Broad Lane, Sheffield, S3 7HQ
Telephone: +44 (0)114 289 2000
Facsimile: +44 (0)114 289 2500

HEALTH & SAFETY LABORATORY

MACHINERY RISK ASSESSMENT VALIDATION LITERATURE REVIEW

HSL/2000/18

Project Leader: Nicola Worsell

Nicola Worsell, BSc, Msc (Eng)
Agamemnon Ioannides, BSc, Msc (Eng)

Human Factors Group

HEALTH AND SAFETY LABORATORY
An agency of the Health and Safety Executive

Summary

Objectives

The Health and Safety Laboratory, with funding from, and in association with, the Health and Safety Executive have developed a machinery risk assessment (MRA) methodology for designing machinery under the project R36.057 [Worsell *et al* 2000]. However only limited validation was carried out so the current project R71.037 was set up in order to enable further validation. An important aspect of this project has been keeping up to date with relevant developments.

The purpose of this report is twofold. Firstly to update members of the project team on literature and developments pertinent to the machinery risk assessment validation project. Secondly to serve as a reference document or aide memoir for the team. However the major part of the report is in the form of a literature review and is therefore expected be found useful by a wider audience.

Main Findings

There is now considerable activity and interest in the use of risk assessment in the machinery sector where it has not been traditionally used in the past. This was not the case when the machinery risk assessment methodology was first developed. The pace of developments in this area is such that it is quite difficult to keep up to date. An aide memoir such as this is therefore essential. Many of the references included have been published in the last 2-3 years.

There is still evidence that there is a need for comprehensive practical guidance for the application of risk assessment to machinery by designers. The design of machinery has also been shown to have important implications for safety in a recent HSE review [Eaton 1999].

Main Recommendations

This literature review should be used as an up to date source of information for the continuation of the validation project and other related support activities. Various other techniques identified as having the potential to be usefully incorporated into the machinery risk assessment toolkit should be looked at in further detail by the project team.

It is therefore important for HSE to remain active in providing input to standards making (European and International) in this area.

Contents

1. INTRODUCTION 1

2. RELATED DEVELOPMENTS 1

3. HAZARD IDENTIFICATION AND RISK ASSESSMENT 4
   - 3.1. HSE/HSC Guidance on Risk Assessment 4
   - 3.2. AS/NZS 4360:1999 Risk Management 6
   - 3.3. SRD's Review of Hazard Identification Techniques 6
   - 3.4. Engineering Council's Guidelines on Risk Issues 7
   - 3.5. Loss Prevention in the Process Industry 7
   - 3.6. Geoff Wells' Hazard Identification and Risk Assessment 8
   - 3.7. Fischoff's Acceptable Risk 8
   - 3.8. Ball and Floyd on Societal Risk 9
   - 3.9. Swiss Report - Risqué 9
   - 3.10. Risk Assessment: The Human Dimension 11
   - 3.11. ISO/IEC Guide 51 11
   - 3.12. IGE's Risk Assessment Techniques 11
   - 3.13. Elvik on Cost-Benefit analysis (CBA) 12

4. MACHINERY STANDARDS 13

5. MACHINERY DESIGN / RISK ASSESSMENT GUIDANCE 13
   - 5.1. BSI Guide to CE Marking for Machinery 13
   - 5.2. Practical Guide to the Machinery Directive 14
   - 5.3. Safeguarding Agricultural Machinery 15
   - 5.4. Machinery Safety: The Risk Based Approach 15
   - 5.5. Australian Guidance 16
   - 5.6. ICI Eutech Paper on Machinery Design 16
   - 5.7. Probability Risk Assessment of Engineering Systems 17

6. CONTROL SYSTEM DESIGN STANDARDS 17
   - 6.1. BS EN 954:1997 Safety Related Parts of Control Systems, ... 17
   - 6.2. IEC 61508 Functional Safety of E/E/PE Safety-Related Systems 18
   - 6.3. DIN V 19 250 20
   - 6.4. DEF STAN 00-56 Safety Management Requirements 20

7. CONTROL SYSTEM DESIGN GUIDANCE 21
   - 7.1. The PES Guide 21
   - 7.2. EEMUA's Safety Related Instrument Systems for the Process Industries 22
   - 7.3. Out of Control 22
   - 7.4. CCPS - Guidelines for Safe Automation of Chemical Processes 22
   - 7.5. Guidance on HAZOP Procedures for Computer-Controlled Plants 23

7.6. MISRA Reports 23
7.7. Safety Aspects of Advanced Transport Telematic Systems 25
7.8. Towards safer industrial computer controlled systems 27
7.9. Design for Safety 27
7.10. Cooper on Fail-Safety 28

8. CONCLUSIONS 28

9. REFERENCES 28

10. ACKNOWLEDGEMENTS 35

1. INTRODUCTION

The Health and Safety Laboratory, with funding from, and in association with, the Health and Safety Executive have developed a machinery risk assessment (MRA) methodology for designing machinery under the project R36.057 [Worsell *et al* 2000]. However only limited validation was carried out so the current project R71.037 was set up in order to enable further validation.

An important aspect of this project is keeping up to date with developments in the field both within and outside HSE. This was recognised when the project was set up and therefore budgeted for from the outset. A significant proportion of the project leader's time has therefore been devoted to tracking down pertinent literature, reading it and keeping in touch with contacts working in relevant areas. The purpose of this report is twofold. Firstly to update members of the project team on literature and developments pertinent to the machinery risk assessment validation project. Secondly to serve as a reference document or aide memoir. The major part of the report is in the form of a literature review and is therefore expected be found useful by a wider audience.

2. RELATED DEVELOPMENTS

This section describes developments, not directly as a result of, but germane to, this validation project. This includes other research and support projects carried out by HSE, for HSE or independently of HSE. A quick review is also made of developments in Europe regarding the Machinery Directive (originally 89/392/EEC now consolidated with all amending directives as 98/37/EEC) and associated standard EN 292.

One justifiable criticism of the machinery risk assessment (MRA) methodology as it stands was that it had not been tested on any equipment containing complex control systems. However in light of ongoing work in collaboration with Joy Mining Machinery this will no longer be the case. Furthermore, an ongoing project R38.022 for TD1, relates to the impact of control systems on fairground safety. In particular the use of risk assessment to specify the integrity requirements of the various safety functions of fairground control systems. This project has provided useful input into the validation project. Another novel hazard identification technique aimed specifically at identifying safety functions of control systems has been developed. This may be usefully included into our toolkit [Worsell & Chambers 2000]. A number of control related references were also identified during this project and have been included in this review.

Another European project, SAFEC, for TD1 is looking at the categorisation of protective measures and safety-related systems for use in potentially explosive atmospheres. This is concerned primarily with setting safety integrity level (SIL) targets rather than with risk assessment per se [Wilday *et al* 2000].

Another justifiable criticism of the MRA methodology is that it does not allow for the easy incorporation of health effects. This is not surprising, as the original remit of the project was to only consider hazards from moving parts. The reactive support project S4000417 for TD3, recently completed [Balmforth 2000], may therefore provide valuable input to the validation project. The objective of this project was: to assess chemical emissions hazards of various

machines; comment on the adequacy of the Essential Health and Safety Requirements (EHSRs) of the Machinery Directive (98/37/EEC) and associated standards for this purpose; and make recommendations for improvements. A wide range of chemical emission hazards were observed; solid particles, toxic fumes (including vaporised metals, rubber and plastics), solvent vapours, mists or aerosols of toxic materials such as metal working fluids and oils. These are associated with a wide range of occupational health effects, acute and chronic, from dermatitis and respiratory complaints to cancer. It was found that the hazard identification stage of our methodology can be used effectively. However, as would be expected, the risk estimation and evaluation stages cannot be used as they stand. This is due to the fact that the underlying fault-tree relies on the risk being dependent on an initiating hazardous event, whereas health problems are generally caused by cumulative long term exposure.

The EU project STandards for SAfety Related Complex Electronic Systems (STSARCES) [Wray 1999] was set up with the overall aim of speeding up the drafting of part two of the standard EN 954. As part of work package 4 of this project standards EN 954-1 and IEC 61508 [IEC 1998] were retrospectively applied to a hydraulic press in order to establish the links and divergencies between their requirements. For the purpose of the analysis only three hazards were considered. However, the report on this work provides valuable background information and analysis of the likelihood of these hazards being realised. Examples are given of the practical application of both of these standards. The HSE project officer for STSARCES is Steve Frost in TD1.

Other developments include comments received from various people within HSE. A Machinery Safety Steering Group (MSSG) meeting was held on 2nd November 1998 to discuss these at which more verbal comments were received. Notes have been made of the issues raised under the headings, concerns, modifications, clarification etc.. These will be discussed in a later report and taken on board as far as possible when the methodology is refined.

A brief review of fatal accidents involving machinery was carried out by HSE operations unit. This covered a six year period from April 1993 to March 1999. The results of this review [Eaton 1999] were presented to the Machinery Safety Steering Group (MSSG). Of 122 fatal accidents during these six years, 106 contained sufficient information to be analysed in terms of: the type of machine involved; the industrial environment; the activity at the time of the accident; and design implications. There are several pertinent findings. Perhaps not surprisingly agricultural machinery and the agricultural environment were involved in significantly more of the fatal accidents than any other sector. Some form of maintenance activity in the broader sense (cleaning, repair, clearing of blockages etc.) was being carried out, either by maintenance staff or operators when 50% of the accidents occurred. Of more significance to us was that design appeared to have been a contributory factor in 32% of the accidents. The overall conclusion was that improved machinery design for safety including safety during maintenance could dramatically reduce the number of fatal accidents.

Research [Hibbert 1999] has revealed numerous cases of manufacturers failing to properly comply with the Machinery Directive (98/37/EEC) and associated standards. The performance of 69 predominantly European Machinery manufacturers were analysed. Problems identified were quite fundamental. For example 13% issued no Declaration of Conformity or Declaration of Incorporation. Of those that did, 3 were not translated into the language of the country where the machinery was intended to operate, and almost a third did not comply with the

recommended format. Only 2 out of 69 companies correctly referenced all relevant directives and EN standards; only 2 referenced EN1050. It would seem, therefore, that as noted by operational FOD inspectors, there is a lot of CE marked machinery being supplied within Europe which does not comply with the Machinery Directive. Often these new machinery deficiencies go unnoticed until there is an incident.

The IEC[1] 62061 standard "Functional Safety of Machinery Control Systems" (machinery sector version of IEC 61508) is in preparation by IEC Technical Committee 44. An informative annex to provide guidance on risk assessment will form part of this standard. Steve Frost of TD1 is a member of working group 7 which has been given the task of writing this guidance. Mark Charlwood of Innovation Electronics (UK) Ltd. is taking a lead on this and is using the machinery risk assessment final report as a basis [Worsell & Wilday 1997b]. The validation project team are collaborating in this work.

Finally, there is a proposal to amend the Machinery Directive (98/37/EEC). The primary purpose being to simplify and clarify the directive. This initially included the restructuring of the order of the Essential Health and Safety Requirements (EHSRs). However, this was not welcomed by any of the member states due to the practical problems that reordering EHSRs will have for manufacturers when switching from one numbering system to another. It also includes a suggestion that the conformity assessment procedures should be brought more into line with the modular structure used in other recently adopted Directives. However, this is still under negotiation. HSE are concerned about the cost implications of, and lack of evidence of potential benefits from, changes to the conformity assessment procedures. The proposal also includes more prescriptive requirements on how member states are expected to enforce the directive. This introduces the term "Market Surveillance" which is not clearly defined. At the moment it seems unlikely that the content of the EHSRs themselves will change.

The revision of the standard EN 292 as both a European and International Standard (ISO 12100) continues and a draft for public comment was issued in April 2000. The revision took place purely because EN 292 was nine years old, and a number of supporting standards have now been completed which affect the content of EN 292 - for example EN 1050. The main change is that Part 1 of the standard has been shortened. The figures showing the scope of the standard and the process of producing a safe machine have also been modified. In addition considerable effort has been put into updating the description of the process of risk assessment and various associated definitions.

[1] International Electrotechnical Commission

3. HAZARD IDENTIFICATION AND RISK ASSESSMENT

3.1. HSE/HSC Guidance on Risk Assessment

There are various HSE documents some internal, others published, which explain HSE's approach to controlling risk [HSE 1995]. Probably the most well known and frequently mentioned is "The Tolerability of Risk from Nuclear Power Stations" often simply referred to as "TOR" [HSE 1992], first published in 1988. It explains HSE's approach to risk assessment, the ALARP principle, the importance of taking into account public perception and explains the uncertainties in risk assessment. As one would expect from the title it is specifically aimed at the Nuclear Industry. However, as it was the first document published in this area that gives some numerical criteria, it has been used as a basis for risk assessment, particularly quantitative, in many other industries. One paragraph (No 10) worth reproducing here describes the meaning of 'tolerability' as follows:

> "Tolerability does not mean acceptability. It refers to the willingness to live with a risk to secure certain benefits and in the confidence that it is being properly controlled. To tolerate a risk means that we do not regard it as negligible or something we might ignore, but rather as something we need to keep under review and reduce still further if and as we can."

Another HSE document, "Quantified Risk Assessment: Its input to decision making", [HSE 1993] develops some of the issues raised in the original TOR document. The use of full quantified risk assessment (QRA) is unlikely to be appropriate, or possible, in most cases (and would in any case be very difficult) when considering risks associated with machinery. However, this document does contain some relevant material. For example, an interesting discussion about societal risk, explaining the factors that seem important in judging the tolerability of societal risk and the essential differences between this and individual risk. It also gives some tentative criteria against which to evaluate societal risk.

In a similar vein "Risk criteria for land-use planning in the vicinity of major hazards" [HSE 1989] discusses individual and societal risk criteria together with quantified risk assessment methods. It gives various examples of consequence modelling of LPG and toxic releases through the use of RISKAT (HSE's computerised risk assessment tool [Hurst, Nussey & Pape 1989]). It gives a general overview of how TOR can be applied to land-use planning in the vicinity of major hazards, giving criteria for both individual and societal risk.

Internal to HSE is the Risk Assessment Policy Unit's document "Principles and guidelines to assist HSE in its judgements that risk has been reduced 'as low as is reasonably practicable (ALARP)" [RAPU 1995] and following on from this the external consultation document "Reducing risks, protecting people, the control of risks from industrial activities" [HSE 1999]. This has been produced as a result of HSE's recognition that many of the principles in TOR can be applied to other industries. It is a useful reference, which covers all the necessary issues in risk assessment, such as societal risk and its representation through FN-curves etc.. It equates tolerable risk with the phrase "safe enough" and accepts that good practice does not always provide a sufficient guide to the tolerability of the risks. In addition, good practice is described as representing, "in effect, the consensus ..... as to what constitutes proportionate action to control a given hazard taking account of what is technical feasible, the balance of

cost and benefits and, if necessary other relevant factors." In addition various estimated values are given for the risk of death or serious injury from various activities, both industrial and leisure, to inform the balancing act between risks and benefits.

The machinery risk assessment project team have not, in any way, been involved in the development of this discussion document, often referred to simply as R2P2, however have found it to be a useful document. It contains the only written criteria and guidance that are applicable to machinery (rather than specific to the nuclear or major hazards industries). These criteria are a fatal accident rate of:

- 1 in a million per annum below which the risk is broadly acceptable.
- 1 in a thousand per annum above which the risk is intolerable, or 1 in 10 thousand per annum for members of the public.

The Advisory Committee on Dangerous Substances report on "Major Hazard aspects of the transport of dangerous substances" [ACDS 1991] gives a comprehensive description and discussion of a complex and resource demanding QRA developed to assess the risks from:

- road and rail transport of toxic and flammable substances;
- road and rail transport of explosive articles and substances;
- ports handling non-explosive substances in bulk.

The methodology is illustrated by a number of detailed case studies. The report openly acknowledges many of the limitations of QRA, particularly the issue of uncertainty, but judges that the use of QRA has provided the best estimates of the risk involved, and given the committee valuable insights in reaching its conclusions. One interesting point is that the report concentrates almost exclusively on the estimation of risk and gives no description on how the scenarios leading up to the hazardous events were identified. Although not directly applicable to our problem, this report is useful in so far as it gives criteria for both individual and societal risk along with an explanation of how these were reached.

An earlier report by the Advisory Committee on Major Hazards [ACMH 1984] listed four principles about risk to be applied to major hazards which reflected HSE's view at the time. These have been reworded below to be more generally applicable.

- Risk should not be significant when compared with other risks to which a person is exposed in everyday life.
- Risk should wherever reasonably practicable be reduced.
- Additional development should not add significantly to existing risk.
- If the possible harm is high, the risk that the incident might actually occur should be made very low indeed. This takes into account society's particular abhorrence of accidents which cause many simultaneous casualties. Note that in light of the Lyme Bay tragedy this should now be extended to include "injuries to children".

There is also "Five Steps to Risk Assessment" [HSE 1998b] a document aimed at firms in the commercial, service and light industrial sectors. It describes risk assessment as being

"nothing more than a careful examination of what, in your work, could cause harm to people, so that you can weigh up whether you have taken enough precautions or should do more to prevent harm." It also explains that the important things that need to be decided are "whether a hazard is significant, and whether it has been covered by satisfactory precautions so that the risk is small." Although obviously aimed at assessing workplace hazards rather than reducing risk during machinery design some of the key phrases may be useful when describing the quick route through our methodology (for example "obvious hazard" and "solution"). Another is "consider whether you have done all the things that the law requires and whether generally accepted industry standards are in place." Also "can the hazard be eliminated and how can risks be controlled so that harm is unlikely?" The following hierarchy of principles to apply in controlling risks is also given:

- Try a less risky option
- Prevent access to the hazard (e.g. guarding)
- Organise work to reduce exposure to the hazard
- Issue PPE
- Provide welfare facilities (removal of contamination, first aid etc.)

Another report [NERA 1998] prepared for the HSE, "Developing a Common UK Approach to Negotiations on Risk Assessment at International Level" builds on the work of the Intergovernmental Liaison Group on Risk Assessment (ILGRA). This is quite a difficult document to read. However, it is interesting in so far as it explains the problems surrounding the use of the ALARP principle in European Directives and standards.

3.2. AS/NZS 4360:1999 Risk Management

Although this Australian / New Zealand Standard [AS/NZS 1999] uses slightly different terminology to that generally used in the UK and Europe it is nonetheless very useful. It is thorough, yet concise and easy to read. It contains a comprehensive list of definitions and describes the complete risk assessment process as part of a risk management program. This includes the general principles of: different types of risk analysis, qualitative, semi-quantitative and quantitative; sensitivity analysis; risk evaluation and the need to set criteria; and risk reduction option analysis (referred to as risk treatment).

3.3. SRD's Review of Hazard Identification Techniques

This report [Parry 1986] by the Safety and Reliability Directorate (SRD) first describes the underlying principles and philosophy of hazard identification techniques, their use and limitations. It then moves on to review various techniques that were available at the time for identifying hazards associated with the processing, storage and handling of dangerous substances. These were HAZOP, Checklists, FMEA, Fault Tree Analysis (FTA), Event Tree Analysis and Cause-Consequence Analysis. Each technique is illustrated by an example of their use. All techniques could be applied to machinery, including HAZOP with similar guide words but different parameters.

3.4. Engineering Council's Guidelines on Risk Issues

The objective of this publication [Engineering Council 1993] is to provide practical and ethical guidance on risk issues. The guidelines are neither a technical code of practice nor a manual for risk management, i.e. they do not explain how to 'do' risk assessment. However, the guidelines do explain the legal requirements for risk assessment and the professional responsibilities of engineers. They then go on to discuss some important issues that need to be borne in mind when conducting risk assessment.

They recognise that it is very difficult to judge levels of risk, and that there is no common framework for evaluating risks or any universally recognised level of risk that is considered to be acceptable. This can and often does lead to conflicts between interested parties and a few pointers are given on how to deal with these conflicts, such as the importance of being objective, making the risk assessment as factual and transparent as possible and clearly explaining any assumptions. One interesting quote is "no matter how good the analysis, there will be no effect on risk until the recommendations are implemented."

The guidelines also recognise the important role that software plays in control systems and states that "the use of computers or Programmable Logic Controllers (PLCs) in systems which have a direct impact on safety obviously requires special care". However no detail is given as to how to do this, instead the reader is referred to HSE publications for further information. Nevertheless the publication is good background reading for its intended audience. A useful list of the causes of human error is given in appendix 2.

Institution of Electrical Engineer's "Professional Brief on Safety-related Systems" [IEE 1992] builds upon these guidelines and includes the concept of the safety-lifecycle from IEC 61508 [IEC 1998] (see 6.2), but not that of safety integrity levels. The brief is intended to provide professional engineers involved in the specification, development, assessment, maintenance or operation of safety-related systems with a concise overview of those matters with which they should be concerned. The bulk of the material is related to legal and professional responsibilities and there is very little guidance for the designer.

3.5. Loss Prevention in the Process Industry

Frank P. Lees' "Loss Prevention in the Process Industry" [Lees 1996] is regarded as an essential reference for process safety engineering. It addresses all aspects of hazard identification, risk assessment and control with comprehensive case studies, reviews and various applications throughout the chemical industry. The second edition comes in three volumes. The first is relevant to this project as it contains a comprehensive description of all the Hazard Identification techniques used in the chemical industry, illustrated by examples, relevant legislation, risk assessment analysis, risk and safety management systems, process design, human factors, human reliability analysis and control system design.

Volume 2 looks in some detail at consequence analysis (i.e. fire, explosion, toxic releases etc.), emergency planning, safety systems, etc..

Volume 3: gives a description of various case studies and incidents world wide.

Some 72 pages of volume one are devoted to control system design. Much of the information is taken from three references discussed in section 7 of this literature review. These are the "PES Guide" [HSE 1987], "Safety Related Instrument Systems for the Process Industries" [EEMUA 1989] and "Safe Automation of Chemical Processes" [CCPS 1993]. The requirements of each reference are described in some detail, including various tables. This is accompanied with some explanation of how the requirements, particularly of the "PES Guide" can be achieved in practice.

The section on risk criteria draws its material from the HSE publications discussed above and the book "Acceptable Risk" [Fischoff *et al* 1981] discussed below. There is quite a lot of material on reliability but nothing of particular interest to machinery risk assessment.

3.6. Geoff Wells' Hazard Identification and Risk Assessment

This book [Wells 1996] gives a thorough explanation of hazard identification and some risk estimation techniques used in the process industries. These techniques form a solid basis on which to develop techniques for other industries, such as we have done in the previous project. There is a chapter on risk criteria which gives a clear explanation of the meaning of individual and societal risk and in addition the complexities which arise when trying to give absolute criteria for tolerable risk. There is also a risk compendium for risk comparison purposes and some targets are given for maximum risk values not to be exceeded. These values indicate a maximum tolerable risk level of 10^{-5} to 10^{-6} for members of the public (which is in the lower half of the ALARP region in TOR[2]) and one order of magnitude greater for workers. The book is illustrated throughout by case studies and generalised failure rates are given for various processes and sub-systems, including human reliability, which can be used in any QRA.

3.7. Fischoff's Acceptable Risk

The most well known reference which deals almost exclusively with the subject of risk criteria is "Acceptable Risk" [Fischoff *et al* 1981]. It poses the question "How safe is safe enough?" and gives a critical analysis of three approaches to making acceptable-risk decisions. These are:

1. Formal analysis, which decomposes complex problems and tries to analyse them from a technical perspective.
2. Professional judgement, which relies upon the wisdom of the best available experts.
3. Bootstrapping, which uses history as a guide and compares the risk to be evaluated with existing risks which society is willing to accept (or as is now more commonly expressed, tolerate).

These are evaluated relative to one another and by contrast with the absolute standard of what one would want from an ideal method described in terms of the following seven criteria which are explained in some detail in the book: Comprehensive, Logically Sound, Practical, Open to evaluation, Politically acceptable, Compatible with institutions, Conducive to learning. Within this framework, recommendations aimed at improving society's ability to make

---

[2] HSE's Tolerability of Risk from Nuclear Power Stations [1992]

acceptable-risk based decisions are offered in the areas of policy, practice and research. A very generic overview is given on the risk based approach through cost-effective analysis, decision-making and other ways of accepting risk decisions. Emphasis is also given to the uncertainty of human judgement and the authors try to analyse the process. No reference is given to specific hazard identification techniques or any QRA methodologies. Fischoff also recognises that there are often a range of potential consequences.

3.8. Ball and Floyd on Societal Risk

This report [Ball & Floyd 1998] reviews the developments in and the debate surrounding societal risk in chronological order against a backdrop of disasters and other events such as major risk studies, issue of key policy documents and public inquiries. It is aimed at risk associated with on and offshore hazardous installations, nuclear power stations and the transport of dangerous goods. It discusses many of the HSE publications described in this review, explains the use of F-N curves for expressing societal risk results and criteria including the difference between risk-neutral and risk-averse criteria and the underlying mathematics. It also discusses a few alternative methods for expressing societal risk including the underlying mathematics and use of the risk integral developed in HSE/CHID 7, (as was). A more detailed reference for the risk integral is [Macbeth 1998] which includes various examples of its use.

3.9. Swiss Report - Risqué

This report was written as the result of a project entitled "Assessment and acceptance of technical risks" set up by the Swiss Academy of Technical Sciences. The report is available in French, German and Italian. The comprehensive summary and conclusions have been translated into English [Schneider *et al* 1995].

The purpose of the project was to establish a dialogue between engineers and sociologists on risk issues - the greater aim being to put the handling of risk within Switzerland on a more uniform basis. Much of the main body of the report appears to be transcripts of various discussions between experts in the two fields. The summary and conclusions however seem to cover all the important points raised and contain some interesting and potentially helpful ideas. Before reading the translation however it is worth bearing in mind that the same word is used in French for both risk and hazard; the report therefore talks about risk identification and occasionally you should read hazard in place of risk. The report stresses the importance of clearly separating the process of risk analysis from the process of risk assessment. We would normally call risk analysis - risk estimation and risk assessment - risk evaluation. The first interesting concept is the categorisation of risks into:

1/ Traditional risks - those with which the general population come into contact on a daily basis and are therefore familiar. Those responsible for managing these sorts of risks have a considerable knowledge about the most effective control measures and statistics to measure existing risk, trends and evaluate alternative control measures. Risk Assessment continues to be carried out on an empirical basis. Road transport and accidents in the home would fit into this category.
2/ Technical or problematical risks - those connected with known and accepted technologies but which present difficulties of assessment because of the increasing scale and

complexity of the installations involved. Fairgrounds and complex machinery would fit into this category.

3/ Politicised risks - those which have global implications with the potential to cause widespread, catastrophic and irreversible damage or for which the cause and effect are not clearly understood. Nuclear power and genetic engineering would fall into this category.

Many of the reservations expressed by sociologists about risk estimation can only be appropriately applied to category 3.

The second important concept relates to the dispute between the objectivity of risk analysis (estimation) and the significance and subjective opinions of laymen. This dispute is seen to be a contentious issue which hampers discussions on risk and needs to be resolved if progress in the field of risk communication is to be made. This is where the importance of distinguishing between the processes of estimation and evaluation is highlighted. The process of risk estimation "can be considered to be objective in so far as it is directed towards the world of physical phenomena and is independent of the observer. Hence they should be reproducible, logical in the mathematical sense and not guided by personal motives." This is relatively straightforward for category 1 - traditional risks, just about possible for category 2 - technological risks but just about impossible for category 3 - politicised risks. However, even in category 2 the result often depends upon the assumptions made, many of which are subjective to some degree. It is then accepted that the process of evaluating risks is very subjective, and political and that issues of risk perception, benefits etc. need to be taken into account. Discussions are further complicated by the fact that the lay person merges these two processes in order to form an opinion. It is interesting to note here the results of a survey which shows that the ambivalence of society towards technology has increased from 15% in the 60s and 70s to 70% today and that in general society appears more sensitive to risk.

The final concept of interest is that of how to structure the acceptance of risk question. This shows that there are in fact 3 levels:

1. Technology level in which it is necessary to answer the questions relating to the suitability, need and essential nature of the technology.

2. Site level in which it is necessary to establish who is at risk, how are the risks distributed, is there a fair distribution of benefits and risks etc..

3. Installation level in which questions about safety are dealt with in the very narrow sense of how the risk posed by a specific installation will be controlled and managed and what level of risk is tolerable.

Problems often arise because analysts often miss out the first two levels and enter into arguments about what is acceptable purely at the installation level. In particular when the lay person objects on purely ethical or moral grounds, i.e. are only considering the issues associated to level 1, and levels 2 and 3 are irrelevant to them. In a nutshell the opposing parties are not talking about the same thing.

3.10. Risk Assessment: The Human Dimension

This book [Hurst 1998] makes the case that any risk assessment must include human factors alongside hardware failures. This is on the basis that equipment and plant are designed by humans, built by humans, operated and managed by humans. These human factors would include safety management and safety culture as well as human reliability. The current international debate about risk perception and risk tolerability is also covered. A case study involving HSE's use of risk assessment as an input to land-use planning advice is used to illustrate many of the points made in the book.

3.11. ISO[3]/IEC Guide 51

This is the second edition [ISO/IEC 1999] of guidelines for the inclusion of safety aspects into standards. It was written by the technical advisory group on safety and is aimed primarily at those developing standards. However it gives some good risk assessment basics, including a straightforward set of definitions along with the recognition that "in other publications slightly different definitions may apply for the same terms, but the concepts are broadly the same." Another useful statement relates to tolerable risk. This is that "there is a need to continually review the tolerable level, in particular when developments, both in technology and knowledge, can lead to economically feasible improvements."

3.12. IGE's Risk Assessment Techniques

This document published by the Institute of Gas Engineers [IGE 1999] gives clear up to date guidance on the process of risk assessment based on HSE's five steps [HSE 1998b]. It then goes on to describe techniques for the steps of hazard identification, consequence analysis, risk estimation and evaluation. Various advice about the risk assessment process is given. Whilst it is important to identify all relevant hazards a recommendation is given against cataloguing every trivial hazard. This may seem a sensible piece of advice but without analysing consequences and likelihoods - i.e. estimating the risk - it is not always obvious whether the hazard is trivial or not and therefore care has to be exercised when eliminating something as trivial. There is also the good advice that risk assessment should be undertaken by or with assistance from personnel who have practical knowledge and experience of the work activity and expert advice should only be called in when the system or situation is particularly complex.

Risk Criteria are also discussed in terms of societal, individual, voluntary and involuntary risk. This is based on the TOR framework [HSE 1992]. The concept that a higher risk can be tolerated in the case of voluntary risk, i.e. when someone voluntarily exposes themselves to a risk in order to obtain some benefit, is discussed.

---

[3] The International Organization for Standardization

A comprehensive glossary is also provided which in general gives clear, well thought out definitions. However the definition of risk does not fit with the simple approach techniques described under the section on risk evaluation. These combine one of three possible levels of consequence with a likelihood in order to obtain risk. Whereas the definition states that risk is the likelihood of a specified undesired event occurring within a specified period or in specified circumstances.

3.13. Elvik on Cost-Benefit analysis (CBA)

This recent paper [Elvik 1999] gives a good overview of the problems associated with the use of cost-benefit analysis. A five stage framework is described which allows the implications of various criticisms of CBA to be discussed so as to enable a decision to be made as to whether the use of cost-benefit analysis is appropriate or not. Some of the criticisms within this paper that are of particular interest were:

- no account is taken of whether risk is reduced to those individuals at highest risk or those already at low risk;
- objectives need to be stated such that values can be assigned to their goals;
- if any benefits or consequences (costs) cannot be valued then CBA cannot be used - obvious but often overlooked, this also applies if there is a high level of uncertainty about consequences;
- if the situation being considered is highly controversial it cannot be resolved by any amount of monetary calculations, this reinforces some of the messages of the SUVA report [Schneider *et al* 1995] discussed earlier.

Various references are given on CBA theory. There are also various values given in Kroner for levels of harm as shown below. Unfortunately the terms critical, serious and slight are not defined. If we assume that they are similar to ours it is interesting to see that there is little difference between critical and fatality but also less of a range than we use for the others.

Fatality		16, 600, 000	(33 x slight, 4.4 x serious, 1.2 x critical)
Injury	Critical	13, 370, 000	
	Serious	3, 780, 000	
	Slight	500, 000	

4. MACHINERY STANDARDS

Those machinery standards relevant to risk assessment are:

BS EN 1050:1997 Principles for Risk Assessment.
BS EN 292:1992 Basic Concepts, General Principles for Design,
parts 1 and 2 both currently under revision.
BS EN 954-1:1997 Safety Related Parts of Control Systems,
discussed in some detail later on in this document.
BS 5304:1988 British Standard Code of Practice for Safety of Machinery
now obsolete but still available, very well illustrated and currently being revised for issue as a published document (PD).

As the project team is very familiar with all these standards no further detail is given here.

5. MACHINERY DESIGN / RISK ASSESSMENT GUIDANCE

5.1. BSI Guide to CE Marking for Machinery

The August 1998 update [BSI 1998] is useful if only for the fact that is contains the complete consolidated text of the Machinery Directive (98/37/EEC). It also gives a list of approved bodies and the CEN programme in terms of a comprehensive list of current standards and provisional drafts of standards. Note that the most recent update is January 1999.

Section 7(ii) Conformity Assessment (page 19 Aug 98 edition, page 21 in Jan 99 edition) explains that "a manufacturer is under an obligation to identify the hazards which are inherent to a specific machine type" and that "the machine must then be designed and constructed taking account of a risk assessment." Also that "a conformity assessment exercise must be carried out against all the relevant EHSRs applicable to the machinery under review". An example of a checklist based on the list of hazards found in EN 1050 is then given. A simple tick indicates if the hazard is 'applicable'. The risk assessment then takes the form of selecting whether the risk is level 1, 2 or 3. The levels are defined as:

1 = High Risk (fatality/major limb loss etc.)
2 = Medium Risk (minor limb loss, severe cuts, major burns etc.)
3 = Low Risk (minor cuts, bruising, burns etc.).

As the reader can no doubt spot these are not actually levels of risk at all, but consequences, however, it is interesting to note that they quite closely follow the same categorisation of consequences as used in the machinery methodology [Worsell & Wilday 1997b]. The conformity assessment on page 20 is probably more useful especially when used in conjunction with the cross-references to parts 1 and 2 of EN 292 on subsequent pages. This may prove useful in updating the CSSR technique and providing help files for MCHA. The August 1999 edition gives further guidance on "Hazard and Risk Assessment basic approach" that appears to follow the guidance given in [HSE 1998b] "Five Steps to Risk Assessment". This edition also recognises that the 'risk levels' are in fact only consequence levels and that in some circumstances the frequency of exposure needs to also be taken into account. There is additional information about what these 'risk levels' mean in terms of what the manufacturer is expected to do about them.

1 (High Risk): is unacceptable and action to reduce these to the minimum would be considered to be 'mandatory'.
2 (Medium Risk): is undesirable and action to reduce these to a lower level is recommended.
3 (Low Risk): is tolerable or acceptable within limits (for example the frequency of exposure etc.).

Finally it is made clear that "manufacturers must provide warnings of residual risks, despite all the measures adopted, where such risks occur". This seems to imply that something must be done about the hazards which have severe consequences irrespective of their likelihood. This is not a bad idea but it is not clear whether the statement above means they must be eliminated such that consequences in fact are less severe or that their likelihood should be reduced as far as possible (practicable). The second statement is less confusing; it appears to recommend that the consequences are reduced to the lower level. Regarding risk level 3, frequency of exposure should be taken into account as suggested but only insofar as this translates into the frequency of occurrence of injury. Finally there is the age old problem of whether the most likely or worst scenario is considered. It is questionable whether this guidance fits in with HSE's ALARP principle and unfortunately potential for it to be misunderstood or misused.

A little more guidance about risk assessment is given in Appendix IV which includes extracts from various other standards and sample forms for recording risk assessment. These include space at the top of each form for the name of the person completing it - something that we have overlooked in our record sheets (but not the computerised version) and needs to be rectified.

5.2. Practical Guide to the Machinery Directive

This guide [van Ekelenburg *et al* 1997] is similar to the one described above and has been translated from Dutch by D. Brown of TecExec Ltd. However, it contains considerably more information about risk assessment. Unfortunately it is no longer being updated. It includes two diagrammatic techniques reviewed by the machinery risk assessment project team [Worsell & Wilday 1997a]. It also contains a comprehensive list of hazards presented in tabular format and includes columns for conditioning factors, possible effects, associated features and cross-referencing to Parts 1 and 2 of EN292, Annex 1, the Essential Health and Safety Requirements, of the Machinery Directive and Harmonised standards. There is also a cross-reference between the full text of Annex 1 of the Machinery Directive and EN292-2. There is also a comprehensive hazard specific checklist which should prove useful when building the help files for the MCHA software.

5.3. Safeguarding Agricultural Machinery

This guidance [HSE 1998a] explains:

- what the law requires;
- how machinery accidents happen;
- the basic principles of risk assessment;
- the mechanical hazards of agricultural machines;
- how guards and safety devices can be used to protect operators.

It deals only with mechanical hazards, e.g. physical hazards which may give rise to injury due to the mechanical action of machine parts or of projected solid or fluid materials. It gives good guidance on the issues surrounding foreseeable misuse and a comprehensive, illustrated list of potential hazards posed by agricultural machinery.

It explains that risk assessment is: identifying the hazards present, e.g. in a machine, and then evaluating the extent of the risks involved, with the object of selecting appropriate safety measures. Furthermore, that risk assessment carried out as part of the design process allows the hazards and risks associated with machinery designs to be evaluated before the machinery is built. It provides information to allow appropriate safety measures to be integrated into designs to reduce risks, so far as is reasonably practicable. It also explains that an assessment can provide information on the residual risks after safeguards have been included in the design, which is useful when deciding on the type of information which needs to be supplied with the machine. Information on designing safe machines is given in paragraphs 104-165. Appendix A provides a very basic example of a manufacturer's risk assessment of a flail hedge cutter.

The process of risk assessment in connection with the use of a machine is summarised as follows:

- identify the uses for which machinery is intended by virtue of its design;
- identify how the machinery is likely to be used and misused;
- identify hazards in connection with the use and operation of the machine;
- assess the level of injury or harm which can result from exposure to each hazard;
- assess what safety measures may be used and the protection that they can provide;
- minimise risks by selecting appropriate practicable safety measures which can be reasonably integrated into the design.

5.4. Machinery Safety: The Risk Based Approach

These practical guidelines [Raafat 1995] on risk assessment, standards and legislation are written by Hani Raafat a consultant who has been active in this field since before the start of the initial project to develop a risk assessment methodology for machinery. He is based at Aston University's Health and Safety Unit, which has close links with HSE. These guidelines also form the basis of a one day seminar which is run regularly for industry. They first give a good background into the development of legislation in the machinery field from the "Factories Act 1961" and the "Health and Safety at Work Act 1974" to the relatively new influence

of European Product Directives on UK legislation. This includes an explanation of the role of standards.

A fairly comprehensive explanation of machinery hazards and methods for safeguarding against them, in particular the use and abuse of interlocks is then given. A hazards checklist is provided, a hazard identification technique similar to HHEA [Worsell & Wilday 1995] is also described along with two techniques for risk estimation/ranking reviewed by our project team [Worsell & Wilday 1997a].

5.5. Australian Guidance

There are two useful publications from WorkSafe Australia, one is aimed at manufacturers of 'plant' [Worksafe Australia 1995a] which includes what we understand as machinery, the other [Worksafe Australia 1995b] at users of 'plant'. Both give a good explanation of risk assessment in practice. The guidance first explains how to systematically identify hazards but unlike '5 Steps' [HSE 1998b] it then suggests considering both the likelihood and consequences of the hazardous situation occurring. Four clearly defined categories are given for both. A risk table is provided which enables risk to be rated (or as we would say ranked) once appropriate categories are selected. Clear guidance is also given on how to do this. It is worth noting that this risk table appears to be a development of the HAZPAK matrix technique published by WorkCover, New South Wales, Australia, which has been reviewed by the project team [Worsell & Wilday 1997a]. The inputs to the table are the same, the guidance is similar but the risk rating has been simplified to High, Medium and Low rather than as in HAZPAK a number from 1 to 6. Both then give clear guidance of how to follow a similar hierarchy of control as given in the Machinery Directive but more comprehensively with useful sub-categories.

5.6. ICI Eutech Paper on Machinery Design

This paper, "Machine reliability and safety methodology of assessment and approval", [Lewis 1998] deals with how the Machinery Directive, Provision and Use of Work Equipment Regulations (PUWER) and the Construction Design and Management Regulations (CDM), fit in with machinery used in process plant. It describes how ICI Eutech comply with these regulations and at the same time reduce the likelihood of major incidents and increase machine reliability. The key seems to be the classification of machinery according to its hazard potential and verification of design intent taking into account the overall process not just the machine in isolation.

5.7. Probability Risk Assessment of Engineering Systems

This book [Stewart & Melchers 1997], describes and discusses how Probabilistic Risk Assessment (PRA) can be used to analyse engineering systems. It attempts to avoid focusing on any particular industry. The book is very thorough. Explanations are given of how to: model an engineering system; identify all sources of risk describing all the well known techniques available for hazard identification and take into account human factors describing the use of various techniques for human error analysis. There is a discussion of uncertainty, risk criteria, communication and perception. The book also contains some failure rate and human reliability data.

6. CONTROL SYSTEM DESIGN STANDARDS

6.1. BS EN 954:1997 Safety Related Parts of Control Systems,

Part one of this British/European standard has been available to designers of control systems for several years now. This has the status of an application standard (Type B1) under the Machinery Directive. Part 2 of this standard "Validation", is available as a prEN.

It is stated in the foreword to this European Standard that it is "intended to give guidance during the design and assessment of control systems and to Technical Committees preparing type B2 or type C standards". It applies to all, but only safety-related parts of, control systems, "regardless of the type of energy used, e.g. electrical, hydraulic, pneumatic, mechanical". This includes programmable systems for all machinery (as defined in the Machinery Directive) and for related protective devices. "The performance of a safety-related part of a control system with respect to the occurrence of faults is allocated in this standard into five categories (B, 1, 2, 3, 4)". These categories state "the required behaviour of safety-related parts of a control system in respect of its resistance to faults". This is described for each category in terms of fault tolerance through the concepts of redundancy and diversity. It does not specify which safety functions and which categories shall be used in a particular case. Instead it requires the designer "to decide the contribution to the reduction of risk which needs to be provided by each safety-related part of the control system" and that "the design of safety-related parts of control systems including the selection of categories should be based on a risk assessment". It is also stated that "the greater the reduction of risk is dependent upon the safety-related parts of control systems, then the ability of those parts to resist faults is required to be higher".

Unfortunately it is not possible to compare one category with another in terms of safety integrity. A well designed and simple control system using highly reliable components, in which there is a low probability of design error could quite conceivably be safer than a highly diverse, complex control system using low reliability components and prone to design mistakes (systematic faults). This is recognised in the standard as it is stated that "these categories are not intended to be used in any given order or in any given hierarchy in respect of safety requirements." But it then goes on to describe a risk graph method for the selection of the appropriate category which implies that the categories are hierarchical in terms of the amount of risk reduction that they provide. The lack of consideration of systematic faults that

could swamp all other considerations (44% of accidents in a recent analysis of accidents by the HSE were attributed to errors in design[4]) is of particular concern.

So to summarise:

categories have no or inconsistently implied reference to reliability;
systematic faults are not properly dealt with;
the importance of quality assurance of design in ensuring functional safety is not properly covered;
the standard uses fault avoidance as its main premise.

An associated undated reference is the Electrical Contractor's Association "Guidance on the use of EN 954-1 machine safety standard for safety-related parts of control systems" [Electrical Contractor's Association]. This helpful document describes the differences between categories.

6.2. IEC 61508 Functional Safety of E/E/PE Safety-Related Systems

This IEC[5] standard uses the concept of the "safety lifecycle" as a framework for dealing systematically with all activities necessary for ensuring the functional safety of Electrical / Electronic / Programming Electronic (E/E/PE) safety-related systems [IEC 1998]. The standard specifies requirements for the control and avoidance of faults in both hardware and software at all stages in the overall systems lifecycle. The standard consists of the following seven parts:

1 General requirements;
2 Requirements for E/E/PE safety-related systems;
3 Software requirements;
4 Definitions and abbreviations;
5 Examples of methods for the determination of safety integrity levels;
6 Guidelines on the application of parts 2 and 3;
7 Overview of techniques & measures.

Parts 1, 2, 3 and 4, with the exception of the annexes to part 1, are normative. The other parts are informative offering guidance and supplementing the normative parts.

Figure 1 in part 1 of the standard illustrates diagrammatically the relationships between each part of the standard in an overall framework. This has been reproduced at the end of this document. In addition, also in part 1, figure 2 illustrates the safety lifecycle mentioned above. For completeness, as this is a key concept on which the standard is based, this figure has also been reproduced at the end of this document.

The main objective of IEC 61508 is to ensure that all the safety-related systems achieve the required level of functional safety for the Equipment Under Control (EUC). This involves first correctly specifying the functional safety requirements and subsequently, what practices, procedures and techniques are required to implement them adequately, i.e. good design is recognised as making a necessary contribution to safety. Secondly, it is essential to ensure that

[4] See section 4 of HSE's "Out of Control"
[5] International Electrotechnical Commission

each safety function achieves its stated level of safety integrity (i.e. the probability of a safety-related system satisfactorily performing the required safety function under all stated conditions within a stated period of time). What is adequate is determined by the extent of the required risk reduction that the safety-related systems are required to deliver, in their application.

This leads us to another important concept in IEC 61508, that of safety integrity levels (SILs). There are four 'SILs' numbered 1 to 4. Unlike the safety categories of EN 954 SILs are in an ascending hierarchy in which 4 represents the highest level of integrity, i.e. the lowest probability of failure to perform its required safety function under all stated conditions and within a stated time period. SILs are a measure of the amount of risk reduction required by the safety-related systems in order to achieve the desired tolerable risk.

Once the designer has selected the appropriate SIL, IEC 61508 recommends procedures and techniques necessary to enable this level of integrity to be achieved. This list is not exhaustive and therefore, difficulties can arise when new technologies are used.

Part 5 of the standard provides information on how to make this selection based on risk and includes examples of various risk estimation techniques. Despite this it is still very difficult to select the appropriate SIL, i.e. to decide how safe is safe enough. It is important however to remember that IEC 61508 is designed as a generic standard and it is expected that sector specific standards will provide clear guidance on risk assessment and appropriate levels of risk. It is also worth mentioning that the status of IEC 61508 is such that any other IEC standards having E/E/PE safety-related systems within their scope will need to, wherever possible, adopt its requirements. To summarise:

- categories are directly related to reliability;
- systematic faults are explicitly considered;
- the importance of quality assurance of design in ensuring functional safety is recognised and covered in some detail;
- however the standard is complex, not particularly easy and time-consuming to use, and could be seen to be bureaucratic, however sector specific standards are expected to overcome this in due course.

Rather than go into any further detail the reader is referred to a number of papers some published and others internal to HSE on the subject of IEC 61508:

The papers "IEC 61508 - Current status and implications for PLCs" [Brown 1998] and "Emerging international standards for instrument protection systems used in safety applications" [Wilson 1997] both give an overview of requirements.

"Framework for computer based safety-related systems: Overview of draft international standard IEC 61508", [Bell 1998] goes into less detail about requirements but adds some background into the development of the standard and future issues.

Another paper, "A case history of the application of draft international standards IEC 1508 to the needs of the process industries" [Tuff & Beale 1997], gives an overview of the contents

but in addition describes practical application in the chemical process industry which includes lessons learnt from the experience.

An earlier paper "Risk and system integrity concepts for safety-related control systems" [Bell & Reinert 1992] describes an earlier draft of IEC 61508 but also usefully goes into some detail about risk estimation techniques for selecting safety integrity levels.

The paper "Generalised calculation of software safety integrity" [Fergus 1998] gives an interesting example of how the risk graph technique, given in IEC 61508, can be used for selection of software integrity levels for a non-control but safety-related application. The application is the development of software used as a decision aid in land-use planning in the vicinity of major hazards.

Finally "IEC 61508 - an influential standard" [Redmill 1999] gives a good overview of the standard's aims and objectives and goes into some detail about management issues.

6.3. DIN V 19 250

This German standard, "Control Technology: Fundamental safety aspects to be considered for measurement on control equipment" [DIN V250 1994] describes the risk graph that was incorporated into IEC 61508 and gives some background into its development. In particular an explanation of why all possible combinations of factors are not shown on the graph. It also includes a number of practical examples of the use of the risk graph.

6.4. DEF STAN 00-56 Safety Management Requirements

This standard is one of a family of standards dealing with safety that is being developed or adopted by the Ministry Of Defence (MOD) [DEF STAN 00-56 1996] taking into account international standardisation activities and supporting research and development. This standard comes in two parts: part 1 describes the requirements for safety management, including hazard analysis and safety assessment and part 2 provides generic information and guidance on the safety management requirements for safety related systems.

The concept of risk and its consequences is described in part 1 section 7.4 of this standard as well as an interesting technique for SIL selection (denoted by the letter S in the document) as defined by IEC 61508. A matrix format is used to classify the integrity levels based on two parameters, the probability of failure of a safety-related component performing its primary function and the accident severity (as shown below).

Failure probability of 1st function	Accident severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	Level S4			
Probable		Level S3		
Occasional			Level S2	
Remote				
Improbable			Level S1	

IEC 61508 adopts a similar approach through the use of a risk graph. However, four parameters are used in IEC to select the SILs instead of two. By including the probability of avoidance and the frequency of exposure of the unwanted event combined with the two parameters mentioned above, the SIL specification can change dramatically. Nonetheless, it is an interesting way of classifying SILs.

7. CONTROL SYSTEM DESIGN GUIDANCE

7.1. The PES Guide

HSE's guidance on "Programmable Electronic Systems in safety related applications" is generally referred to as "the PES guide" [HSE 1987]. It comes in two parts. The first explains in general terms what PES is and goes into some detail about how PES can fail. It requires the designer to follow the steps given below and gives guidance on how this can be achieved in practice.

A: Hazard analysis: What are the likely sources of danger?
B: Identification of the safety-related systems: On which systems does the safety of the installation depend?
C: Determination of the required safety level: How safe is safe enough?
D: Design of the safety-related systems: How can these systems be designed to meet the required safety level?
E: Safety analysis: Does the installation meet the safety requirements?

The safety strategy involves an understanding and appreciation of the importance of the principles of reliability, configuration and quality. The second part of the guide, general technical guidelines" covers in more detail what is referred to as "the three point strategy". It describes techniques for hazard analysis, the reliability analysis of alternative configurations, gives guidance on quality assurance, and comprehensive checklists for software failures.

The PES guide is currently the only available detailed guidance. It was published in 1987 and has been used for many years by a wide range of industries. However it does not give industry specific guidance on how to determine the required safety levels for each safety function. The requirements of paragraph 29 (b) and (c) "no failure of: a single channel of hardware; or fault within the software associated with a single channel; should cause a dangerous mode of failure of the safety related system" is also considered by some people in industry to be too restrictive.

7.2. EEMUA's Safety Related Instrument Systems for the Process Industries

This publication [EEMUA 1989], produced by a subcommittee of the EEMUA (Engineering Equipment Manufacturers and Users Association) is intended to be the process industries' specific application of the PES Guide and has been produced in accordance with HSE's invitation in part 2 of the PES Guide. The general advice in this document is to separate safety protection systems from control systems and a formal method of categorising systems is described in a tabular format. Only category 1 systems need then to be designed in accordance with the PES guide. However the reliability of category 2 and 3 systems could affect the demand rate on category 1 systems.

Very little reference is made to safety integrity levels (this publication predates IEC 61508), beyond the definition of safety integrity as being "that characteristic of a safety related system relating to its ability to perform its required functions in the desired manner under all the relevant conditions and on the occasions when it is required so to perform". Safety integrity criteria are also defined as "the criteria used as the basis for the safety integrity design and analysis of the safety related system". We were then unable to find any further reference to these concepts. Overall the document adds little from the point of view of machinery risk assessment that has not already been covered in PES part 2.

7.3. Out of Control

This guidance [HSE 1995] is aimed particularly at those concerned with the technical aspects of the specification, design, fabrication, commissioning and maintenance of control systems. The purpose of the guidance is to raise awareness of the technical causes of control system failure through their illustration by examples of incidents which have happened in the past. It contains an analysis of accidents which shows that just over 44% could have been prevented if more care had been put into the specification of a control system, thereby highlighting the importance of a systematic approach to hazard identification and risk assessment when specifying the control system.

The examples of actual incidents are taken from a range of industries and are very effective at getting various messages across, which otherwise would have seemed rather theoretical. Appendix 2 describes the safety lifecycle model as used in IEC 61508.

7.4. CCPS - Guidelines for Safe Automation of Chemical Processes

The chemical process industry is also becoming increasingly automated with the advent of PES for measurement, control and alarm systems and this trend is expected to continue. The Center for Chemical Process Safety of the American Institute of Chemical Engineers (CCPS/AIChE) recognised the potential of this technology to increase design and maintenance errors and the consequent implications for safety. As a result they published the above book [CCPS 1993] aimed at the chemical process industry. It takes a similar approach to ensuring safety as that taken by IEC 61508, including the use of safety integrity levels.

A technique for the selection of an appropriate SIL, which takes into account the number of independent layers of protective against the hazard in question, is described in chapter 2. Examples of its use are given in chapter 7. It is also worth noting that appendix G contains a list of potential PES failure modes.

7.5. Guidance on HAZOP Procedures for Computer-Controlled Plants

This contract research report [HSE 1991] produced by KBC Process Technology Ltd is also aimed at the chemical process industry. The HAZOP methodology described could equally be applied to machinery control systems. However, further consideration of the procedures and guide words would be required before we could recommend its use as described in the report. As the conclusions to the report itself point out, the methodology is only tentatively proposed and should be tested before wider dissemination. It is also worth remembering that HAZOP is very familiar in the chemical process industry but not in others. A number of interesting comments were made during an industry survey and these are described in appendices one and two.

7.6. MISRA Reports

MISRA's "Development Guidelines for Vehicle Based Software" [MISRA 1994] follow a similar approach to IEC 61508, for example the safety lifecycle, integrity levels etc.. They are aimed specifically at the Motor Industry considering only issues relevant to this industry. The Motor industry is one in which there has been a rapid increase in the use of PES, a trend which is expected to continue with increasing sophistication and complexity. Public perception is an important issue in this industry as cars are expected to be safe and the driver does not expect to be put at risk by the electronics under the bonnet.

The guidelines describe an interesting technique for the selection of SILs. This has been adopted from the 'DRIVE' project aimed at Transport Telematic Systems. The DRIVE project is discussed separately in the following section of this report. Each hazard is assessed for the degree of control over the safety of the situation that remains after a failure has occurred, one of the controllability categories listed in the table below is selected, and this defines the SIL required along with an acceptable failure rate. It is worth noting that there is a deviation from IEC 61508 by the reference to a SIL of 0.

Controllability Category	Acceptable Failure Rate	Integrity Level
Uncontrollable	Extremely improbable	4
Difficult to control	Very remote	3
Debilitating	Remote	2
Distracting	Unlikely	1
Nuisance only	Reasonably possible	0

Various factors are described which need to be considered when selecting the appropriate category. Some of these are quite general and others are more specific to motor vehicles such as vehicle stability, controllability of acceleration, braking, visibility impairments etc. In many

ways machinery can be likened to a motor vehicle driven by the operator, so many of the factors can also be related to machinery. This would therefore seem to be a simple way of selecting SILs.

A later report [MISRA 1995] builds on the report discussed above and incorporates much of the material presented in the reports discussed in the following section, for example the concept of confidence levels. This MISRA report also gives considerable detail on how to achieve both the specified integrity level and associated confidence level once a SIL has been selected based on the process described above.

There are several other publications by MISRA relevant to the design of PES safety-related control systems in line with IEC 61508. These are briefly described below.

- *"Guidelines for the use of the C Language in Vehicle Based Software"*, this document provides guidance for C programming of safety-related automotive embedded systems.
- *MISRA report 1, "Diagnostics and Integrated Vehicle Systems"*, this report covers the aspects of vehicle engineering which relate to the use of software to support integrated communications and diagnostics networks. The report covers vehicle architecture, communications and multi-plexing, on-board diagnostics, off-board diagnostics, tools and testing.
- *MISRA report 3, "Noise, EMC, and Real-time"*, this report covers issues associated with electromagnetic compatibility (EMC) and also those associated with the implementation of real-time systems. This report generally assumes that hardware has been designed to reject electromagnetic interference and considers only what additional steps may be taken in software.
- *MISRA report 4, "Software in Control systems"*, this report examines the role of software in the design of control systems. It is divided into three parts: theoretical considerations; design considerations and practical considerations.
- *MISRA report 5, "Software Metrics*", this document identifies a number of software attributes and metrics which may be used to provide a measure of those attributes and hence of the quality of software.
- *MISRA report 6, "Verification and Validation*", this document presents the verification and validation activities that should be performed upon the component subsystems of a modern vehicle with emphasis on software components.
- *MISRA report 7, "Subcontracting of Automotive Software"*, this report gives an overview of the topics which should be considered by engineers, managers and purchasing departments involved with purchasing, selling, creating and managing software products.
- *MISRA report 8, "Human factors in Software Development"*, this document presents the human factors engineering implications and influences.

- *MISRA Survey report, "Sources of reference"*, this covers a list of references, background documents and the summary of the findings of the MISRA study into safety-related PES.

Some of the information and documentation presented above was downloaded from MISRA's web site at www.misra.org.uk. It is also worth noting that MISRA has recently started some work to produce guidelines on Preliminary Safety Analysis for the Motor industry. This will include further advice on safety integrity levels and the first draft is due out in 2000.

7.7. Safety Aspects of Advanced Transport Telematic Systems

Various project reports and other documents relating to several EMCATT (Electromagnetic Compatibility of Advanced Transport Telematics) [EMCATT 1995] European research projects were obtained from Peter Jesty of Leeds University.

The first report of interest from the DRIVE II project - "Functional System Safety and Electromagnetic Compatibility" [Jesty *et al* 1995] considers faults caused to advanced transport telematics (ATT) systems by electromagnetic interference. It repeats a lot of what can be found in IEC 61508, in particular it includes a full description of the techniques for selecting SILs as given in part 5 of the standard. It also gives a little more detail, in appendix 2, about the same technique described in the MISRA document, in particular the use of other factors to select the appropriate controllability category.

There is also a clear, concise description of the ALARP principle following on from which is a good argument for the need for different levels of integrity. It explains that this need arises from the fact that some activities are perceived as being more hazardous than others. It then moves on to explain that the use of SILs is desirable because the costs associated with the higher integrity levels can be very great and therefore a balance must be struck between using too low a level, which will increase the risk, and using too high a level which will result in unnecessary costs.

In addition this document introduces, in section 6.2, the concept of confidence levels. This relates to the level of confidence that the designer/provider has that the end result will be used safely by the public. In general the report states that as the SIL level increases so must the confidence level, not only that the system will provide the desired function but also that the function is the correct one. This concept is incorporated in the requirements of IEC 61508 although the terminology "confidence level" is not used as something distinct from the SIL.

The second report of interest is "Framework for Prospective System Safety Analysis: Volume 1 - Preliminary Safety Analysis" [Hobley *et al* 1995], referred to as PASSPORT II. This describes a systematic methodology for performing safety analyses on advanced road transport telematics.

The methodology is divided into two phases. The first, referred to as Preliminary Safety Analysis, consists of:

- Modelling the system using the novel PASSPORT diagram, an essential feature of which is that it can be checked for completeness and consistency.
- Hazard analysis to identify the safety requirements using the "What If?" technique.
- Assignment of preliminary SIL using the controllability technique described earlier.

The second phase consists of a detailed safety analysis to confirm the findings of the first and establish that the safety requirements have been implemented. This is essentially to ensure that system safety is adequately accounted for during system definition and design. This is then followed by a certification process, which aims to ensure that the system is safely and correctly implemented.

In addition Mr Jesty provided some useful internet web addresses. In particular the following www.trentel.org./index.htm from which it was possible to download the report on a "Co-ordinated Dissemination in Europe of Transport Telematics (CODE TR) System Safety Guidelines" [Jesty *et al* 1998]. This is quite a large document which neatly summarises the contents of the other reports, the developments and background to the DRIVE and PASSPORT projects. It describes in general terms the DRIVE II framework and the relevant techniques used for the hazard identification process from the PASSPORT II report as well as the adaptation from the Automotive Industry.

Appendix B of this report gives a clear and easily understood description of the technique for assigning SILs based on controllability categories. Of more interest though perhaps is the following statement found in this appendix:

> "the basic principle is to choose the lowest SIL necessary, rather than the highest SIL possible".

This could possibly be incompatible with the ALARP principle depending on how one defines the word necessary. The reports produced by these two programmes (which follow on from the original DRIVE project documented in the report “Drive safely - towards a European Standard: the development of safe road transport informatic systems” [Jesty et al 1992] go a long way towards providing Motor industry specific guidance to IEC 61508, something that no other industry sector have yet achieved.

"Integrity Levels and their Application to Road Transport Systems", [Jesty and Hobley 1996] gives a quick overview of the work of these projects prior to 1996. It is quite brief compared to the other references. Mr. Jesty is also author or co-author of several very readable papers of background interest which are listed in the references. One of the more interesting is perhaps “As safe as necessary” [Jesty 1997] which makes a good argument for the use of SILs in designing systems to be “as safe as necessary” rather than “as safe as possible”. The paper also explains why in this industry traditional risk estimation techniques such as those used in the chemical process industry were not suitable and hence the usefulness of the concept of ‘controllability’.

This paper also discusses the subtle but serious differences between software and hardware and the difficulties in ensuring the safety of software systems; thereby making a strong case for reducing as far as possible the reliance for safety of the system on its software.

7.8. Towards safer industrial computer controlled systems

There are two papers [Croll *et al* 1997] with a similar title, one of which was presented at the 16th International Conference on Computer Safety, Reliability and Security 1997. It describes the development of the HAZAPS methodology and supporting software tool for hazard analysis of computer systems. This work follows on from an earlier analysis of incidents involving programmable electronic safety-related systems [Chambers *et al* 1999], only recently published, which showed that many incidents were due to inadequate system or safety requirement specification or poor design of either software or hardware. This paper demonstrates that a good hazard analysis technique would have helped prevent the majority of these accidents but that unfortunately there was a general lack of experience of such techniques in the industry.

7.9. Design for Safety

This paper [Storey 1999] (presented at the symposium "Towards System Safety" organised by the safety-critical systems club) is of background interest as it contains one possible description of the design process as being made up of:

abstraction	-	generalising the problem (normally referred to as the problem statement), identifying the essentials of the solution (concepts);
decomposition	-	breaking the problem and solutions down into simpler smaller parts;
elaboration	-	the detailed design or detailing;
decision making	-	identification of and selection between alternative strategies.

Note that decisions need to be made throughout the other steps not just at the end.

It points out that the safety requirements i.e. what the system must and must not do in order to maintain safety, need to sit alongside the functional requirements; but it is not clear during which of the above processes these requirements are drawn up. It then goes on to describe the ways in which safety can be assured during design and suggests 4 basic concepts and specific techniques that can be used to achieve them:

fault removal	-	maintenance
fault avoidance	-	reliability engineering and quality assurance
fault detection	-	monitoring/testing
fault tolerance	-	redundancy and diversity

These concepts and techniques are then described in some detail.

7.10. Cooper on Fail-Safety

This paper [Cooper 1999] gives some useful guidance on the concept of fail-safety. It warns that claims that a particular system or instrument can only fail-safe needs critical appraisal. It further states that a product or process should fail to a known condition. Whether that condition is safe or not is not the sole decision of the equipment supplier but of a partnership between supplier and operator. Also that the key to fail-safety is "the assessment of what the safe condition of the process really is". As far as risk assessment goes the paper recommends an all embracing approach which encompasses the design of the equipment, operating procedures, maintenance requirements and the suitability for purpose of safety related devices.

8. CONCLUSIONS

There is now considerable activity and interest in the use of risk assessment in the machinery, and other similar sectors, where it has not been traditionally used in the past. This was not the case when the machinery risk assessment methodology was first developed. The pace is such that it is quite difficult to keep up to date with developments. However this report has captured the bulk of the information that has been digested to date by members of the project team. Many of the references included have been published in the last few years. It should therefore provide a useful source of information for the continuation of the validation project and other related support activities.

There is still evidence that there is a need for comprehensive practical guidance for the application of risk assessment to machinery by designers. The design of machinery has also been shown to have important implications for safety in a recent HSE review [Eaton 1999]. Moreover, this indicates that it is important for HSE to remain active in providing input to standards making (European and International) in this area.

Various other techniques identified as having the potential to be usefully incorporated into the machinery risk assessment toolkit should be looked at in further detail by the project team.

9. REFERENCES

ACDS (1991)
"Major Hazard Aspects of the Transport of Dangerous Substances", HSC

ACMH (1984)
"Third Report", HSC

AS/NZS 4360:1999
"Risk Management"
Joint publication of Standards Australia and Standards New Zealand

Ball D J and Floyd P J (1998)
"Societal Risk"
Report prepared for the HSE available from risk assessment policy unit

Balmforth H (2000)
"An Approach to Assessing the Adequacies of the Machinery Directive and its Associated Standards for Chemical Hazards Emissions", RAS/00/08

Bell R and Reinert D (1992)
"Risk and System Integrity Concepts for Safety-Related Control Systems"
Safety Science

Bell R (1998)
"Framework for Computer Based Safety-Related Systems: Overview of Draft International Standard IEC 61508", HSE PES Seminar

Brown S (1998)
"IEC 61508 - Current Status and Implications for PLCs", HSE

BS EN 292 (1991)
"Basic Concepts, General Principles for Design"
parts 1 and 2 (revision issued for public comment April 2000)

BS EN 954 (1997)
"Safety of Machinery - Safety Related Parts of Control Systems",
Part 1. "General Principles for Design"

BS EN 1050 (1997)
"Principles for Risk Assessment"

BS 5304 (1988)
"British Standard Code of Practice for Safety of Machinery"

BSI (1998 and 1999)
"CE Marking for Machinery (Europe)"

CCPS (1993)
"Guidelines for Safe Automation of Chemical Processes"

Chambers C, Croll P R and Bowell M. (1999)
"A Study of Incidents Involving Programmable Electronic Safety-Related Systems" Interacting with Computers, 11(1999), 597 - 609, Elsevier Science

Cooper S P (1999)
"Fail-Safety - Availability of European standards in order to meet ATEX requirements"
3rd World wide seminar on the explosion phenomenon and the application of explosion protection techniques in practice, European Institute for Explosion Safety and Related Industrial Risks (EuropEx), Flanders Expo, Ghent, Belguim, Feb 99

Croll P R, Chambers C, M Bowell and Chung P W H (1997)
"Towards Safer Industrial Computer Controlled Systems"
16th Int. conference and workshop SAFECOMP'97, University of York

DEF STAN 00-56/Issue 2 (1996)
"Safety Management Requirements for Defence Systems" - Part 1: "Requirements" and Part 2: "Guidance"

DIN V 19 250 (1994), "Control Technology: Fundamental Safety Aspects to be Considered for Measurement on Control Equipment"

Eaton S (1999)
"A Brief Review of Fatal Accidents at Machinery", MSSG 33/99

EEMUA (1989)
"Safety Related Instrument Systems for the Process Industries: Including Programmable Electronic Systems", publication No. 160.

van Ekelenburg H P, Hoogerkamp P and Hopmans L J (1997)
"A Practical Guide to the Machinery Directive", May 1997 update, MEP

Electrical Contractor's Association (undated)
"Guidance on the Use of EN954-1 Machine Safety Standard for Safety-Related Parts of Control Systems"

Elvik R (1999)
Cost-Benefit Analysis of Road Safety Measures: Applicability and Controversies"
ESReDA Conference, Oslo, Norway, May 1999

EMCATT (1995)
"Safety Aspects of Advanced Transport Telematic Systems", DRIVE II project V2064.

Engineering Council (1993)
"Guidelines on Risk Issues"

EU (1998)
Machinery Safety Directive, (89/392/EEC), amended, (98/37/EEC)

Fergus E (1998)
"Generalised Calculation of Software Safety Integrity", HSE PES seminar

Fischhoff B, Lichtenstein S, Slovic P, Derby S L and Keeney R L (1981)
"Acceptable Risk"

Hibbert L (1999)
"Machinery Falling Short of the Mark",
Professional Engineering, Volume 11, Number 22

Hobley K M and Jesty P H *et al* (1995)
"Framework for Prospective System Safety Analysis:
Volume 1 - Preliminary Safety Analysis", PASSPORT II

HSE (1987)
"PES Programmable Electronic Systems in Safety Related Applications: Part 1 An Introductory Guide, Part 2 General Technical Guidelines"

HSE (1989)
"Risk Criteria for Land-use Planning in the Vicinity of Major Industrial Hazards".

HSE (1991)
"Guidance on HAZOP Procedures for Computer-Controlled Plants"

HSE (1992)
"The Tolerability of Risk from the Nuclear Power Stations"

HSE (1993)
"Quantified Risk Assessment: Its Input to Decision Making."

HSE (1995)
"Out of Control", C50

HSE (1998a)
"Safeguarding Agricultural Machinery", HSG89

HSE (1998b)
"Five Steps to Risk Assessment", IND(G) 163 (rev 1)

HSE (1999)
"Reducing Risks, Protecting People: The Control of Risks from Industrial Activities"
Discussion Document DDE11 C150 5/99
Hurst N W, Nussey C and Pape, R P (1989)
"Development and Application of a Risk Assessment Tool (RISKAT) in the HSE"
Chem. Eng. Res. Des., Vol 67, July

Hurst N W (1998)
"Risk Assessment: The Human Dimension"
Royal Society of Chemistry

IEC (1998)
IEC 61508 “Functional Safety of Electrical / Electronic / Programming Electronic Safety-Related Systems”
-Part 1 “General requirements”,
-Part 2 “Requirements for E/E/PE safety-related systems”,
-Part 3 “Software requirements”,
-Part 4 “Definitions & abbreviations”,
-Part 5 “Examples of methods for the determination of safety integrity levels”,
-Part 6 “Guidelines on the application of parts 2 and 3”
-Part 7 “Overview of techniques & measures”

IEE (1992)
"Professional Brief on Safety-related Systems"

IGE(1999)
"Risk Assessment Techniques"
IGE/SR/24:1999, Institute of Gas Engineers Communication 1655

ISO/IEC (1999)
Guide 51

Jesty *et al* (1992)
“Drive safely - towards a European Standard: the development of safe road transport informatic systems”

Jesty P H, Hobley K M, Klinger M and Szelag M (1995)
"Functional System Safety and EMC"
DRIVE II Project (V2064)

Jesty P H and Hobley K M (1996)
"Integrity Levels and their Application to Road Transport Systems",
SafeComp96, Vienna, Austria.

Jesty P H (1997)
"As Safe as Necessary"
Traffic Technology International June/July

Jesty P H, Giezen J and Fowkes M (1998)
"Co-ordinated Dissemination in Europe of Transport Telematics: System Safety Guidelines", CODE TR 1103.

Lees F P (1996)
"Loss Prevention in the Process Industry"

Lewis J J (1998)
"Machine reliability and safety - methodology of assessment and approval"
IChemE Loss Prevention Bulletin No 144.

Macbeth R W (1998)
"A Study into the Use of the Approximate Risk Integral as a Representation of Societal Risk in Toxic RISKAT", IR/RAS/98/10

MISRA (1994)
"Development Guidelines for Vehicle Based Software"

MISRA (1995)
"Report 2 - Integrity"

NERA (1998)
"Developing a Common UK Approach to Negotiations on Risk Assessment at International Level", Final report for HSE prepared by National Economic Research Associates

Parry S T (1986)
"A Review of Hazard Identification Techniques and Their Application to Major Accident Hazards", SRD/R/379

Raafat H (1995)
"Machinery Safety: The Risk-Based Approach",
Technical Communications (Publishing) LTD

RAPU (1995)
"Principles and Guidelines to Assist HSE in its Judgements that Risk has been Reduced 'As Low As is Reasonably Practicable' (ALARP)", HSE

Redmill F (1999)
"IEC 61508 - An Influential Safety Standard"
The Safety and Health Practitioner, Feb

Schneider T, Weber K and Locher R (1995)
"Risque, acceptation des risques du point de vue technique et sociologique, approche du dialogue sur les risques", study of the Swiss acadamy of science, SUVA, CNA, INSAI (also available in German and Italian), Summary and conclusions translated into English (Ref 16110/9900 20002) "Risk, acceptance of risk from the technical and sociology point of view, an approach for dialogue on risk".

Stewart M G and Melchers R E (1997)
"Probabilistic Risk Assessment of Engineering Systems"

Storey N (1999)
"Design for Safety"
Proceedings of the 7th Safety-critical Systems Symposium, Huntingdon, UK

Tuff G C and Beale C J (1997)
"A Case History of the Application of Draft International Standards IEC 1508 to the Needs of the Process Industries"
IChemE Symposium Series No 141, Hazards 13 Conference

Wells G (1996)
"Hazard Identification and Risk Assessment", IChemE

Wilday J and Worsell N (1997)
"The Application of Risk Assessment to Machinery Safety, Risk Estimation and Risk Evaluation", RAS/97/13

Wilday J, Wray A, Eickhoff F, Unruh M, Halama S, Fae E, Conde E and Reina P (2000)
"Determination of Safety Categories of Electrical Devices Used in Potentially Explosive Atmospheres: Final Report", PS/00/draft

Wilson M (1997)
"Emerging International Standards for Instrument Protection Systems used in Safety Applications", IChemE Symposium Series No 141, Hazards 13 Conference

Worksafe Australia (1995a)
"Plant Design Making it Safe"

Worksafe Australia (1995b)
"Plant in the Workplace Making it Safe"

Worsell N and Wilday J (1995)
"The Application of Risk Assessment to Machinery Safety, Hazard Identification Techniques", IR/L/RAM/95/01

Worsell N and Wilday J (1997a)
"The Application of Risk Assessment to Machinery Safety, Review of Risk Ranking and Risk Estimation Techniques", RAS/97/12

Worsell N and Wilday J (1997b)
"The Application of Risk Assessment to Machinery Safety, Final Report", RAS/97/14

Worsell N and Chambers C (2000)
"Other Hazard Identification Techniques for the Machinery Risk Assessment Toolkit", RAS/00/draft

Wray A M (1999)
"The Link Between the EN 954-1 and IEC 61508 Standards: The STSARCES Project", CI/99/1

10. ACKNOWLEDGEMENTS

The project leader would like to acknowledge all those people in TD and HSL who provided me with relevant references, in particular those who provided me with information and draft reports on relevant project work, Tony Wray, Helen Balmforth, Tom Treble and Jill Wilday. In addition, Richard Wilson for keeping me up to date with developments in Europe. Also the Sheffield HSE library and information centre for providing many of the references, often at short notice. I would also like to acknowledge the helpful comments and contributions to this report from Jill Wilday and Colin Chambers.