factor.


Accident synopsis
On August 7, 1997, at 1236 eastern daylight time, a Douglas DC-8-61, N27UA, operated by Fine Airlines Inc. (Fine Air) as flight 101, crashed after takeoff from runway 27R at Miami International Airport, Miami, Florida. The accident resulted from the airplane being misloaded to produce a more aft center of gravity and a correspondingly incorrect stabilizer trim setting that precipitated an extreme pitch-up at rotation. The three flightcrew members and one security guard on board were killed, and a motorist was killed on the ground. The airplane was destroyed by impact and a postcrash fire.

Design related factors
Design was not a factor.


Accident synopsis
SilkAir flight MI 185 was operating as a scheduled passenger flight from Jakarta Soekarno-Hatta International Airport to Singapore Changi Airport. The flight departed about 15:37 local time with 97 passengers, five cabin crew and two cockpit crew. The airplane descended from its cruising altitude of 35,000 feet and impacted the Musi river, near the village of Sunsang, about 30 nautical miles north-north-east of Palembang in South Sumatra. Visual meteorological conditions prevailed for the flight, which operated on an instrument flight rules flight plan. Prior to the sudden descent from 35,000 feet, the flight data recorders stopped recording at different times. There were no mayday calls transmitted from the airplane prior or during the descent. All 104 persons on board did not survive the accident, and the airplane was completely destroyed by impact forces.

The Indonesian NTSC concluded that the technical investigation has yielded no evidence to explain the cause of the accident.

The US NTSB has responded to the draft final accident report by stating that the examination of all of the technical evidence is consistent with the conclusions that 1) no airplane related mechanical malfunctions or failures caused or contributed to the accident, and 2) the accident can be explained by intentional pilot action.

Design related factors
Design was not a factor.

Accident synopsis
On 2 September 1998, Swissair Flight 111 departed New York, United States of America, at 2018 eastern daylight savings time on a scheduled flight to Geneva, Switzerland, with 215 passengers and 14 crew members on board. About 53 minutes after departure, while cruising at flight level 330, the flight crew smelled an abnormal odour in the cockpit. Their attention was then drawn to an unspecified area behind and above them and they began to investigate the source. Whatever they saw initially was shortly thereafter no longer perceived to be visible. They agreed that the origin of the anomaly was the air conditioning system. When they assessed that what they had seen or were now seeing was definitely smoke, they decided to divert. They initially began a turn toward Boston; however, when air traffic services mentioned Halifax, Nova Scotia, as an alternative airport, they changed the destination to the Halifax International Airport. While the flight crew was preparing for the landing in Halifax, they were unaware that a fire was spreading above the ceiling in the front area of the aircraft. About 13 minutes after the abnormal odour was detected, the aircraft's flight data recorder began to record a rapid succession of aircraft systems-related failures. The flight crew declared an emergency and indicated a need to land immediately. About one minute later, radio communications and secondary radar contact with the aircraft were lost, and the flight recorders stopped functioning. About five and one-half minutes later, the aircraft crashed into the ocean about five nautical miles southwest of Peggy's Cove, Nova Scotia, Canada. The aircraft was destroyed and there were no survivors.

Design related factors
Findings as to causes: use of flammable material in the aircraft contributed to the propagation and the intensity of the fire, use of circuit breakers that were not capable of protecting against all types of wire arcing events, the fire initiation event was likely an arcing event of a in-flight entertainment system power supply cable, the lack of built-in smoke and fire detection suppression devices allowed the fire to propagate unchecked until it became uncontrollable.


Accident synopsis
On 12 January 1999, at 1614 hrs, the Channel Express flight departed Luton airport for a cargo flight to Guernsey. During the final stages of the approach to Guernsey, moments after the wing flaps were lowered to their fully down position, the nose of the aircraft rose and the crew were unable to prevent it rising further. The nose continued to rise until the aircraft's pitch attitude was near vertical. Although the crew applied nose down pitch trim and high engine power, the aircraft lost flying speed, stalled and entered an incipient spin. It descended in a shallow nose down pitch attitude with little forward speed and crashed at the rear of a private house, striking the house with its port wing. Both the house and the aircraft caught fire. The two pilots were killed but the sole occupant of the house escaped without physical injury.

Design related factors
Design was not a factor.

**Accident synopsis**
On June 1, 1999, at 2350:44 central daylight time, American Airlines flight 1420, a McDonnell Douglas DC-9-82 (MD-82), N215AA, crashed after it overran the end of runway 4R during landing at Little Rock National Airport in Little Rock, Arkansas. Flight 1420 departed from Dallas/Fort Worth International Airport, Texas, about 2240 with 2 flight crewmembers, 4 flight attendants, and 139 passengers aboard and touched down in Little Rock at 2350:20. After departing the end of the runway, the airplane struck several tubes extending outward from the left edge of the instrument landing system localizer array, located 411 feet beyond the end of the runway; passed through a chain link security fence and over a rock embankment to a flood plain, located approximately 15 feet below the runway elevation; and collided with the structure supporting the runway 22L approach lighting system. The captain and 10 passengers were killed; the first officer, the flight attendants, and 105 passengers received serious or minor injuries; and 24 passengers were not injured. The airplane was destroyed by impact forces and a postcrash fire.

**Design related factors**
Design was not a factor.


**Accident synopsis**
On 14 September 1999, the aircraft performed flight OAL3838, from Athens to Bucharest as a government flight. During climb, after flap and slats were retracted, the flight crew noticed illumination of the “PITCH FEEL” light on the warning panel. The “PITCH FEEL” warning light, remained continuously ON during cruise and descent until the slats were extended. During descent the Indicated Air Speed (IAS) increased from 240 Kts to 332 Kts. Approaching FL 150, the first officer requested a further descent. Just before FL 150 the ATC re-cleared OAL3838 to continue descent to FL 50. One second later, the autopilot disengaged and for the next 1 minute and 36 seconds the aircraft was manually flown by the Captain. Between FL 150 and FL 140, for approximately 24 seconds, the aircraft experienced 10 oscillations in the pitch axis which exceeded the limit manoeuvring load factor. Maximum recorded values of the vertical accelerations recorded by an accelerometer located in the landing gear bay were: +4.7 g and -3.26 g. Due to accelerations occurring during the pitch oscillations the passengers (who were not wearing seatbelts) were thrown against the cabin ceiling and aircraft furniture. This caused fatal injuries to 7 passengers, serious injuries to 1 crew member and 1 passenger and minor injuries to 2 passengers.

**Design related factors**
Causal factor of the accident was an inadequate risk assessment of the PITCH FEEL malfunctions.

21. EgyptAir Flight 990, Boeing 767-366ER, SU-GAP, 60 Miles South of Nantucket, Massachusetts, USA, October 31, 1999.

**Accident synopsis**
On October 31, 1999, about 0152 eastern standard time (EST), EgyptAir flight 990, a Boeing 767-366ER (767), SU-GAP, crashed into the Atlantic Ocean about 60 miles south of Nantucket, Massachusetts. EgyptAir flight 990 was being operated as a scheduled, international flight from John F. Kennedy International Airport (JFK), New York, New York, to Cairo International Airport, Cairo, Egypt. The flight departed JFK about 0120,
with 4 flight crewmembers, 10 flight attendants, and 203 passengers on board. All 217 people on board were killed, and the airplane was destroyed. The aircraft crashed into the ocean as a result of the relief first officer's flight control inputs.

Design related factors
Design was not a factor.


Accident synopsis
On 22 November 1999 the ATR 42 chartered by the World Food Program was going to land at Pristina after a flight from Rome. The meteorological conditions at the aerodrome corresponded to visibility of four thousand metres with a layer of compact clouds at three thousand feet. In radar and radio contact with the military air traffic control organisation for an ILS approach, the aircraft, which was outbound to the north at an altitude of 4,600 feet, entered a sector where the minimum safety altitude is 6,900 feet and struck a mountain whose peak is at 4,650 while turning to return towards the airport. The 3 crewmembers and 21 passengers on-board the aircraft were killed and the aircraft was totally destroyed by the impact.

Design related factors
Design was not a factor.


Accident synopsis
At 1727 hrs, the aircraft was ready to depart. However, there were delays caused by various factors outside of the crew's control and they were not cleared to taxi until 1825 hrs. By 1835 hrs, the crew had contacted the 'Tower' and were instructed: "AFTER THE NEXT LANDING AIRCRAFT ON FINAL LINE UP AND WAIT RUNWAY 23". Subsequently, at 1836 hrs HL-7451, using the callsign KAL 8509 was cleared to take off with a reported surface wind of 190°/18 kt. The Tower controller considered that the takeoff was normal and the aircraft disappeared from sight as it entered the cloud base at about 400 feet agl. At 1838 hrs, as the aircraft indicated altitude passed 1,400 feet, KAL 8509 was transferred to 'London Control' on frequency 118.82 MHz. The crew had been cleared for a departure procedure, which required a left turn at 1.5 nm from the Stansted DME (co-incident with the 152° radial from Barkway VOR) onto a radial of 158° to the Detling VOR. No radio calls were heard from the aircraft subsequent to the frequency transfer instruction from 'Stansted Tower'. The ATC personnel in the 'Tower' then saw an explosion to the south of the airport and immediately implemented their emergency procedures. The four persons on board the aircraft, the three flight crew members and the company ground engineer, were fatally injured during the impact.

Investigations revealed that, throughout the accident flight, the captain's ADI indicated the correct pitch attitude but that the roll attitude remained at a wings level indication. Radar and Flight Data Recorder data showed that the aircraft commenced a turn to the left but that this turn was continuous until impact with the ground. At impact, the aircraft was assessed to be pitched approximately 40° nose down, banked close to 90° to the left and with a speed in the region of 250 to 300 kt.

Design related factors
Design was not a factor.

**Accident Synopsis**
The aircraft took off from Tripoli International airport enroute to Marsa Brega at 0929 UTC with 38 passengers and 3 crew members. While the aircraft was on final approach, preparing for landing, at about 4.5 nm from the airport, the left engine flamed out followed by the right engine. The aircraft ditched in the sea and sank in a few minutes. Twenty passengers and one crewmember were killed, eleven passengers and 2 crew members were seriously injured. The engine flameouts were caused by the failure of the crew to operate the engine anti-icing system.

**Design related factors**
Design was not a factor.


**Accident synopsis**
On January 31, 2000, about 1621 Pacific standard time, Alaska Airlines, Inc., flight 261, a McDonnell Douglas MD-83, N963AS, crashed into the Pacific Ocean about 2.7 miles north of Anacapa Island, California. The crash was caused by a loss of airplane pitch control resulting from the in-flight failure of the horizontal stabilizer trim system jackscrew assembly’s acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airline’s insufficient lubrication of the jackscrew assembly. The 2 pilots, 3 cabin crewmembers, and 83 passengers on board were killed, and the airplane was destroyed by impact forces. Flight 261 was operating as a scheduled international passenger flight under the provisions of 14 Code of Federal Regulations Part 121 from Lic Gustavo Diaz Ordaz International Airport, Puerto Vallarta, Mexico, to Seattle-Tacoma International Airport, Seattle, Washington, with an intermediate stop planned at San Francisco International Airport, San Francisco, California.

**Design related factors**
Contributing to the accident was the absence on the McDonnell Douglas MD-80 of a fail-safe mechanism to prevent the catastrophic effects of total acme nut thread loss on the horizontal stabilizer jackscrew assembly.


**Accident synopsis**
On February 16, 2000, about 1951 Pacific standard time, Emery Worldwide Airlines, Inc., (Emery) flight 17, a McDonnell Douglas DC-8-71F (DC-8), N8079U, crashed in an automobile salvage yard shortly after takeoff, while attempting to return to Sacramento Mather Airport (MHR), Rancho Cordova, California, for an emergency landing. Emery flight 17 was operating as a scheduled cargo flight from MHR to James M. Cox Dayton International Airport, Dayton, Ohio. The flight departed MHR about 1949, with two pilots and a flight engineer on board. Shortly after take-off, there was a loss of pitch control resulting from the disconnection of the right elevator control tab. The disconnection was caused by the failure to properly secure and inspect the attachment bolt. The three flight crewmembers were killed, and the airplane was destroyed.
Design related factors
The circumstances of the Emery flight 17 accident show that the current DC-8 design does not preclude a catastrophic result from a disconnection or failure of the existing control tab crank fitting to pushrod attachment. Therefore, the National Transportation Safety Board believes that the FAA should require Boeing to redesign DC-8 elevator control tab installations and require all DC-8 operators to then retrofit all DC-8 airplanes with these installations such that pilots are able to safely operate the airplane if the control tab becomes disconnected from the pushrod.

Accident synopsis
On May 25, 2000, The MD 83 registered F-GHED was cleared to take off from runway 27 at Paris Charles de Gaulle Airport. The Shorts 330 registered G-SSWN was then cleared to line up and to wait as “number two”. The controller believed that the two aircraft were at the threshold of the runway, whereas the Shorts had been cleared to use an intermediate taxiway. The Shorts entered the runway at the moment the MD 83 was reaching its rotation speed. The tip of the MD 83’s left wing went through the Shorts 330’s cockpit and hit both pilots. The MD 83 aborted its takeoff. The captain of the Shorts was killed, the first officer was seriously injured. The tip of the left wing of the MD 83 was damaged. The Shorts 330 starboard engine nacelle was deformed and the cockpit was partly destroyed.

Design related factors
Contributing factor: the radar information from the ASTRE and AVISO systems was difficult to see from the position of the tower controller.

Accident synopsis
On 17th July, 2000, Alliance Air flight CD-7412, a Boeing 737-200 ADV aircraft VT-EGD crashed at 0734 hrs. (IST) while on approach to Patna airport. The flight had taken off from Kolkata at 0650 hrs and was on a scheduled flight to Delhi via Patna and Lucknow. Two Pilots, four Air-hostesses and 52 passengers were on board. Patna weather was clear with a visibility of four kilometers. Approximately 30 seconds prior to the crash, the crew requested a 360° turn due to being high on approach and were cleared by the Air Traffic Controller on duty. The aircraft stalled shortly after commencing the 360° turn and crashed in the Gardani Bagh residential area. All the crew and 49 passengers were killed as a result of the crash. The aircraft was completely destroyed by the crash and post crash fire. Five persons on the ground lost their lives.

Design related factors
Design was not a factor.

Accident synopsis
On 25 July 2000, an Air France Concorde crashed immediately after take-off from runway 26 R at Paris Charles de Gaulle Airport. During take-off, shortly before rotation, the front right tyre (tyre No 2) of the left landing gear ran over a strip of metal, which had fallen from another aircraft, and was damaged. Debris was thrown against the wing structure leading to a rupture of tank 5. A major fire, fuelled by the leak, broke out almost immediately under the left wing. Problems appeared shortly afterwards on engine 2 and for a brief period on...
The aircraft took off. The crew shut down engine 2, then only operating at near idle power, following an engine fire alarm. They noticed that the landing gear would not retract. The aircraft flew for around a minute at a speed of 200 kt and at a radio altitude of 200 feet, but was unable to gain height or speed. Engine 1 then lost thrust, the aircraft's angle of attack and bank increased sharply. The thrust on engines 3 and 4 fell suddenly. The aircraft crashed onto a hotel. All 9 crewmembers and 100 passengers on board and 4 people on the ground were killed. 6 people on the ground were injured. The aircraft was destroyed.

Design related factors
The certificates of airworthiness for Concorde were suspended until the following measures had been taken:

- Installation of flexible linings in tanks 1, 4, 5, 6, 7, and 8.
- Reinforcement of the electrical harnesses in the main landing gear bays.
- Modification of the Flight Manual procedures so as to inhibit power supply to the brake ventilators during critical phases of flight and revision of the Master Minimum Equipment List to ensure that technical operational limitations cannot be applied for the tyre under-pressure detection system.
- Installation of Michelin NZG tyres and modification of the anti-skid computer.
- Modification of the shape of the water deflector and removal of the retaining cable.
- A ban on the use of volatile fuels and increase in the minimum quantity of fuel required for a go-around.


Accident synopsis
On 23 August 2000, about 1930 Bahrain local time, Gulf Air flight 072, (GF-072) an Airbus A320-212, Sultanate of Oman registration A40-EK, crashed in the Arabian Gulf near Muharraq, Bahrain. GF-072 departed from Cairo International Airport, Cairo, Egypt, with 2 pilots, 6 cabin crew, and 135 passengers on board, for Bahrain International Airport, Muharraq, Kingdom of Bahrain. GF-072 was operating as a regularly scheduled international passenger service flight under the Convention on International Civil Aviation and the provisions of Sultanate of Oman Civil Aviation Regulations Part 121 and was on an instrument flight rules flight plan. The airplane had been cleared to land on Runway 12 at BAH, but crashed at sea about 3 miles north-east of the airport soon after initiating a go-around following the second landing attempt. The airplane was destroyed by impact forces, and all 143 persons on board were killed. Night, visual meteorological conditions existed at the time of the accident.

Design related factors
Design was not a factor.


Accident synopsis
On October 31, 2000, at 1517 UTC, 2317 Taipei local time, Singapore Airlines Flight SQ006, a Boeing 747-400 aircraft, crashed on a partially closed runway at Chiang Kai-Shek (CKS) International Airport during take-off. Heavy rain and strong winds from typhoon "Xangsane" prevailed at the time of the accident. SQ006 was on a scheduled passenger flight from CKS Airport, Taoyuan, Taiwan, Republic of China (ROC) to Los Angeles International Airport, Los
Angeles, California, USA. The flight departed with 3 flight crewmembers, 17 cabin crewmembers, and 159 passengers on-board.

The aircraft was destroyed by its collision with construction equipment and runway construction pits on Runway 05R, and by post crash fire. There were 83 fatalities, including 4 cabin crewmembers and 79 passengers, 39 seriously injured, including 4 cabin crewmembers and 35 passengers, and 32 minor injuries, including 1 flight crewmember, 9 cabin crewmembers, and 22 passengers.

Design related factors
Findings related to risk: At the time of the accident, there were a number of items of CKS Airport infrastructure that did not meet the level of internationally accepted standards and recommended practices. Among these items were:

- There should have been 16 centreline lights spaced 7.5 meters apart along a particular section of Taxiway N1 rather than 4 centreline lights spaced at 30 meters, 55 meters, 116 meters and 138 meters.
- Segments of the straight portion of the taxiway centreline marking did not extend all the way down to the runway.
- Runway guard lights and stopbars were not provided.
- Alternate green/yellow taxiway centreline lights to demarcate the limits of the ILS sensitive area were not installed.
- The mandatory guidance lights installed on the left and the right sides of taxiway N1 were located after the holding position for runway 05L and were not collated with the runway holding position marking.
- There was no interlocking system installed at CKS airport to preclude the possibility of simultaneous operation of the runway lighting and the taxiway centreline lighting.


Accident synopsis
A crew of two was operating the aircraft on a scheduled mail service from Edinburgh Airport to Belfast International Airport, with 1,040 kg of cargo aboard. The aircraft, a twin engined turboprop type, suffered a double engine flameout shortly after takeoff. The flight crew ditched the aircraft in shallow water in the Firth of Forth, close to the shoreline. The aircraft was severely damaged on impact with the water and the forward fuselage section became submerged. Neither crew member survived. The engines had flamed out because a significant amount of snow entered into the engine air intakes as a result of the aircraft being parked heading directly into strong surface winds during conditions of light to moderate snowfall overnight.

Design related factors
Design was not a factor.


Accident synopsis
On October 8, 2001, SAS flight 686 taxied to Milan Linate’s Runway 36R for departure. At the same time, a Cessna CitationJet received instructions to taxi out from the general aviation ramp “north via Romeo 5”. The Citation crew were instructed to “call back at the stop bar of the main runway extension”. The CitationJet crew acknowledged “Roger, Romeo 5 and call you back before reaching the main runway”. Unchallenged by the controller, the
CitationJet taxied to the east via taxiway Romeo 6. The MD-87 was instructed to line up and wait on runway 36R. The Citation crew reported approaching Sierra and they were told to hold at the stop bar. The ground controller then cleared them to “continue your taxi on to the main apron”. Ten seconds later flight SK 686 was cleared for take-off. Immediately after rotation, the MD-87 collided with the CitationJet. The MD-87 remained airborne for a few seconds and then crashed into a baggage handling building. All 104 passengers and 6 crewmembers on board the MD-87 and 4 occupants of the CitationJet were killed, as well as 4 ground staff. An additional 4 ground staff were injured.

Design related factors
Airport markings and signs were not fully compliant to ICAO Annex 14.


Accident synopsis
Bashkirian Airlines flight 2927 was operating on a charter flight from Moscow to Barcelona. The aircraft has just been handed over to the Swiss Air Traffic Control when the Tupolev’s TCAS gave a traffic advisory against probable conflicting traffic. Seven seconds later, ACC Zurich instructed the crew of the Tupolev to conduct an ‘expedite descent’ from FL 360 to FL 350 and advised the crew of the conflicting traffic. This descent was needed to achieve a vertical separation with respect to a DHL Boeing 757 cargo aircraft en-route from Bergamo to Brussels. The Tupolev crew initiated a descent. Simultaneously, the Tupolev’s TCAS issued the command to climb. Another seven seconds later the radar controller repeated his instruction to the Tupolev crew to conduct an ‘expedite descent’ to FL 350, which was immediately acknowledged by the crew. Nineteen seconds later the Tupolev’s TCAS commanded to ‘increase climb’. On board the DHL aircraft, the TCAS had first alerted the crew of probable conflicting traffic simultaneously with the Tupolev’s initial TCAS traffic advisory. The Boeing’s TCAS then issued an avoidance command to descend, which was immediately followed by the crew. Fifteen seconds later the Boeing’s TCAS commanded to increase the descent. The crew reported to ACC Zurich that they had initiated a TCAS descent. At 23:36 both aircraft collided. The two flight crew on board the Boeing were killed, as well as the 12 flight crew and 57 passengers on-board the Tupolev.

Design related factors
Design was not a factor.
APPENDIX B: LIST OF NUCLEAR INCIDENTS

INCIDENT 00/4/1

SELLAFIELD (British Nuclear Fuels plc)

Incident synopsis
A loss of electrical supplies to a large portion of the Sellafield site was experienced during Monday 9th October 2000. The failure centred on faults experienced on a new section of 11kV switchgear. Supplies were re-established within 47 minutes of the loss, well within the two hours allowed for in the safety case.
The actions of BNFL during the recovery phase from the incident were found to be generally commendable, ensuring reinstatement of electrical supplies to the affected area well within the time allowed in the safety case.
An NII team carried out an initial investigation into the incident. It concluded that the direct cause was a defective component in new electrical switchgear being installed as part of a project to update the electrical infrastructure on the site. The work was being carried out by Norweb, as contractors to BNFL, to arrangements that were regarded as standard practice for this sort of work.
BNFL also carried out an investigation, which came to similar conclusions.
The incident was classified as Level 1 on the International Nuclear Events Scale (INES).

Design related factor
Design was not a factor

INCIDENT 01/1/1

HUNTERSTON B (British Energy Generation (UK) plc)

Incident synopsis
During routine monitoring of Hunterston B, it was discovered that there was radioactivity in the ground water in the bore holes associated with reactor 4. This event was reported under the site arrangements, initially to the Nuclear Installations Inspectorate (NII) and Scottish Environment Protection Agency (SEPA), and later to other government departments.
The licensee continues to investigate this matter with the assistance of company specialists and external contractors. The findings so far suggest that the levels of radioactivity present in the ground water are low and are decreasing. The source of the activity has not yet been conclusively identified, and this continues to be investigated by the licensee. Indications are that it was a one-off rather than continuous or recurring event.
So far there are no detectable off-site effects, and steps are being taken to remove the arisings as they build up in the bore holes. Currently the evidence suggests that this event is not of radiological significance for workers and the public.
The incident was classified as Level 1 on the International Nuclear Event Scale (INES).

Design related factor
Design was not a factor.
INCIDENT 01/1/2

SELLAFIELD (British Nuclear Fuels plc)

Incident synopsis
On 6 March 2001, during a routine glove change operation on a glovebox in the plutonium processing section of the B205 Magnox reprocessing plant at Sellafield, plutonium contamination was released into the working area. This occurred when a seal weld on a waste export bag failed, releasing contaminated waste items onto the floor. Two workers were exposed to elevated levels of airborne plutonium, and BNFL’s early estimate is that they have each received an effective internal exposure of about 4 mSv. BNFL’s best estimate of the amount of radioactive material spilled is 24 MBq of plutonium-239 and 720 MBq of plutonium-241. This is 24 times the reporting level specified in IRR99 for plutonium-239 and seven times that specified for plutonium-241. BNFL has recovered the spilled material and decontaminated the working area. There was no release of radioactivity to the environment following the event or during the clean up activities. HSE investigated the event and required BNFL to undertake a site wide review of similar operations. This confirmed that there was a wide variation in the methods used for work within plutonium gloveboxes on the site. BNFL has developed an action plan to prevent a recurrence in B205. In addition, BNFL is reviewing its methods for carrying out plutonium glovebox operations. HSE is considering taking formal regulatory action. The incident was classified as Level 1 on the International Nuclear Event Scale (INES).

Design related factor
Design was not a factor.

INCIDENT 01/1/3

CHAPELCROSS (British Nuclear Fuels plc)

Incident synopsis
During refuelling operations on Reactor 2, an irradiated fuel element failed to release from the grab (this is used to hold an element while it is withdrawn from a reactor). Routine methods were used to release the grab. However, the irradiated fuel element snagged during the operation and was lifted out of its shielding resulting in the operators on the pile cap being exposed to the intense radiation being emitted from the irradiated fuel element. Personnel responded quickly, and the radiological dose received by them was small. The event revealed shortfalls in the safety of the refuelling operation and the licensee took the immediate step of halting all refuelling operations while it investigated the event and reviewed the safety of the equipment. The NII investigated the event and judged that it was due to inadequate design and operation of the equipment. The licensee has modified the equipment and procedures in accordance with the nuclear site licence requirements and NII has agreed to fuelling operations continuing. The incident was classified as Level 1 on the International Nuclear Event Scale (INES).

Design related factor
The NII concluded that the event was due to inadequate design and operation of the equipment.

INCIDENT 01/3/1
HEYSHAM 1 (British Energy Generation Limited)

Incident synopsis
To meet the requirements of the nuclear site licence, each of the two reactors at Heysham 1 is shutdown periodically to enable examination, inspection, maintenance or testing of safety related components that cannot be accessed when the reactor is operating. Reactor 1 was subject to a periodic shutdown in August/September 2001.

Inspections of the reactor graphite core are carried out using remote TV cameras and equipment to measure the geometry of the core components. The aim of the inspections is to confirm that the core components are performing in accordance with the predictions assumed in the safety case. During the planned inspections of the Reactor 1 core fuel channels, BEGL found cracks in some of the graphite bricks. The cracking of reactor core bricks is a known and predicted ageing condition for irradiated graphite and has been observed at other AGR stations. BEGL responded to the inspection findings in a conservative way by revisiting and updating their existing core safety case for Heysham 1. Consideration was also given to the possible implications of the inspection findings to the other operating AGRs. The BEGL review considered the inspection results against the assumptions made in the existing safety case, which included the possibility of cracks in the core bricks, and concluded that the revised core safety case was valid for a further period of operation.

Specialist graphite inspectors from the HSE's Nuclear Installations Inspectorate carried out a detailed assessment of the revised core safety case, to ensure that the required safety functionality of the reactor core would be maintained for a further period of operation. NII's assessment focussed on ensuring sufficient safety margins were available in the safety case to allow for any further cracking of the core bricks. The NII assessment concluded that the safety case was adequate to support the return to service of Heysham 1 Reactor 1 and that the safety cases for other AGR stations remained valid.

The event was classified as Level 1 on the International Nuclear Events Scale (INES).

Design related factor
Design was not a factor.

INCIDENT 01/3/2

SELLAFIELD (British Nuclear Fuels plc)

Incident synopsis
During a rainstorm on 6 July 2001, localised flooding about 10-15 centimetres deep occurred outside a laboratory complex and overflowed an external door threshold into the building. The water entered an old laboratory which is currently being decommissioned. Historic plutonium (Pu) contamination, probably from under a floor lining, was re-suspended by the flooding and spread over part of the laboratory floor. The area has subsequently been cleaned up and decontaminated. There was no release of radioactivity from the building and no radiation dose received by the workforce.

BNFL reported the incident as a spill under the Ionising Radiations Regulations 1999 (IRR99). The estimated amount of activity involved was equivalent to 10MBq of 239Pu and 200MBq of 241Pu which is respectively 10 and two times the IRR reporting level. The incident was classified as Level 1 on the International Nuclear Event Scale (INES).

BNFL carried out remedial work on the building to prevent a reoccurrence of the water ingress, and additional work is in hand to strengthen these measures. HSE's Nuclear...
Installations Inspectorate investigated the incident, and is monitoring progress with the remedial work.

Design related factor
Design was not a factor.

INCIDENT 01/3/3
CHAPEL CROSS (British Nuclear Fuels plc)

Incident synopsis
At 1.20 am on 5 July, during routine discharge operations on Reactor 3 at BNFL's Chapelcross nuclear power station, a basket containing 24 irradiated magnox fuel elements dropped. It fell about 5 feet onto a door in the pile cap floor, but was still contained within the discharge machine. BNFL stood down its Emergency Control Centre at about 6pm when it concluded that the fuel was stable and that no radioactivity had been released. On the evening of 12 July, BNFL reported that it had carried out a detailed remote TV examination, and found that 12 fuel elements were missing from the basket. After further checks, BNFL concluded that the door the basket had been resting upon must have been opened during discharge operations, and that the missing elements must have fallen about 80 feet, down the discharge shaft through which the elements are normally lowered in the baskets.

BNFL declared a site incident on 12 July in order to be better able to co-ordinate its activities. The NII set up its Response Centre and dispatched a team of inspectors to the site. NII focused upon ensuring that BNFL took appropriate steps to locate and recover the missing fuel. They recovered it safely on 17 July, and the NII was able to stand down its Response Centre as it was satisfied that no member of the public or employees had incurred any harm from the incident.

Subsequently, priority was given to regulating BNFL's recovery of the 12 irradiated fuel elements still within the discharge machine. This was achieved safely on 27 October. BNFL has embargoed routine refuelling operations at Chapelcross, and will have to provide a safety case to satisfy the NII that it can return to routine refuelling safely. Similar measures have been taken at its sister station at Calder Hall.

This incident which was classified as Level 1 on the International Nuclear Event Scale (INES).

Design related factor
Design was not a factor.

INCIDENT 01/4/1
SELLAFIELD (British Nuclear Fuels plc)

Incident Synopsis
British Nuclear Fuels reported the detection of Tc99 in groundwater taken from a borehole on its Sellafield site close to the Main Gate. This was the result for the first analysis of groundwater from this borehole for this isotope. The incident report noted that the sample may have been a false analysis. Subsequent analyses have confirmed Tc99 in this borehole and, at lesser concentration, in others in the same area. Activity has also been detected beyond the site boundary but at much lower concentrations.
The Health and Safety Executive's Nuclear Installations Inspectorate (NII) has asked BNFL to determine the source of the activity and to report the work the company is undertaking to prevent further leakage from the plant and to prevent activity leaving the site.

The company has confirmed that the probable source of activity in the ground is the sludge storage tanks in Building B241. These old tanks have been suspected to be leaking for some years and recent modifications have been made to address this. The recent detection appears to be confirmation that leaked material has reached the groundwater on the site. The fall off of activity concentration in boreholes away from the plant is consistent with B241 being the source of the activity.

To remove the potential for leakage from this old facility, BNFL proposed to commence emptying the storage tanks in 2002. The NII is currently considering the safety case for BNFL's plans to do this. The Inspectorate has requested BNFL's proposals for control of the radioactive material that has entered the ground and expects to receive this soon.

In respect of the activity detected off the site, the Environment Agency has stated that it is satisfied that the reported concentration of Tc99 is radiologically insignificant. However, until the source of the activity is known, the Agency has regulatory concern. It also has requested BNFL to undertake monitoring to confirm the point of leakage, and will work with NII to consider any regulatory action.

The incident has been classified as Level 0 (which is highest) on the International Nuclear Event Scale (INES).

Design related factor
Design is not a factor.

INCIDENT 02/1/1

Dungeness B - British Energy Generation Limited (BEGL)

Incident synopsis
In January 2002 BEGL reported two events that had each led to water leaks from joints in large diameter pipes of the Dungeness B Water Spray Fire System. In both cases, the system was removed from service to enable the leaks to be repaired. As the Water Spray Fire System protects safety-related equipment from fire, the reactors were shut down to maintain nuclear safety. The Nuclear Installations Inspectorate (NII) Site Inspector's initial investigation raised a number of concerns with respect to the adequacy of the Water Spray Fire System. A Direction to review and reassess safety was issued under Licence Condition 15(4). The results of this were reported to NII by the end of March 2002 as required. BEGL has already made some improvements to the system and the Site Inspector is continuing with his investigations.

Design related factor
A number of concerns with respect to the adequacy of the Water Spray Fire System were raised.

INCIDENT 02/1/2

HEYSHAM 1 - British Energy Generation Limited (BEGL)

Incident synopsis
British Energy reported an event at Heysham 1 on 11 March involving a fuelling machine operation at a Fuel Storage Tube. The machine had collected a new fuel assembly from the
tube and had replaced this with a short shield plug. Unknown to the operators, and contrary to the indications at the fuelling machine, the shield plug had not disconnected from the machine grab. A mechanical interlock designed to prevent the machine moving until safe to do so had failed. This allowed the machine to move sideways which resulted in impact between the shield plug and the storage tube. The shield plug was severed into two parts with the lower part falling into the storage tube.

The NII Site Inspector visited the site within a few hours of the event being reported. He confirmed that the nuclear safety significance of the actual event was low, but that it could have been more serious if the fuelling machine had been operating at the reactor. There are, however, other interlocks to provide protection in this case. He also confirmed that a full investigation was underway and that the refuelling safety case would be revalidated before the machine was used again over the reactor. The event was subsequently categorised as a level 2 event (an incident) on the internationally used INES scale of nuclear events, due to the implications of multiple failures of safety provisions.

**Design related factor**
A mechanical interlock designed to prevent the machine moving until safe to do so had failed.

**INCIDENT 02/3/1**

Torness - British Energy (BE)

**Incident synopsis**
The sudden and extensive failure of a gas circulator at Torness in May 2002 was thought, from forensic evidence, to be linked to the development of an unexpected fatigue related crack in part of the impeller. In August, another gas circulator on the other Torness reactor showed signs of increasing vibration and was promptly shut down by the operators. Its subsequent disassembly revealed a fully developed fatigue related crack in a similar position to the first failure, but the prompt shutdown had prevented consequential damage.

Following the initial failure, British Energy (BE) increased the attention given to circulator vibration monitoring. As a result of the second failure, more extensive routine monitoring of circulator characteristics is being undertaken and more extensive circulator monitoring equipment is being fitted to allow efficient, cross-fleet monitoring of circulator behaviour. Activities in this area are being brought up to best practice standards.

Inspectors from HSE’s Nuclear Installations Inspectorate (NII) monitored the recovery of the first failed circulator and its examination by BE specialists, and BE’s examination of the fixed structure for any signs of damage. Agreement to replace the failed generator was given by HSE when it was satisfied that there was no structural damage to the reactor. As the second failure did not result in the disintegration of the circulator impeller there was no damage to the reactor structure.

With the discovery of a systematic and comparatively frequent failure mechanism, safety concerns increased and NII required a revised and extended safety case to cover operations. This incorporated forewarning of failure by early and effective detection of changes in vibration patterns together with recognition of the need to shut down any affected circulators before major failure and consequential challenge to the circulator casing occurs.

BE has inspected all gas circulator impellers in service at Torness and found no evidence of developing defects. Only a limited number of impellers have been inspected at Heysham 2, but again no defects have been found. BE has provided acceptable interim safety cases justifying continued operation of the reactors at Torness and at its sister station Heysham 2.
Design related factor
The events were caused by the development of unexpected fatigue related cracks in gas circulator impellers.

INCIDENT 02/4/1

Harwell (United Kingdom Atomic Energy Authority)

Incident synopsis
On 6 November 2002 during operations in a glove box in B220, the over pressure alarm sounded. The operators evacuated and shortly afterwards the airborne activity monitors also sounded. The building emergency arrangements for airborne activity alarms was initiated to ascertain the source and to manage the operations. An investigation by UKAEA confirmed that a release of Americium 241 into the working area had occurred at a quantity in excess of Schedule 8 column 4 of the Ionising Radiations Regulations 1999 (IRRs). A number of personnel have received intakes including the two operators and the health physics personnel who attended the event. The highest dose (up to 6 mSv.) was received by the Health Physics charge hand.

UKAEA placed an embargo on the use of similar systems and have completed their own management investigation and produced an internal report. It concluded that the likely cause of the event was over-pressurisation of the vacuum equipment used in the process. The report also highlights improvements required to the ventilation system in the laboratory and adjoining areas. An action plan has been developed for this work and progress is being made.

NII has followed the UKAEA investigation and carried out its own study including a visit by a ventilation specialist. This has confirmed the problems with the ventilation system. It is a complex issue that may have a wider impact across the building. A letter has been sent to UKAEA detailing a series of short-term requirements and the need to review implications and produce a longer-term action plan. UKAEA is cooperating fully with these requirements.

Design related factor
The likely cause of the event was over-pressurisation of a ventilation system. Improvements to the ventilation system in the laboratory and adjacent areas are required.

INCIDENT 02/4/2

Dounreay (United Kingdom Atomic Energy Authority)

Incident synopsis
On 12 November 2002, two contractors leaving the D2001 Intermediate Level Waste Processing facility were found to have contaminated shoes and one had contamination on his hands. All personnel in the building were withdrawn and monitored, and as a result contamination was revealed on the shoes of a further fifteen individuals. Of these, one other person had contamination on his hands and face. The two individuals with personal contamination were sent to the Occupational Health Department where decontamination was successfully carried out the following day.

In parallel with UKAEA’s investigation, an investigation into the incident was carried out by NII commencing at site on 13 November 2002. The investigation concluded that the source of the contamination was the leakage of a small quantity of contaminated Zinc Bromide liquid from a flask. This had been swabbed up from the inside of a shielded waste cell and placed in a waste container which was then posted out of the cell into the flask for processing and
consignment for storage. The flask, waste container and the associated bagging system is not designed to provide containment of free liquids and the Zinc Bromide leaked to the outside of the flask and was spread around the working area on the shoes of the workers.

The actual doses received by the individuals affected by the incident were confirmed to be very low. In addition, checks of the discharge stack monitors concluded that there was no evidence of a release to the environment.

NII’s investigation report revealed a number of shortcomings which are being addressed by UKAEA. An Improvement Notice was served under the Ionising Radiation Regulations 1999 (IRRs) requiring improvements to be made to the flasking system design and operations. The incident has been classified as Level 0 on the International Nuclear Event Scale.

Design related factor
The event was caused by a leaking flask. The flask, waste container and associated bagging system were not designed to provide containment of free liquids. Improvements to the flasking system design were required.
APPENDIX C : RAILWAY ACCIDENTS AND INCIDENTS

Ladbroke Grove Crash, Paddington (UK)
Accident Synopsis
A train crash occurred at Ladbroke Grove Junction on 5 October 1999 which caused considerable loss of life and injuries. A Turbo left Paddington Station at about 08:06 bound for Bedwyn in Wiltshire. At about 08:08:25 the Turbo passed signal SN109 on gantry 8 at red for Danger, travelling at 41 mph. It had passed the previous signal, SN87, at single yellow. The state of the points beyond SN109 was such that the Turbo was inevitably carried towards the Up Main line. Meanwhile a High Speed Train (HST) was approaching on the Up Main on green signals. Shortly before the crash a signaller at the Integrated Electronic Control Centre (IECC) at Slough, who had been monitoring the progress of trains, put signal SN120 back to red in face of the HST. Both train drivers applied their brakes, but this had no significant effect on the impact, which took place at a combined speed of about 130 mph. The crash caused a fire. Both drivers were among the dead.

The report of the Public Inquiry into the crash, led by Lord Cullen, noted that the positioning of signal SN109 was a contributory factor to the crash. It was positioned so that it could not be seen fully by the driver of the Turbo train as he approached it. After the red aspect of SN109 ceased to be obstructed, he could have seen it during a period of eight seconds as he approached that signal, but it appears that he either did not see it or did not realise that there was a red aspect. While it might well be expected that if he was concentrating on his duties he would look again at the signal, this depended on his various tasks and the confidence with which he had already identified what he thought that the signal was showing. The unusual configuration of SN109 – a “reverse L” – not only impaired initial sighting of its red aspect, but also might well have misled an inexperienced driver, such as the driver of the Turbo, who was looking at the signal at close range, into thinking that it was not showing a red but a proceed aspect.

Design-related Factors
Part 1 of the report of the Public Inquiry made 89 recommendations, some of which relate to design issues. These include:

- Recommendations to improve the sighting of signals, including involving human factors experts in the revision of the standard for sighting of signals.
- Recommendations to improved cab design to enhance driver survivability.
- Recommendations to improve the crashworthiness of passenger coaches, including the design requirements for more realistic scenarios.
- Recommendations to improve the design so as to reduce the likelihood and consequences of fire after a crash.
- Recommendations to improve the design so as to improve the ability to evacuate a train after a crash.

Hatfield Derailment (UK)
Accident Synopsis
On 17 October 2000 four people were killed and 70 injured as a result of a derailment near Hatfield. The immediate cause of the derailment was fracture and subsequent fragmentation of a rail. The Hatfield derailment happened because a rail, in which there were multiple...
cracks and fractures due to rolling contact fatigue (RCF), fragmented when a high speed train passed over it. The train was travelling at the permitted speed.

**Design-related Factors**
The investigation, undertaken jointly by HSE and the British Transport Police (BTP) with the latter in the lead, made 16 recommendations. Two of the recommendations relates directly to design:
- Train sets should be designed, built and maintained to maximise the chance of their remaining upright and intact during high speed derailment. (Particular aspects for review are given.)
- The design of overhead line equipment stanchions should be reviewed with a view to making them less likely to penetrate passenger space in the event of a collision.

**Southall East Derailment (UK)**
**Accident Synopsis**
At around 20.05 on Sunday, 24 November 2002 the leading bogie of the fifth coach of the Swansea to Paddington express derailed at a set of points east of Southall station. It was travelling at approximately 120mph. The train remained upright and in line, and finally came to a halt just before West Ealing station, some two miles further on. There were no serious injuries, but because of the catastrophic potential of this incident the Health and Safety Executive (HSE) launched an immediate investigation. Key interim findings are:
- The bogie was derailed when the flange of a wheel struck one half of a broken fishplate which had lodged in the nose of a cast manganese steel crossover forming part of the points; The fishplate had been securing the running rail to the crossover. It broke under fatigue stresses and became detached as a result of the bolts securing it coming undone.
- It has also been established that the fishplates were changed in July 2002 after a previous instance when one was found to be cracked. Forensic examination suggests that gross ripping fatigue, in which a crack might advance rapidly (tearing or ripping) due to the variable loads applied, was involved in the failure of these fishplates. This might not have been visible until a short time before failure.

**Design-related Factors**
Fatigue failure of the fishplate after only 4 months in service, and after a previous one had been found to be cracked, suggests that the design may not be appropriate for the conditions to which it is exposed.

**Eschede Accident (Germany)**
**Accident Synopsis**
On Wednesday 3 June 1998, a fast passenger train was derailed near Eschede killing over 100 people. Following an unusual noise and vibration, five passenger coaches were successively derailed. The fourth of the coaches hit a bridge over the railway, causing the bridge to collapse. The bridge collapsed onto the fifth passenger coach. The train was travelling at high speed, within the operating envelope of both the train and the track. No other train was involved.

Investigations into the crash established that the root cause was failure of a wheel on the leading passenger coach. The wheels were of a special, composite design with a rubber insert that had been introduced to reduce vibration. A crack occurred caused by excessive load and wear. There was no indication of material or production failure. When ICE began operations, there was no certification in place that would document appropriate design and reliability. Moreover no fracture mechanic calculation was done that could prove the strength
of the wheel during its lifetime. According to experts such wheels should not have been
operated at less than 880 mm diameter, subject to annual testing for inner and middle zone
cracks. The diameter of the accident wheel was 862 mm.

A contributing factor to the severity of the crash was the design of the track. The track layout
consisted of a pair of fast tracks and a pair of slow tracks. Points were included at intervals to
enable trains to transfer from the fast track to the slow track and vice versa. Following
derailment of the first three coaches, one of the points for transferring a train from the fast
track to the slow track (‘facing points’) may have caused a wheel of the fourth passenger
coach to leave the fast track, leading to derailment of the coach. Such points have been
recognised as a potential hazard since the 19th century.

It has also been suggested that passenger survivability was compromised by the passenger
coaches not following the traditional practice of designing the passenger compartment as a
single, steel compartment but instead designing the upper section as an aluminium section
welded to the base (this was a weight-saving feature).

Design-related Factors
The design of the wheel had not been confirmed for this specific application, either by
analysis or by in-service testing. The wheel was being used outside the range considered
acceptable by experts.
The track layout included features (‘facing points’) that can present a hazard, particularly to
fast trains, in certain abnormal situations.
The non-traditional design of the passenger coaches may have reduced passenger
survivability.

Train Protection and Warning System (UK)
Synopsis
The Train Protection and Warning System (TPWS) is a safety system that is being
introduced in the UK. It detects when a train is approaching a signal at danger and is likely to
pass it, warns the driver then, if necessary, applies the brakes on the train. The warning
enables the driver to take action (e.g. additional braking) to avoid passing the signal or
minimise the over-run. The application of brakes by TPWS is intended to stop the train within
a safe distance beyond the signal. TPWS is being introduced in order to reduce the risk from
SPADs, which have caused a number of recent major accidents.

Although not yet fully implemented, TPWS is currently (2002/3) involved in about 50% of
SPADS and is a significant factor in reducing the risk from SPADs. However, due to design
and operational issues there has been a high incidence of incorrect TPWS interventions (i.e.
TPWS warning when not needed). This has lead to driver mistrust, with drivers believing that
TPWS intervention is either incorrect or inappropriate. In 15% of correct TPWS interventions
in 2002/3, the driver reset TPWS and continued without contacting the signaller. This is
clearly hazardous. The fact that TPWS is designed to reset itself after an interval without the
driver taking any action may add to this problem.

Design-related factors
The effectiveness of a safety system has been compromised by a high incidence of incorrect
interventions due, in part, to design. High incidence of incorrect interventions has resulted in
mistrust of the system so that correct intervention is over-ridden.