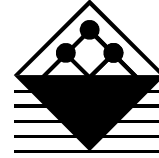


Broad Lane, Sheffield S3 7HQ

Telephone: 0114 289 2000



**HEALTH & SAFETY
LABORATORY**

SAFETY INTEGRITY LEVELS OF FAIRGROUND

RIDE CONTROL SYSTEMS:

Project leader: Nicola Worsell

Agamemnon Ioannides BSc, MSc

Nicola Worsell BSc, MSc

HEALTH AND SAFETY LABORATORY

An agency of the Health and Safety Executive

DISTRIBUTION

Mr R Bell	TD1
Eur Ing S Brown	TD1
Eur Ing S Frost	TD1
Mr N Gove	TD1
Mr J McDonald	TD2
Mr E Pirie	FOD, Food & Entertainment Sector
Mr T Williams	FOD, Food & Entertainment Sector
Research Committee Members (10)	Fairgrounds and Amusement Parks Joint Advisory Committee
Dr A Jones	HSL, Operations Director
Dr N G West (circulation)	HSL, Head of Human Factors Group
Mr A J Jackson	HSL
Dr A M Wray	HSL
Ms A J Wilday	HSL
RAS (circulation)	HSL
Mr A Ioannides	ex-HSL
RAS Library (2)	HSL
HSE LIS (10)	

Available to the Public.

HSE Authorising Officer: Mr Neil Gove

HSL Report Approval: Dr Sandra Gadd
Date of Issue: March 2000
Job Number: R38.022
Registry File: RA/PR/17/1999
Document Filename: Q\RASREPS\R38.022\REP2.LWP

HEALTH AND SAFETY LABORATORY

An agency of the Health and Safety Executive

SUMMARY

Objectives

DST E1 (Directorate of Science and Technology) have identified a need to ensure that PES based control systems for fairground rides are designed, implemented and installed, operated and maintained in such a way that an adequate level of safety integrity is achieved. The Health and Safety Laboratory in Sheffield (HSL), was asked to propose a method for conducting risk assessments of fairground rides which identifies safety functions relevant to IEC 61508: "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems".

As preparatory work to the development of this method HSL has carried out an accident analysis relating to control system failures of fairground rides. This is documented in an earlier report [Ioannides & Worsell 2000]. A literature survey was also conducted to identify available guidance for fairground ride safety, control system design, relevant standards and available risk assessment techniques. This report describes the findings of the literature review.

Main Findings

A comprehensive literature review has confirmed that there is a lack of specific guidance to enable those involved with the implementation, use and maintenance of safety-related programmable fairground ride control systems to select the appropriate measures and techniques so that an adequate level of safety integrity is achieved and maintained. This lack of guidance also makes it very difficult for inspection, certification and regulatory bodies to determine whether measures and techniques taken by designers are adequate in relation to any particular application.

Although very little information is aimed directly at the fairground industry, there is considerable information and guidance for the effective operation, control, design specification and implementation of an amusement ride available in some form. There are only two standards aimed specifically at the fairground industry but these do not provide any detailed information about control system design. They are the American (ASTM) and Australian (AS 3533/1988) standards. A European standard is in the process of being drafted. The July draft provides more information about the required functionality, but not integrity, of the control system than the American and Australian standards. However this standard is not currently generally available, not yet having even a provisional reference number, and is also subject to change.

There is also a considerable amount of information and ideas on risk assessment in general that can be drawn upon. However these are distributed over numerous documents. Various other industries have made progress towards a methodology for SIL selection and validation and have proved to be valuable sources of information. These are the Gas, Motor and Chemical industries.

Main Recommendations

The information and guidance relevant to the fairground industry needs to be collected together into one document for ease of use by the industry. Those existing techniques, modified as appropriate, for hazard identification and risk estimation/evaluation which can be usefully applied by the fairground industry need to be explained in an industry context; preferably with examples.

The ideas, presented in guidance from other industries, for the risk-based selection of SILs need to be considered in detail in the context of HSE's approach to risk, and a methodology appropriate for fairground rides developed. It is intended that this will be done in the further stages of this project.

CONTENTS

1. Introduction	1
2. Fairground References	
2.1 HSE's Fairground and Amusement Parks: Guidance for Safe Practice	1
2.2 SRD's Assessment of Risks at Fairground Rides	3
2.3 ASTM Standards	3
2.4 AS 3533:1988 - Amusement Rides and Devices	3
2.5 European Standard for Fairground Rides	4
2.6 HSE's Video	4
2.7 HSE / FOD's Survey of the use of PES in Fairground Rides	4
3. Control System Design Standards	
3.1 BS EN 954: Safety of Machinery - Safety Related Parts of Control Systems	4
3.2 IEC 61508 Functional Safety of E/E/PES Safety-related Systems	6
3.3 DIN V 19 250 Control Technology Standard	8
3.4 DEF STAN 00-56 / Issue 2 Safety Management Requirements	8
3.5 ANSI/ISA standard S84.01-1996	9
4. Control System Design Guidance	
4.1 The HSE PES Guide	10
4.2 IGE's Programmable Equipment in Safety Related Applications	10
4.3 EEMUA's Safety Related Instrument Systems for the Process Industries	11
4.4 Out of Control	12
4.5 CCPS - Guidelines for Safe Automation of Chemical Processes	13
4.6 Guidance on HAZOP Procedures for Computer-controlled Plants	14
4.7 MISRA Reports	14
4.8 Safety Aspects of Advanced Transport Telematics Systems	17
4.9 The Use of Computers in Safety-Critical Applications	19
4.10 Proceedings of 7th Safety-Critical Systems Symposium	20
4.11 Cooper on Fail-Safety	22
5. Hazard Identification and Risk Assessment	
5.1 HSE/HSC Guidance on Risk Assessment	22
5.2 SRD's Review of Hazard Identification Techniques	24
5.3 Engineering Council's Guidance on Risk Issues	24
5.4 Loss prevention in the Process Industry	24
5.5 Geoff Well's Hazard Identification and Risk Assessment	25
5.6 Fischhoff's Acceptable Risk	26
5.7 Ball and Floyd Report for HSE on Societal Risk	26
5.8 Swiss report Risqué	27
5.9 ISO/IEC Guide 51	28
5.10 Towards Safer Industrial Computer Controlled Systems	29
5.11 IGE's Risk Assessment Techniques	29

5.12 Probability Risk Assessment of Engineering Systems	30
5.13 Plant Functional Modelling Hazard Identification	30
5.14 Qualitative Techniques for Risk Estimation/Ranking	30
5.15 Elvik on Cost-Benefit-Analysis	32
6. Techniques for SIL selection	
6.1 Techniques Recommended by Summers	32
6.2 Techniques Described in Draft Standard IEC 61511	34
7. Discussion	36
8. References	41

1. INTRODUCTION

The safety of fairground rides is increasingly becoming reliant on complex programmable electronic control systems (PES) and it seems likely that this trend will continue. DST E1 (Directorate of Science and Technology) have identified a need to ensure that PES based control systems for fairground rides are designed, implemented and installed, operated and maintained in such a way that an adequate level of safety integrity is achieved.

The Risk Assessment Section of HSL was therefore asked to:

- conduct a literature survey on the guidance for fairground ride safety and available risk assessment techniques and standards.
- propose a method for conducting risk assessments of fairground rides which identifies safety functions relevant to IEC 61508¹ and which allows the determination of appropriate safety integrity levels for safety functions in programmable electronic control systems which are in line with HSE concepts of risk.
- to record the results of the above in a research report suitable for open publication to further the debate within the industry.

This document describes the results of the literature review. The references are subdivided into: those which relate directly to fairground safety - section 2, control system design standards - section 3, control system design guidance - section 4, information and guidance on hazard identification and risk assessment - section 5.

2. FAIRGROUND REFERENCES

2.1 HSE's Fairgrounds and Amusement Parks: Guidance for Safe Practice

There is very little guidance specific to the fairground industry with the notable exception of this guidance [HSE 1997]. Whilst addressing many of the general principles appropriate to safe practice, it does not set out any PES specific requirements. It also appears to be more applicable to small travelling amusement fairs rather than stationary theme parks. From this publication the following list of relevant legislation was drawn, all of which is general to many industries rather than specific to the fairground industry.

- The Health and Safety at Work etc. Act 1974.
- The Management of Health and Safety at Work Regulations 1992.
- The Electricity at Work Regulations 1989.
- The Provision and Use of Work Equipment Regulations 1992.
- Disability and Discrimination Act 1995.

¹ International Electrotechnical Commission for Functional safety of Electronic / Programming Electronic Safety-related systems.

It also lists the bodies represented on the Joint Advisory Committee (JAC) on Fairgrounds and Amusement Parks. These are:

- Health and Safety Executive (HSE)
- The Amusement Catering Equipment Society (ACES).
- The British Amusement Catering Trades Association. (BACTA).
- The British Association of Leisure Parks, Piers and Attractions (BALPPA).
- The National Association for Leisure Industry Certification (NAFLIC).
- The Showmen's Guild of Great Britain (SGGB).
- The Society of Independent Roundabout Proprietors (SIRP).

The HSE National Interest Group (NIG) responsible for the fairground industry has an agreement with this JAC to keep them informed of all ongoing HSE fairgrounds related research. Steve Frost (DST) therefore presented an outline of this project at their last research meeting at Drayton Manor on 18th August. By all accounts this was well received, and agreement was obtained for a small number of visits to theme parks to provide input to this project.

There is also a comprehensive reading list which includes a number of ride specific guidance notes in the Plant and Machinery series (see below). These guidance notes deal with structural integrity, passenger containment, general ergonomic principles and operating procedures. They do not cover the specification and design of the control system although many of them are capable of incorporating PES; these are indicated by an asterisk.

Table 1. HSE fairground ride guidance

Guidance notes in Plant & Machinery series	Reference
Safe operation of passenger carrying devices:	
* The waltzer	PM 47, ISBN 0118836080
* The octopus	PM 48, ISBN 0118836072
*The cyclone twist	PM 49, ISBN 0118835254
*The big wheel	PM 57, ISBN 011883536X
*The paratrooper	PM 59, ISBN 011883534X
*The chair-o-plane	PM 61, ISBN 011839284
*The rollercoaster	PM 68, ISBN 0118839284
The ark/speedways	PM 70, ISBN 0118854070
*The water chute	PM 71, ISBN 0118854151
The trabant	PM 71, ISBN 0118854240
Inflatable bouncing devices	PM 76, ISBN 0118856049
Passenger carrying aerial ropeways	PM 78, ISBN 0717607488

2.2 SRD's Assessment of Risks at Fairground Rides

This contract research report prepared for HSE [Holloway & Williams 1990], documents the results of a study which investigated the magnitude of risk to fairground workers and the general public. The risks quoted are based on a review of accidents over the period 1981-1986/87. These are then compared with risks posed by other similar activities. The main conclusion was that the risk to members of the public using fairground rides was low compared with those of similar activities for example "the risk of motoring to and from the fair is higher than the risk of riding when at it". The report shows that the risk of being killed or seriously injured whilst driving to the fair is seven times higher. There are several recommendations made however to ensure that risk is maintained ALARP, covering mainly maintenance and operational issues along the same lines as those made in the guidance described above [HSE 1997]. The accident data, risks and other useful statistics are reproduced in our earlier accident analysis progress report [Ioannides & Worsell 2000].

2.3 ASTM Standards

There are a number of American standards specific to the fairground industry produced by ASTM, the American Society for Testing and Materials. Those that we were able to identify are listed below.

- F 698 - 94 Physical information to be provided for amusement rides and devices
- F747 - 97 Terminology relating to amusement rides and devices
- F770 - 93 Operation procedures for amusement rides and devices
- F846 - 92 Testing performance of amusement rides and devices
- F853 - 93 Maintenance procedures for amusement rides and devices
- F893 - 87/95 Inspection of amusement rides and devices
- F1159 - 97 Design and manufacture of amusement rides and devices
- F1193 - 97 Amusement ride and device manufacturer quality assurance program
- F1305 - 94 Classification of amusement ride and device related injuries and illnesses

Whilst comprehensive in their coverage, none of these standards is more than two pages long, and many consist of a single page. They can therefore not be expected to contain much detail. Instead they are more akin to the Essential Health and Safety Requirements of the Machinery Directive (98/37/EC). Nevertheless it is worth knowing of their existence. There is a cursory reference to control systems in F1159-97.

2.4 AS 3533:1988 - Amusement Rides and Devices

There are very few countries who have standards for amusement rides. Apart from the American ones given above there is Australia's standard "Amusement rides and devices [AS 3533-1988]. We suspect that this standard will have a similar emphasis to the American ones. However it has not been possible to confirm this as loan copies of the standard are not available.

2.5 European Standard for Fairground Rides

A European standard "Fairground and amusement park machinery and structures - Safety, Part 1: Design and Manufacture" is in the process of being drafted [CEN 99]. The July 1999 draft provides useful information about the required functionality of the control system. There is no guidance on safety integrity levels for these functions although the phrase "function and integrity shall be determined by the risk assessment" crops up quite frequently. There is a section which gives an overview of risk assessment based on EN 1050 and 292. This does not provide details of how to carry out a risk assessment in practice but usefully extracts the hazards relevant to fairground rides from EN 292. This standard is not currently generally available, not yet having even a provisional reference number, and is subject to change. It is also unusual in that it is not linked to any specific Directive.

2.6 HSE's Video

In 1998 HSE produced the video "Thrills Not Spills", which is now available to the public. It illustrates how to design a safe passenger containment system from an ergonomics point of view. It covers the significant areas of the safe operation of amusement rides, but does not address issues such as operating procedures, design, safety-related system requirements and specifications.

2.7 HSE / FOD's Survey of the Use of PES in Fairground Rides

In 1996 a survey of fixed and travelling fairs was conducted by HSE / FOD to establish the extent of, and provide information on the safe use of, PES in fairground rides [Burstow 1996]. The inspectors involved found it very difficult to obtain any detailed information from the ride operators. However it was possible to confirm that the use of PES was widespread and growing and that control system failures were a problem that inspectors need to be aware of. Other recommendations made in the report referred to the need for information about the control system in the operating manual and the significant detrimental effect of voltage fluctuations on control system reliability.

3. CONTROL SYSTEM DESIGN STANDARDS

3.1 BS EN 954 Safety of Machinery - Safety Related Parts of Control Systems

This British/European standard has been available to designers of control systems for several years now. It has the status of an application standard (Type B1) under the Machinery Directive (originally 89/392/EEC now consolidated with all amending Directives as 98/37/EC). Part 2 of this standard "Validation", intended to take into account the requirements of IEC 61508, is not yet available, even as a draft. Before discussing this as a potentially useful reference, it is important to realise that "equipment for use in fairgrounds and/or amusement parks" is specifically excluded from the Machinery Directive. All standards, including BS EN 954, under this Directive therefore have no legal standing as far as fairground rides are concerned.

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 reliability (fault avoidance), structure i.e. diversity and redundancy (fault tolerance) and fault detection. 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 then it 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 which could swamp all other considerations (44% of accidents in a recent analysis of accidents by the HSE were attributed to errors in design²) 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;
- there is little guidance relating to the design of PES;
- and finally it is confusing to use.

An associated reference is the undated Electrical Contractor's Association guidance on the use of EN954-1 machine safety standard for safety-related parts of control systems. This helpfully describes the differences between categories.

² See section 4 of HSE 1995 "Out of Control", C50

3.2 IEC 61508: Functional safety of E/E/PE Safety-related Systems

This IEC³ standard uses the concept of the "safety life-cycle" as a framework for dealing systematically with the activities necessary for ensuring the functional safety of Electrical / Electronic / Programmable Electronic (E/E/PE) safety-related systems. The standard specifies requirements for the control and avoidance of faults in both hardware and software at all stages in this comprehensive life-cycle. The standard is therefore not so much a system design standard as a standard for the management of safety throughout the entire life of a system. It 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, 3, 4 and 5 are now published as international standards. The rest are at their final draft and expected to be published as international standards during 1999. Parts 1, 2, 3 and 4, with the exception of the annexes to part 1, are normative. Parts 5, 6, and 7 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 life-cycle 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 functional safety. This involves first correctly specifying what the safety function's task is and how it carries it out, i.e. good design is recognised as making an important contribution to safety. Secondly, it is necessary to ensure that for each safety function there is an adequate 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 reductions which the safety-related system is required to deliver, in its application. This means that [Redmill 1999] it is not valid to assume that, if the equipment and its control systems are built well and are reliable that they will be safe. They must be built to be safe and operated safely, and the safety functions designed to achieve safety should be based on an understanding of the risks posed by the equipment under control (EUC) and its control system.

³ International Electrotechnical Commission

Another important concept in IEC 61508 therefore is that of safety integrity levels (SILs). There are four of these 'SILs' numbered 1 to 4. Unlike BS EN 954: 1997 they are in a hierarchy in which 4 represents the highest level of integrity, i.e. the lowest probability of failure to perform its required safety function. This is highlighted by the fact that target failure rates (referred to as measures) are assigned to each SIL both in terms of probability of failure on demand and probability of failure per hour i.e. when operating continuously. These values are reproduced in the table below. In the standard they are accompanied by numerous notes (Part 1, page 33) which should be referred to if planning to make use of them.

Table 2. Target SIL failure rates

SIL	Probability of failure per hour	Probability of failure on demand
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

Once the designer has selected the appropriate SIL, IEC 61508 contains all the necessary information to enable this level of integrity to be achieved. It is important to realise that although the standard gives guidance on good practice and makes recommendations it does not absolve its users from responsibility for safety [Redmill 1999]. It is also important to realise that it is not possible to retrospectively prove a particular safety integrity level.

It is a requirement of the standard to carry out hazard and risk assessment but it is left to the user to determine how to do this. Part 5 of the standard provides some information on how to select a SIL based on risk and includes examples of various risk estimation techniques.

It is important to remember that IEC 61508 is designed as a generic standard. Although it is possible to be used directly it is more likely to be used as a basis for writing sector or application specific standards. These will then be able to provide clearer guidance on the risk assessment phase of the safety life-cycle and take into account the fact that what may be tolerable in one industry section may not be tolerable in another. 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 to use, and seen to be bureaucratic, however sector specific standards are expected to overcome this.

Rather than go into any further detail the authors will instead mention a number of papers some published and others internal to HSE on the subject of IEC 61508.

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

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

Another paper presented at the Hazards XIII conference "A case history of the application of draft international standards IEC 1508 to the needs of the process industries" [Tuff and Beale 1997], also gives an overview of the contents but in addition describes the 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 and Reinert 1992] published in Safety Science 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] presented at the HSE PES seminar 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 although safety-related application. The application was the development of software used as a decision aid in land-use planning in the vicinity of major hazards.

Finally there is "IEC 61508 - an influential standard" [Redmill 99] which gives a good overview of the standard's aims and objectives and goes into some detail about management issues.

3.3 DIN V 19 250 Control Technology Standard

The [DIN V 19 250, 1994] standard with the full title "Control Technology: Fundamental safety aspects to be considered for measurement on control equipment" 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.

3.4 DEF STAN 00-56/Issue 2: 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) taking into account international standardisation activities and supporting research and development. This standard comes in two parts, part 1 [DEF STAN 00-56/Issue 1:1996] describes the requirements for safety management, including hazard analysis and safety assessment and part 2 [DEF STAN 00-56/Issue 2: 1996] 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).

Table 3. SIL selection matrix

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 61508 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 changes dramatically. Nonetheless, it is an interesting way of classifying SILs.

3.5 ANSI/ISA standard S84.01-1996

We have not been able to obtain of a copy of this ANSI/ISA (American National Standards Institute / Instrument Society of America) standard however it is described in the paper “Are your instrumented safety systems up to standard?” [Ford and Summers 1998]. The standard is described as being of particular importance because it is considered by the USA Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) as "accepted industry practice". The paper goes on to explain that the standard has placed new requirements on the design, selection, installation, operation and maintenance of instrumented safety systems. A safety system is considered to include everything from the input sensors to the output actuators and any interfaces.

The standard seems to be very similar to IEC 61508, using the same concepts of the safety life-cycle and SILs but there only appear to be three of these. Also like IEC 61508, in fact probably more so, the standard does not cover SIL selection which as the authors of the paper say "must be carefully performed and thoroughly documented". The standard instead concentrates on how to ensure that the selected SIL is achieved.

Table 4. SIL definition

SIL	Probability of failure on demand	Availability
1	0.01 - 0.1	90 - 99 %
2	0.001 - 0.01	99 - 99.9 %
3	0.0001 - 0.001	99.9 - 99.99 %

The paper itself didn't go into any detail about how to select SILs as its purpose was only to give background information about the issue. However it did usefully reference another more detailed paper [Summers 1997] which the author kindly sent us. This is described in section 6 later in this report.

4. CONTROL SYSTEM DESIGN GUIDANCE

4.1 The HSE PES Guide

This is HSE's guidance on "Programmable Electronic Systems in safety related applications" but is generally simply referred to as "The PES guide". It is included in the reading list of HS(G)175 as a standard for the design of programmable control systems. The PES guide comes in two parts. The first part 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 was published in 1987 and has been used for many years by a wide range of industries including the fairground industry. For some time it was the only available detailed guidance. However it does not give industry specific guidance on how to determine the required safety levels for each safety function. Furthermore the scope was limited to PES applications only and did not include electronic or electrical based control systems. 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 [Frost 1998].

4.2 IGE's Programmable Equipment in Safety Related Applications

When HSE's PES guide was published, industry was encouraged to publish application specific guidance. In response the Institution of Gas Engineers (IGE) published the Safety Recommendations IGE/SR/15: 1994 "Programmable Equipment in Safety Related Applications" aimed at the gas industry. This guidance is an update of an earlier version called "Use of Programmable Electronic Systems in Safety Related Applications in the Gas Industry" which was published in 1989 and written to take into account current developments of formal methods and tools for validating the integrity of software. The third edition written to harmonise the recommendations with IEC 61508 has now been published [IGE 1999].

The main purpose of this document is to provide guidance on the design principles and implementation of control and safety systems in the gas supply industry. The original document was based on the content of HSE's PES guide. However the 1999 publication essentially provides an industry route map of IEC 61508.

IGE recognise that "programmable electronics has penetrated every aspect of the gas industry" and that "control systems perform both functional and safety operations and the boundary between the two has become indistinct". In the introduction to the recommendations care is taken to define the term safety-related as "any control or safety function wherein failure or failures could lead to death, injury or environmental damage". Furthermore it is pointed out that an application cannot be considered to be non-safety-related merely by the fact that it is equipped with alternative means of protection and that a formal safety integrity assessment will still be required. A flowchart is given in figure 1 of this guidance to show the process that needs to be followed in order to demonstrate that the system is acceptable. It is expected that a hazard analysis to identify hazards along with any separate study of the control and safety systems indicated to be necessary by this analysis will already have been carried out. Another publication in the same series, Safety Recommendations IGE/SR/24, goes into some detail about risk assessment techniques and is described later in section 5.

Two methods are described for "establishing safety integrity levels (SILs). The first is based on quantifying an acceptable annual frequency of a fatality then estimating the percentage of the failures of the type being studied that could lead to a fatality. If the actual failure rate is known then a target probability of failure for the protective system can be calculated which will then lead directly to the SIL by using the tables relating SIL to failure probabilities on demand. The second method is very industry specific and is a lookup table where the user selects appropriate categories for consequence and cause of risk, which give the user numbers for three variables a, b and d which are combined according to the equation: $SIL = a-b-d-1$.

The rest of the document is then devoted to how the SIL can be achieved.

4.3 EEMUA's Safety Related Instrument Systems for the Process Industries

The [EEMUA 1989] publication, produced by a subcommittee of the EEMUA (Engineering Equipment and Manufacturers and Users Association) is intended to be the application specific guidance for the process industries and has also been produced in accordance with HSE's invitation in the PES guide, part 2. 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 table 1 of this publication. 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 a category 1 system.

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.

4.4 Out of Control

This guidance [HSE 1995/1] is aimed particularly at all 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% of the incidents 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 life-cycle model as used in IEC 61508.

4.5 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 Centre for Chemical Process Safety of the American Institute of Chemical Engineers (CCPS/AIChE) recognised the potential of this technology to increase the potential for 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. Although not of direct relevance to the fairground industry it is interesting in so far as 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 (figure 3), which takes into account the number of independent layers of protection against the hazard in question, the likelihood of the hazardous event and the consequences is described in chapter 2 and reproduced below. Examples of its use are given in chapter 7.

This reference therefore may prove useful when developing a similar technique for the selection of SILs in the fairground industry. It is also worth noting that appendix G contains a list of potential PES failure modes.

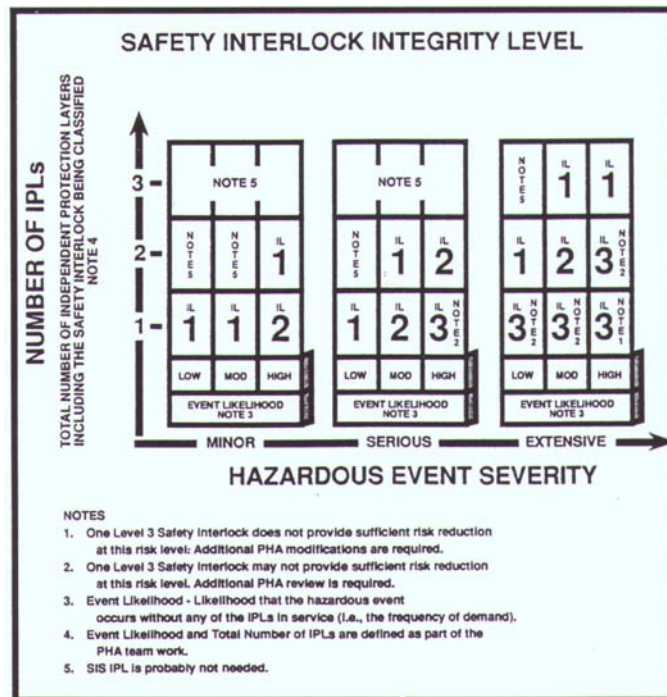


Figure 3 - Linkage of process risk to SIS integrity classification

© Copyright (1992) American Institute of Chemical Engineers. Figure 2.6 of "Guidelines for Safe Automation of Chemical Processes" reproduced by permission of Center for Chemical Process Safety of AIChE

4.6 Guidance on HAZOP Procedures for Computer-Controlled Plants

This is the title of an HSE contract research report [HSE 1991] produced by KBC Process Technology Ltd. As with [CCPS 1993] it is aimed at the chemical process industry. The HAZOP methodology could equally be applied to fairground PE 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 of 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 the fairground industry. A number of interesting comments were made during an industry survey, some of which are applicable to the fairground industry. These are described in appendices one and two.

4.7 MISRA Reports

MISRA's "Development Guidelines for Vehicle Based Software" [MISRA 1994] follow a similar approach to IEC 61508, in that they make use of the concepts of the safety life-cycle, and integrity levels etc. They are strongly aimed at the Motor Industry, only considering issues relevant to this industry. The Motor industry is another 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 also equally important in the motor as in the fairground industry in that 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 (discussed separately in section 4.8) aimed at Transport Telematic Systems. The main concept behind the MISRA guidelines for SIL selection is the introduction of the term 'controllability'. Between a failure and an accident there is a loss of control, and it is this loss of control of the safety of the situation that is categorised. Each hazard is assessed for the degree of control that remains after a failure has occurred and one of the controllability categories listed in the table below is selected. This then defines the SIL required with the appropriate acceptable failure rate. There is a deviation from IEC61508 by the reference to a SIL of 0.

Table 5. Assignment of SILs according to controllability categories

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

Reproduced with kind permission from Motor Industry Research Association

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 a fairground ride can be likened to a motor vehicle driven by the ride operator, so many of the factors can be related to a fairground ride. This would therefore seem to be a simple way of selecting SILs. However, it is unlikely that there would be many situations that didn't fall into the top category.

A later report simply called "Report 2 - Integrity" [MISRA 1995] builds on the report discussed above and incorporates much of the material presented in the reports discussed in section 4.8, for example the concept of confidence levels. This is not surprising as at least one of the authors of the DRIVE project report (Peter Jesty) is acknowledged as a contributor to this one. 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.

The report goes into further detail, describing three possible ways of selecting appropriate SILs.

-The Pragmatic approach. This approach requires less effort than the other approaches but relies on a rigidly defined classification scheme which may be difficult to apply to novel applications. Integrity levels are selected qualitatively by associating each level with a given severity as follows:

Integrity level 4 - represents the integrity level required to avoid disastrous accidents. However, what is meant by disastrous is not defined.

Integrity level 3 - represents the integrity required to avoid serious incidents involving a number of fatalities and/or serious injuries.

Integrity level 2 - represents the integrity to avoid more serious, but limited, incidents some of which may result in serious injury or death to one or more persons.

Integrity level 1 - represents the integrity required to avoid relatively minor incidents and is likely to be satisfied by a certain degree of fault tolerant design using guidelines which follow good practice.

Integrity level 0 - represents the integrity associated with no risk to persons and in effect represents the "don't care" condition.

-The Controllability approach. In appendix B, a detailed description is given on the controllability approach for determining the integrity level as explained earlier.

-The Standards based or systematic approach. In appendix A, a good explanation is given of integrity level determination through quantitative generic risk assessment as already described in IEC61508, DEF STAN 00-56 and DIN V19250 standards.

There are several publications by MISRA relevant to the design of PES safety-related control systems in line with IEC61508. Only those two described above are helpful to this project but the others 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 multiplexing, onboard 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. From this web page we also learnt that MISRA has recently started work to produce guidelines on Preliminary Safety Analysis for the Motor industry. This will include further advice on safety integrity levels.

4.8 Safety Aspects of Advanced Transport Telematic Systems

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

The first report of interest from the DRIVE (Dedicated Road Infrastructure for Vehicle Safety) II programme - "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 a balance must therefore 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. It therefore seems particularly relevant to fairground rides as public safety is of prime importance. 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 IEC61508 although the terminology "confidence level" is not used as something distinct from the SIL.

The second report of interest under the DRIVE II programme "Framework for Prospective System Safety Analysis", [Hobley et al 1995] documents the results of the project referred to as PASSPORT II (Promotion and Assessment of System Safety and Procurement of Operable and Reliable Road Transport Telematics). This report consists of two volumes. Volume 1 - "Preliminary Safety Analysis" 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 described in Volume 2 - "Detailed safety analysis" 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 [Astruc et al 1995], which aims to ensure that the system is safely and correctly implemented. This report is not directly relevant but is interesting in that it describes one of the goals of the PASSPORT project as being to provide a framework for the retrospective system safety evaluation of ATT systems.

In addition Mr. Jesty provided some useful Internet web addresses. In particular the following www.trentel.org./index.htm from which the "Co-Ordinated Dissemination in Europe of Transport Telematics (CODE TR) System Safety Guidelines" [Jesty, Giezen and Fowkes

1998] has been downloaded. This is quite a large document which comprehensively summarises the contents of the other reports, the developments and background to the DRIVE programme 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 Motor 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 which would be interpreted in this context as that the risk imposed from any failure of a safety-related system should be reduced to as low as reasonably practicable. However as this is one of the few industry sectors which has come up with a practical methodology for selection of SILs it bears looking into in more detail. Figure 4 at the end of this report shows the controllability category model taken from the DRIVE report.

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. "Integrity Levels and their Application to Road Transport Systems", [Jesty and Hopley 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. The one of most relevance being "As safe as necessary" [Jesty 1997]. This paper 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.

4.9 The Use of Computers in Safety-Critical Applications

This is the title given to the final report [HSE 1998] of the study group on the safety of operational computer systems set up by the Advisory Committee on the Safety of Nuclear Installations (ACSNI). It was published by HSC in October of 1998.

The terms of reference for the study group were:

- to review the current and potential uses of computer systems in safety-critical applications;
- to consider the implications for the nuclear industry;
- in this context, to consider developments in the design and safety assessment of such computer-based systems, including other aspects of control systems; and to advise ASCNI where further research is necessary.

The document therefore discusses in some depth the various issues surrounding the design and use of computers (including PES) in safety-critical applications and how to ensure the highest integrity of these systems, and furthermore how to demonstrate this, for example in safety-cases.

Reference is made to integrity levels by relating them to Mean Times Between Failures (MTBF), illustrated by the graphical representation reproduced below.

This has been used to plot MTBF of pre-existing software in safety-critical applications as implemented in the nuclear, chemical and aerospace industries and thus compare them with safety integrity levels given in IEC 61508. As can be seen there was only one circumstance in which the MTBF was high enough to achieve that expected from a system designed to SIL2. Worse, almost half had a MTBF below that expected from a system designed to SIL1. However, it must be noted that account was only taken of the software contribution to the SIL without taking into account any other protective measures.

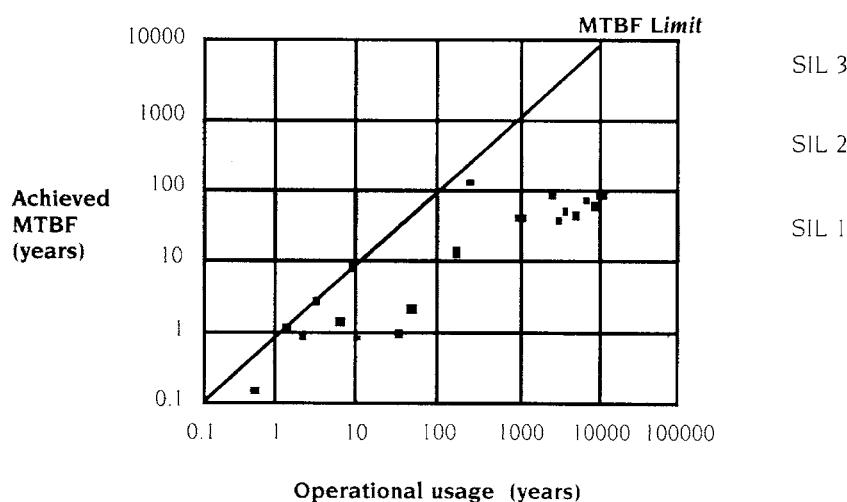


Figure 5. Plot of Mean time Between Failure against Operational usage in years

Risk is taken into account in a fairly limited way in appendix A which gives an insight into how safety-cases are evaluated. This is done by categorising systems as follows:

- Cat 1 - any structure, system or component which forms a principle means of ensuring nuclear safety;
- Cat 2 - any structure, system or component which makes a significant contribution to nuclear safety;
- Cat 3 - any other structure, system or component.

There is unfortunately no guidance about how to select appropriate SILs. The implication however seems to be that the highest integrity possible needs to be achieved.

4.10 Proceedings of 7th Safety-Critical Systems Symposium

This contains papers presented at the symposium “Towards System Safety” organised by the safety-critical systems club. The purpose of the symposiums, held annually, are, to quote from the preface of the proceedings: “to bring together practitioners and researchers in a quest to inculcate a higher degree of safety engineering into the development and operation of critical software-based systems”. The purpose of the seventh symposium was to explore recent work and experience which leads further towards system safety. Described below are those papers of relevance to the project.

“Design for Safety” [Storey 1999]

This paper was of background interest as it describes the design process as being made up of:

- abstraction - generalising the problem, identifying the essentials of the solution
- decomposition - breaking the problem and solutions down into simpler smaller parts
- elaboration - the detailed design
- decision making - identification of and selection between alternative strategies.

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

These concepts and techniques are then described in some detail.

“Safety Integrity Levels: An Industrial Viewpoint” [Hamilton and Rees 1999]

This paper looks in some detail at how the concept of safety integrity levels (SILs) are used in various different standards and industrial guidance drawn from these standards. The documents discussed are IEC 61508, DO-178B, Def-Stan 00-56 and Mil-Std 882C. After discussing the different approaches taken by these documents the paper comes to the following conclusions:

- each standard has a subtly different philosophy behind the assignment and use of SILs;
- there is no clear consensus about what SILs actually mean or how they should be used;
- without first revising standards to some common framework, there can never be any simply, generally applicable mapping between the SILs of the different standards.

“Independent Verification Magic or Myth?” [Nolan 1999]

This paper goes into some detail about testing of software in order to explain why the use of independent verification can be flawed. The paper then moves on to demonstrate why software testing needs to be conducted by the developer with the role of the independent verifier being that of verifying the results of the developer’s tests. Various other important points are made among which are the following:

- one should decide how to test a system at the beginning of the design process not at the end;
- only developers can ensure that the system is designed for testability;
- the person testing a system must have a thorough understanding of it;
- one must have a specification of the system against which to test it.

4.11 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 need 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.

5. HAZARD IDENTIFICATION AND RISK ASSESSMENT

5.1 HSE/HSC Guidance on Risk Assessment

There are various HSE documents some internal, others published which explain HSE's approach to controlling risk. Probably the most well known and frequently mentioned is "The Tolerability of Risk from Nuclear Power Stations" often simply referred to as "TOR". This was first published in 1988 and revised in 1992 [HSE 1992]. 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 which gives some numerical criteria it has been used as a basis particularly for quantitative risk assessment in many other industries. Many of the issues discussed can equally be applied to the fairground industry, particularly the importance of public perception.

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 publication "Quantified Risk Assessment: Its input to decision making", [HSE 1993] develops some of the issues raised in the original TOR document. The use of QRA is unlikely to be appropriate (and would in any case be very difficult) when considering risks associated with the safety-related parts of fairground control systems. However this document does contain some relevant material. For example it includes 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 is HSE's "Risk criteria for land-use planning in the vicinity of major hazards" [HSE 1989] which 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 and Pape 1989]). It also 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 "Principles and guidelines to assist HSE in its judgements that risk has been reduced 'as low as is reasonably practicable (ALARP)" [RAPU 1995]. Following on from this is the recently published discussion 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, like societal risks through FN-curves etc.. Also, various estimated values are given for the risk of death or

serious injury from various activities, industrial and leisure, including fairground rides. These are risk of death of 1 in 250 million rides and risk of serious injury of 1 in 17 million rides over the period 1981-88 and are based on the data given in the SRD report [Holloway & Williams 1990].

The Advisory Committee on Dangerous Substances (ACDS) report on "Major Hazard aspects of the transport of dangerous substances" [ACDS 1991] was published by HSC. It gives a comprehensive description and discussion of a complex and resource demanding Quantified Risk Assessment methodology (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 of 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) [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".

5.2 SRD's Review of Hazard Identification Techniques

This report [Parry 1986] by SRD (Safety and Reliability Directorate) 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 in 1986 for identifying hazards associated with the processing, storage and handling of dangerous substances. These were HAZOP, Check-lists, 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 fairground rides, including HAZOP with similar guide-words but different parameters.

5.3 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. The guidelines then go on to discuss some important issues that need to be born 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 which is considered to be tolerable/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. The guidelines also recognise the important role that software plays and states that "the use of computers or 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.

IEE's undated "Professional Brief on Safety-related Systems" builds upon these guidelines and includes the concept of the safety life-cycle, but not that of 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.

The Hazards Forum has also published guidance [Hazards Forum 1995] very much along the same lines giving an overview of all relevant legislation and guidance.

5.4 Loss Prevention in the Process Industry

"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 latest edition (second) published in 1996 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 and 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 already discussed in section 3 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. It is rather surprising that IEC 61508 is not mentioned by name as most parts were available as provisional standards some years before the second edition was published. However, the revision was drafted some years before publications. The only reference is to IEC SC65A WG9:1991 "Software for computers in the application of industrial safety-related systems" listed as a safety standard, which we believe is the same working group that produced IEC 61508.

The section on risk criteria draws its material from the HSE publications discussed above and the book "Acceptable Risk" by Fischhoff discussed below.

5.5 Geoff Wells' Hazard Identification and Risk Assessment

This book [Wells 1996], published by IChemE gives a through 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 has been done by the Risk Assessment Section of HSL for the machinery sector. 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 target values are given for maximum risk not to be exceeded. These figures indicate a maximum tolerable risk level of 10^{-5} to 10^{-6} for members of the public which is the lower half of the ALARP region in TOR. The book is illustrated throughout by case studies and generalised failure rates are given for various processes and subsystems including human reliability which can be used in any QRA.

5.6 Fischhoff's Acceptable Risk

The most well known reference which deals almost exclusively with the subject of risk criteria is "Acceptable Risk" [Fischhoff 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 we now say in HSE 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 acceptable-risk based decisions are offered in the areas of policy, practice and research. A very generic overview is given of 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.

5.7 Ball and Floyd report for HSE on Societal Risk

The [Ball and Floyd 1998] report, 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. It 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/CHID7. However a better reference for this is Risk Assessment Section's internal report "A study into the use of the approximate risk integral as a representation of societal risk in Toxic RISKAT" [Macbeth 1998] which includes various examples of its use.

5.8 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 French version was given to me by Alfred Sutter of SUVA, one of the co-ordinators of the project. The comprehensive Summary and Conclusions have been translated into English (Ref 16110/9900 20002).

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 insofar 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.

5.9 ISO/IEC Guide 51

This is the second edition 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."

5.10 Towards safer industrial computer controlled systems

There are two papers [Chambers et al 1997] with this title, one of which has been submitted to 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.

5.11 IGE's Risk Assessment Techniques

This document published by the Institute of Gas Engineers (IGE) gives clear up to date guidance (it was published in 1999) on the process of risk assessment based on HSE's five steps [HSE 1995/2]. 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 likelihood's - 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 writing something out 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 HSE's TOR framework. 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. This is an interesting and tricky concept where fairground rides are concerned. No-one can suggest that the industry forces anyone to participate and the participant does obviously at least anticipate some benefit in terms of enjoyment otherwise one would assume that they wouldn't have parted with their money in the first place. However this situation differs significantly from the usual industrial case. Firstly voluntary versus involuntary would normally differentiate employees from members of the public, on whose behalf it is politically correct to tolerate lower levels of risk. Secondly the benefit to the person voluntarily exposed to the risk is generally assumed to be monetary, whereas in the case of fairground rides the money changes hands in the opposite direction. Thirdly does an employee have more knowledge about the risk or its existence? Finally those exposed to risk are generally children, to which it is politically correct to tolerate only the lowest levels of risk.

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.

5.12 Probability Risk Assessment of Engineering Systems

The [Stewart and Melchers 1997] book, 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 are also discussions of uncertainty, risk criteria, communication and perception. The book also contains some failure rate and human reliability data.

5.13 Plant Functional Modelling Hazard identification

This paper [Rasmussen and Whetton 1997] describes a technique developed as part of the EU TOMHID project which enables a process plant to be modelled as a socio-technical system. This is achieved by the process of top-down functional decomposition of the plant into intents which are made up of methods and constraints, and can have inputs and outputs. Each method and constraint forms the intents on the next layer in the system. Once the process has been modelled in this way either a CHA type analysis can be carried out by applying the keywords to on each intent or a 'What-If?' analysis based on the failure to satisfy each intent, method or constraint can be performed. The great advantage of this technique over HAZOP and FMEA is that a comprehensive hazard identification can be conducted before the detailed design is available.

5.14 Qualitative Techniques for Risk Estimation/Ranking

There are various qualitative techniques found in the literature which may usefully be applied to the problem of selecting the appropriate SIL for safety-related functions of fairground rides. They have all been reviewed in an earlier project report on machinery risk assessment [Worsell and Wilday 1995], however for completeness they are briefly described below:

- *BS 5304 Nomogram*. This technique is contained within "BS 5304:1988, the British Standard Code of Practice for Safety of Machinery" [BS 5304: 1988] prepared under the direction of the Machinery and Components Standards Committee. The bulk of the standard is concerned with describing various hazards arising from the use of machinery, methods for their elimination or reduction, safeguarding of machinery and the use of safe working practices.
- *Rafaat's Risk Calculator*. The risk calculator [Raafat 1995] was developed by Hani Raafat to provide a tool for the rapid screening of risks in order to focus attention on risk levels which are intolerable. Its main objective is "the ranking of risks rather than providing criteria for risk tolerability". One of the main characteristics of this technique is, that unlike many others, it explicitly takes into account the frequency and duration of exposure to a hazard.

- *Machinery Directive Practical guide Risk Nomograph*. This technique [Engelenburg, Hoogerkamp and Hopmans 1995] has been developed specifically for machinery risk assessment during design in order to satisfy the requirements of the machinery directive and related standards. Risk is therefore defined in accordance with EN1050.
- *Machinery Directive Practical Guide Risk Graph*. This technique [Engelenburg, Hoogerkamp and Hopmans 1995] has also been developed for machinery risk assessment and is based on the same principles as above. It could also be used taking into account existing or proposed safeguards.
- *Bell and Reinert (IEC 61508) Risk Graph*. This is the technique given in [IEC 61508: 1997] and is therefore of particular relevance to this project. The risk graph, expresses the risk diagrammatically. It calls for the subjective evaluation (supported by whatever objective evidence is available) of a number of relevant factors, and then combines them using a graphical algorithm to indicate the required SIL value.
- *BSEN 954-1 Risk Graph*. The form of the risk graph in [EN 954-1:1997] is strikingly similar to that in the Master's technique, see below, but sufficiently different to warrant separate treatment. This technique differs from others in the way that the user is invited to select the severity category in terms of the 'usual' consequences rather than 'worst' consequences. This is the only technique which gives any guidance for the selection of the exposure category. There is guidance in addition to that given in other techniques for the selection of the avoidance category.
- *Master's Risk Graph*. This technique [Masters 1996] seems to be more about justifying not using certain types of safeguard than ranking or estimating risk: the only definite information being which safeguards would be considered as unnecessarily expensive (over-dimensioned) for the hazard in question. Even though two are *preferred*, or maybe only one, all the other types of safeguard associated with lower risk are *possible*.

5.15 ELVIK ON COST-BENEFIT ANALYSIS (CBA)

This recent paper [Elvik 99] 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 can not 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, Weber and Locher 1994] 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	(33xslight, 4.4xserious, 1.2xcritical)
Injury Critical	13, 370, 000	
Serious	3, 780, 000	
Slight	500, 000	

6. TECHNIQUES FOR SIL SELECTION

6.1 Techniques Recommended by Summers

Six techniques for assigning target safety integrity levels to safety functions, are described in some detail in the paper "Techniques for assigning a target safety integrity level" [Summers 1997]. The purpose of these techniques is to allow the selection of a SIL to be based on "the amount of risk reduction that is necessary to mitigate the risk associated with the process to an acceptable level". The paper also highlights the fact that there are as yet no regulations or standards that assign or assist in the assignment of a SIL to particular processes, hazards or chemical operations. It further points out that assignment of SIL has to be therefore "a corporate or company decision based on risk management and risk tolerance philosophy."

The simplest and most conservative technique is a qualitative selection of a SIL based on a consideration of consequences only, i.e. there is no consideration of likelihood so for example all situations with the potential to cause fatalities would require SIL 3 no matter how remote or likely. It is often very difficult to make any realistic estimate of likelihoods so this

technique may be more appropriate than it initially appears. This "**Consequence Only Technique**" is readily represented by the table below.

Table 6. Allocation of SIL according to consequence

SIL	Consequence
4	Potential for fatalities in the community (members of the public)
3	Potential for multiple fatalities (employees only)
2	Potential for major serious injuries or one fatality
1	Potential for minor injuries

Note that no definition is given for the terms major and minor and the paper itself says that these definitions remain open for discussion.

Another approach being adopted by many small, speciality chemical plants that do not wish to devote extensive manpower to SIL selection has been referred to as the "**Corporate Mandated SIL**". This is where a company makes the decision that all safety systems will be designed to the same SIL - usually SIL 3. The resources needed for the time-consuming discussions about which SIL is appropriate, what the consequences are and how likely an event is can be redirected into ensuring high quality design and validation. Unfortunately there is the danger that one of the most useful benefits of risk assessment is lost, namely a good understanding of the hazard potential and what can go wrong.

However perhaps the technique which finds the most favour across a wide range of industries is the "**Risk Matrix**". A recent HSL/RAS review identified ten published risk matrix type techniques [Worsell and Wilday 1997]. This technique is essentially an extension of the "Consequence Only Technique" to allow the selection of the SIL to be adjusted to take into account the likelihood of the hazardous event. However the matrix given in the paper does not correspond exactly with the consequence only table. The general principle can however be seen as the SIL needs to be increased by 1 if the likelihood is considered to be high and decreased by 1 if the likelihood is low. Again there are no definitions for 'Low', 'Medium' and 'High', the three expressions of likelihood.

In using the risk matrix when assessing the incident severity and likelihood it is necessary to take into account the effects of the available layers of protection. The paper points out that "for risk reduction consideration, the layers of protection must be independent, verifiable, dependable, and designed for the specific risk." If there is the need to formally consider the independent layers of protection (IPL) then a three dimensional risk graph can be used. The third dimension being an IPL of low, medium and high. An example is given in the paper.

The paper also describes as a technique the "**Risk Graph**" from IEC61508. However it extends the guidance by listing various questions to consider when selected each of the four parameters. However these are aimed primarily at the chemical process industry.

It is already a requirement by OSHA that "a process hazard analysis be used to determine the protective measures necessary to protect workers, the community and the environment." HAZOP is a widely used technique in the chemical process industry for the identification of potential hazards. It is therefore an obvious candidate for modification to incorporate SIL

selection taking advantage of the fact that the people with the appropriate knowledge and experience are already gathered together. This is then referred to as the "**Modified HAZOP**" technique. Once the requirement for a safety instrumented system has been identified then a SIL should be qualitatively assigned based on the team's in-depth knowledge of the process operation, process risk and company risk tolerance policy. In essence the team selects a SIL that they feel is appropriate according to their estimation of the risk. Summers then makes the important point that "since the assignment is very subjective, there needs to be some consistency between personnel on the SIL assignment teams from project to project." The obvious question that springs to mind is - how does one ensure consistency across industry?

Finally there is always the quantitative approach. "**Quantitative Analysis**" as it is referred to is the most rigorous and consequently also the most time-consuming. The SIL is assigned by determining the process demand or incident likelihood quantitatively by modelling the incident causes using standard QRA techniques such as fault-tree-analysis. An appropriate SIL is then selected by dividing the risk frequency considered to be tolerable by the calculated frequency of demand on the safety function. This then gives the tolerable probability of failure on demand and hence the SIL. This method, where only demand is estimated, is also described in IGE's risk assessment guidance [IGE 1999]. Summers recommends the use of this technique in cases where there is very limited historical information such that a qualitative estimate of the likelihood is very difficult. It would therefore seem particularly appropriate for the use of novel control systems in the fairground industry. However this technique requires a thorough understanding of how systems can fail and probabilities or frequencies for base events which are very hard to determine or estimate. The time required to use this technique effectively is probably also prohibitive, unless a generic fault-tree with tables of suggested values can be provided along similar lines to that done for machinery in [Worsell and Wilday 1997].

6.2 Techniques Described in Draft Standard IEC 61511

This draft international standard "Functional Safety of Safety Instrumented Systems for the Process Industry Sector" addresses the application of safety instrumented systems (i.e. sensors, logic solvers and final elements) in the process industries. It is the process industry specific standard for IEC 61508 and is in a fairly early stage of development. We have obtained copies of parts 2, 3 and 4 of the 1998 draft. Part 2 - "Guidelines in the application of part 1" contains design guidelines. Part 3 - "Guidelines in the application of hazard & risk analysis" provides information on the underlying concepts of risk, the relationship with safety integrity and various methods to enable SILs to be selected. These methods are described below. Part 4 - "Overview of techniques and measures" consists only of annexes which do just that and includes descriptions of such techniques as FMEA/FMECA, fault tree, event tree and cause-consequence analysis under the general heading of failure analysis.

Annex A of Part 3 gives a useful overview of risk and safety integrity. This is followed up by Annex B which describes in some detail ALARP and tolerable risk concepts. Annex C describes how SILs can be defined quantitatively and is sufficiently similar to those described earlier not to go into any detail here except to mention that it is usefully illustrated with an example. Annex D is much more interesting as it proposes the use of the risk graph in IEC 61508 calibrated for use in the process industry sector. Alternative descriptions, as shown in the table below, are given for the risk graph parameters felt to be more appropriate to the

process industry. There is also guidance on the selection of the values for each parameter with the caution that those responsible for safety must ensure that they are suitable for use within the context of the project under consideration.

Table 7. Guidance for selection of risk graph parameters

Risk Parameter	Classification	Comments
<p><u>Consequence (C)</u> Average number of fatalities, calculated by determining the average numbers present when the area exposed to the hazard is occupied multiplying by the vulnerability to the hazardous event. Where the vulnerability V is 0.01 for small releases 0.1 for large releases 0.5 for large releases with high prob. of fire 1 for a rupture or explosion.</p>	<p>C_A Minor injury C_B Range 0.01 to 0.1 C_C Range >0.1 to 1.0 C_D Range >1.0 to 10</p>	<p>1. The classification system has been developed to deal with injury and death to people. 2. For the interpretation of C_A, C_B, C_C and C_D, the consequences of the accident and normal healing shall be taken into account. 3. Greater than 10 use quantified approach.</p>
<p><u>Occupancy (F)</u> This is calculated by determining the length of time the area exposed to the hazard is occupied during a normal working period. Note - If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected.</p>	<p>F_A Rare to more often exposure in the hazardous zone. Occupancy less than 0.1 F_B Frequent to permanent exposure in the hazardous zone</p>	<p>4. See comment 1 above. Note - It is only appropriate to use F_A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up.</p>
<p><u>Probability of avoiding the hazard (P)</u> if the protection system fails to operate.</p>	<p>P_A Assumed to be 0.9 if all conditions in column 4 are satisfied P_B Assumed to be zero if all the conditions are not satisfied</p>	<p>5. P_A should only be selected if all the following are true:</p> <ul style="list-style-type: none"> • facilities are provided to alert the operator that the SIS has failed. • independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area • the time between the operator being alerted and a hazardous event occurring exceeds 1 hour.
<p><u>Demand Rate (W)</u> given no protection system To determine demand rate it is necessary to consider all sources of failure that will lead to a demand on the SIS. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61508, is limited to below the performance ranges associated with SIL1. For simple applications it will be sufficient to sum the demand frequencies. For more complex systems it may be necessary to construct fault trees.</p>		<p>6. The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS. Credit can be taken for relief valves provided that these are fully sized for the expected duty. 7. If little or no experience of the process or the control system, or of a similar process or control system the estimation of the W factor may be made by calculation. In such an event a worst case prediction shall be made.</p>

Another risk graph has also been proposed in this draft of 61511 to determine the integrity level requirements where the consequences of failure include acute environmental loss. In this case the integrity level needed will depend on the characteristics of the substance released

and the sensitivity of the environment. An alternative description is therefore given for the consequence parameters. The risk graph is also modified as in terms of environmental release the exposure category does not apply and has therefore been removed. The other parameters P and W do apply and definitions can be identical to those applied above to safety consequences.

Annex E describes another technique “the safety layer matrix method” which relates the required SIL to the severity of the hazardous event, its likelihood and the number of independent protective layers (IPLs) which provide protection against the hazardous event using other technology. This technique is identical to the one described in [CCPS 1993].

Annex F develops the idea of IPLs further and describes the technique “Layer of Protection Analysis - LOPA”. This technique provides a list of IPLs commonly used in the process industry and requires the probability of failure on demand to be estimated for each of them. Any resulting gap in the risk reduction required to meet the risk criteria defines the SIL of the safety control system provided.

7. DISCUSSION

Guidance for the effective operation, control, design specification and implementation of an amusement ride is readily available in some form. Although very little information is aimed directly at the fairground industry, a comprehensive literature review identified the [HSE 1997] guide described in section 3.1 and the [HSE Video 1998]. Moreover the only standards aimed specifically at the fairground industry are American, section 1.3, and Australian [AS 3533-1988]. We believe that a European one is currently being drafted. However, the information contained within these references relate to structural integrity, operating procedures and passenger containment rather than control system design.

A comprehensive literature review has confirmed that there is a lack of specific guidance to enable those involved with the implementation, use and maintenance of safety-related programmable fairground ride control systems to select the appropriate measures and techniques so that an adequate level of safety integrity is achieved and maintained. Instead the fairground industry has to rely on generic guidance such as [HSE 1987] PES guide and [IEC 1997]. This situation is not really satisfactory considering the increasing use of PES in fairground rides demonstrated by Burstow's survey [Burstow 1996] and the important contribution to serious accidents indicated in our accident analysis [Ioannides and Worsell 2000]. This lack of guidance also makes it very difficult for inspection, certification and regulatory bodies to determine whether measures and techniques taken by designers are adequate in relation to any particular application.

There are numerous texts and standards that deal with hazard identification and risk assessment issues a summary of which is given in section 5. Most have their foundations in the Chemical Process and Nuclear industries, although many can be applied successfully to other applications, including the amusement industry. However, the PES systems recently introduced to the fairground industry are systems for which techniques such as HAZOP, FMEA or QRA are complicated and time-consuming to use.

The industries that have made any progress towards a methodology for SIL selection and validation are the motor (MISRA), gas (IGE) and Chemical (CCPS, IEC61511) industries. The methodologies described in [MISRA 1994], [MISRA 1995], [EMCATT 1995], [Hobley, et al 1995], [Jesty, Giezen and Fowkes 1998], [Jesty and Hobley 1996], [CCPS 1993] and [IEC 61511] have been necessarily specific to their own industries, however the same basic principles could be applied to the fairground industry with some modifications.

Public perception is important for both risks induced by road vehicle usage and fairground rides. However there are important differences due to the facts that children are involved and that those at risk of injury are not the same as those in control, as defined in the DRIVE/MISRA reports, should something go wrong. Users of amusement rides, once they are in operation, have no influence on the risks, unless they try to defeat the passenger containment system. The principle on which the motor industry bases its methodology is the driver's capability of influencing the consequences. This can only be compared with ride operator intervention. There are also the issues of whether the consequences of a control system failure in a fairground ride are comparable and whether a range of controllability categories exist. We suspect that most major failures would lead to an uncontrollable situation in which the operator is either unable or unlikely to successfully intervene. In some ways the chemical and gas industry guidance may be more relevant in that risk to members of the public, who have no influence on the risk, is considered. However, the hazards and the way that they develop are totally different for the chemical industry compared with fairground rides.

There are several HSE documents, both internal and published which enable us to appreciate HSE's approach to risk assessment, management and control. These are usefully supplemented by other references in particular the books by [Fischhoff, Lichtenstein and others 1981], [Wells 1996] and [Stewart and Melchers 1997] and the guidance issued by the Engineering Council [Engineering Council 1993].

This literature review therefore provides a good basis for the development of a SIL selection methodology for fairground rides. However, it is apparent that novel solutions will be necessary given that none of the SIL selection methods already developed are fully applicable. The ideas, presented in guidance from other industries, for the risk-based selection of SILs therefore need to be considered in detail in the context of HSE's approach to risk, and a methodology appropriate for fairground rides developed. It is intended that this will be done in the further stages of this project.

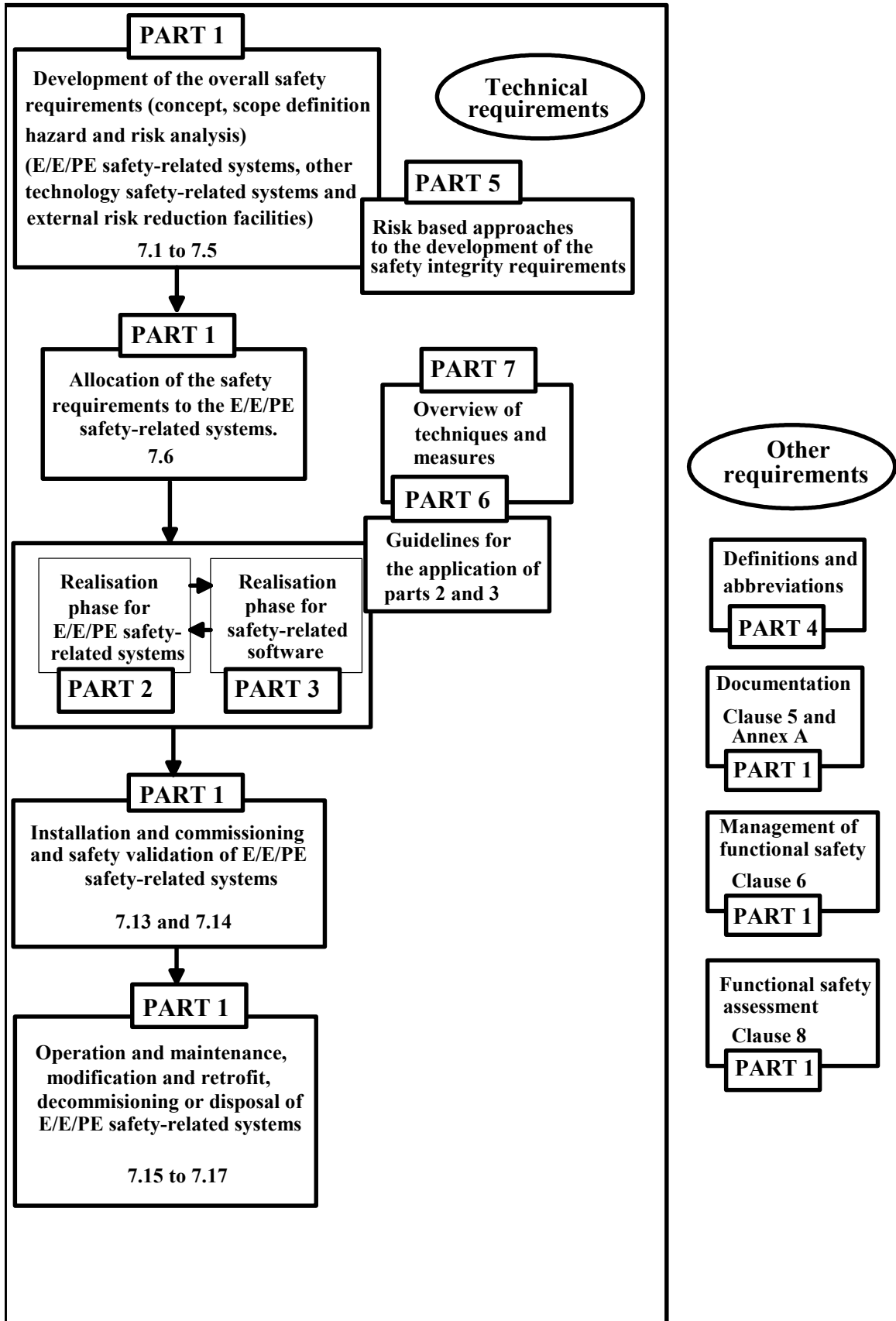


Figure 1 - Overall framework of IEC 61508.

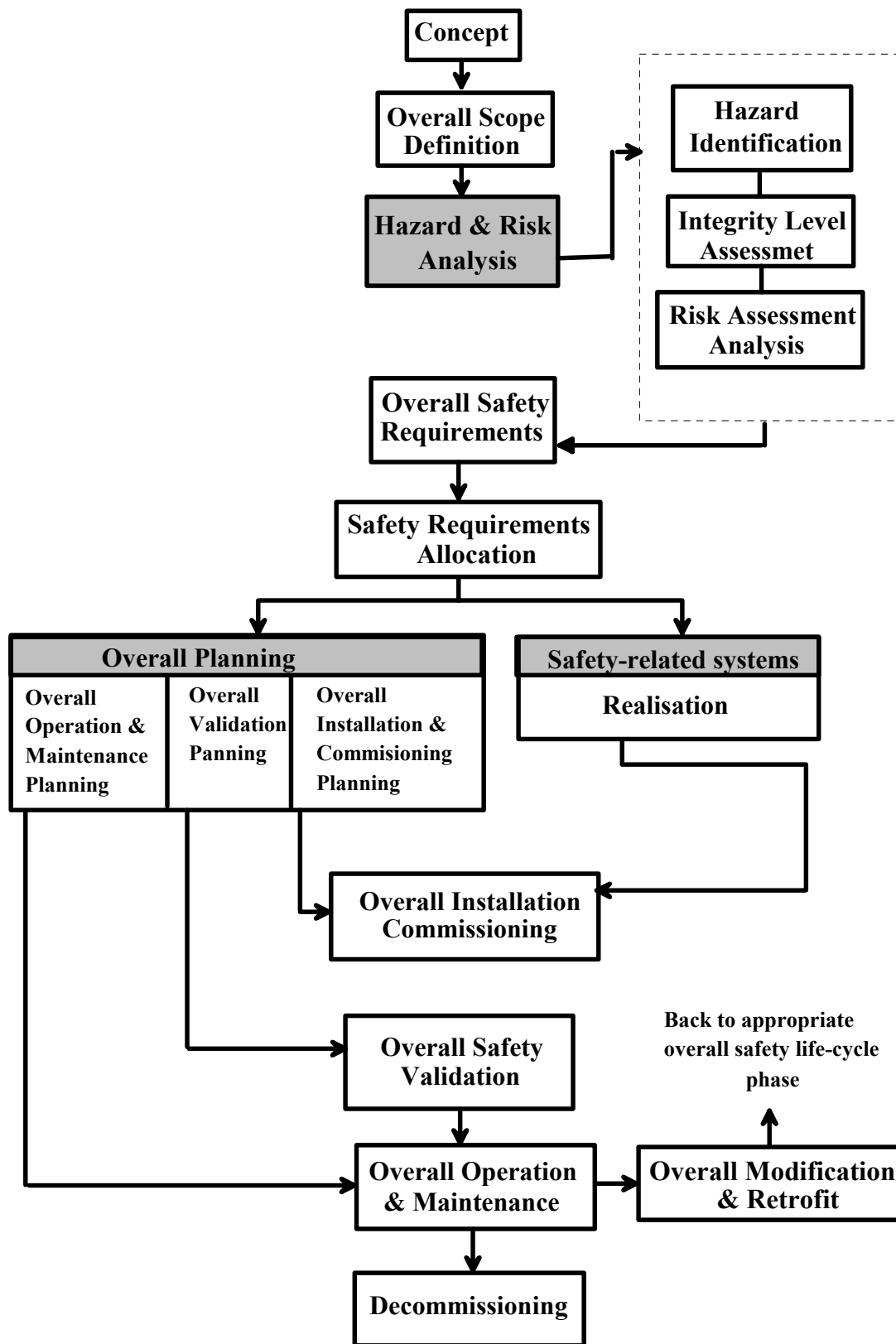


Figure 2 - IEC 61508 Safety Lifecycle

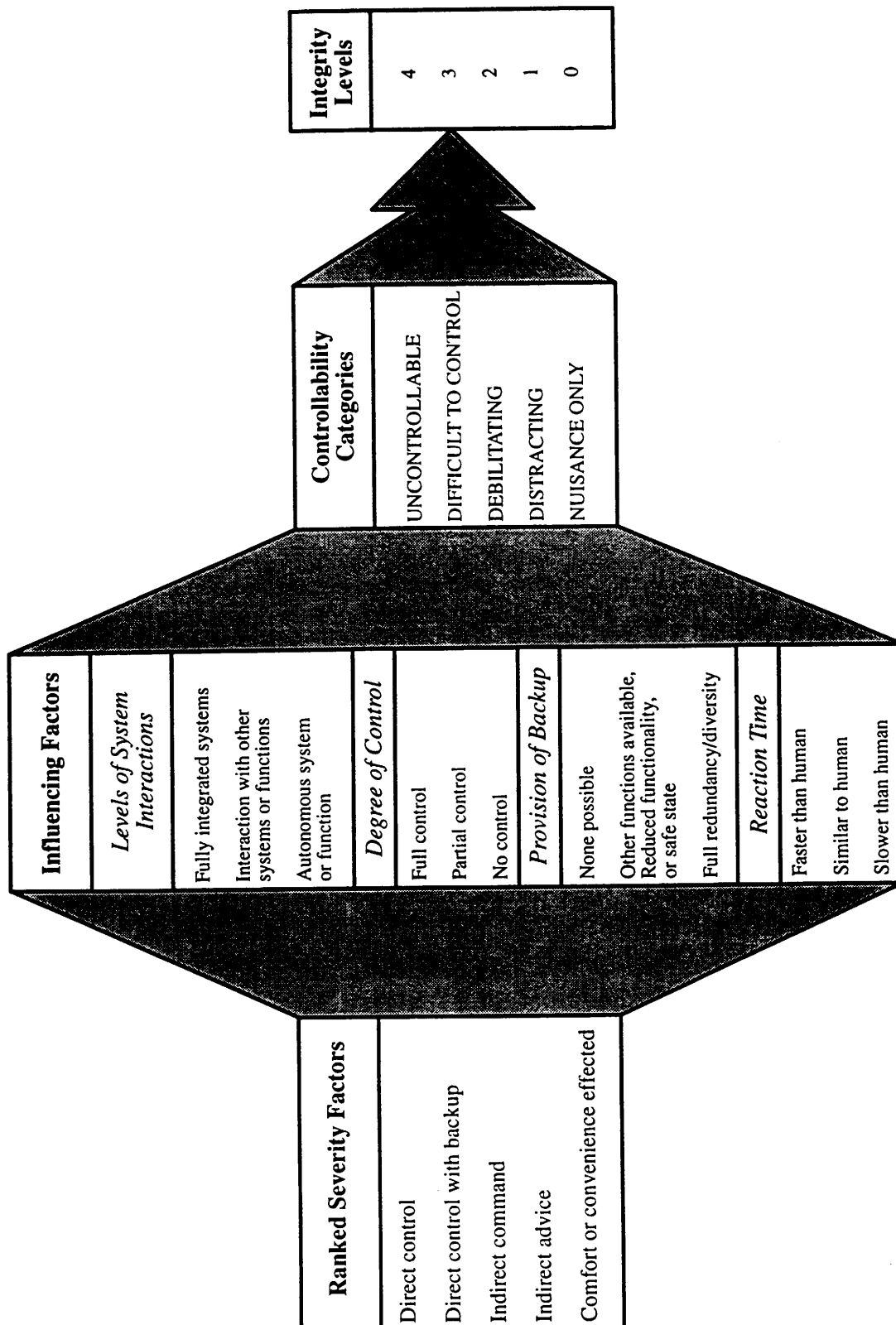


Figure 4 - Relationship between controllability categories and SILs
 © Copyright MIRA 1994, Reproduced with kind permission

8. REFERENCES

ACDS (1991)

"Major Hazard Aspects of the Transport of Dangerous Substances"
Advisory Committee on Dangerous Substances, HSC, ISBN 0118856995

ACMH (1984)

Advisory Committee on Major Hazards, Third Report, HSC, ISBN 0118837532

AS 3533-1988 standard

"Amusement Rides and Devices", Australia

J-M. Astruc and others (1995)

"Towards the Certification of ATT Systems, System Safety Aspects"
PASSPORT II / DRIVE II Project V2058

D. J. Ball and P. J. Floyd (1998)

"Societal Risk", a report prepared for the HSE

R. Bell (1998)

"Framework for Computer Based Safety-Related Systems: Overview of Draft International Standard IEC 61508"

ACOS (Advisory Committee on Safety) Workshop, Toronto, May 1998

R. Bell and D. Reinert (1992)

"Risk and System Integrity Concepts for Safety-Related Control Systems"
Safety Science

S. Brown (1998)

"IEC 61508 - Current Status and Implications for PLCs"

3rd International Symposium on Programmable Electronic Systems in Safety Related Applications, 5-6 May 1998, Cologne, TUV Nord, TUV Rheinland, EWICS

BSI (1988)

"BS 5304:1988 - The British Standard Code of Practice for Safety of Machinery"

BSI (1997)

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

D. J. Burstow (1996)

National Project 3: "Passenger Carrying Amusement Devices Controlled by PES at Fixed and Travelling Fairs", HSE, OM 1996/2 Supplement 3

CCPS (1993)

"Guidelines for Safe Automation of Chemical Processes", ISBN 0816905541

CEN (1999)

"Fairground and Amusement Park Machinery and Structures - Safety"

Part 1: "Design and Manufacture"

Draft Standard of CEN Technical Committee 152, Working Group 1

C. Chambers, P. R. Croll, M. Bowell and P. W. H. Chung (1997)

"Towards Safer Industrial Computer Controlled Systems"

C. Chambers, P. R. Croll and M. Bowell (1997)

"A Study of Incidents Involving Programmable Electronic Safety-Related Systems"

Elsevier Interacting with Computers 11 (1999) 597-609

S. P Cooper (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, Belgium, Feb 99

DEF STAN 00-56/Issue2 (1996)

"Safety Management Requirements For Defence Systems "

Part 1: " Requirements"

Part 2: " Guidance"

DIN V 19 250 (1994)

"Control Technology: Fundamental Safety Aspects to be Considered for Measurement on Control Equipment"

Electrical Contractor's Association

"Guidance on the Use of EN954-1 Machine Safety Standard for Safety-Related Parts of Control Systems"

R. Elvik (1999)

"Cost-Benefit analysis of road safety measures: applicability and controversies"

ESReDA, Oslo, Norway, May 1999

Engineering Council (1993)

"Guidelines on Risk Issues", ISBN 0951661175

EEMUA (1989)

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

H. P van Engelenburg, P Hoogerkamp and L. J. Hopmans (1995)

"A Practical Guide to the Machinery Directive"

Mechanical Engineering Publications Ltd, ISBN 0852989733

- E. Fergus (1998)
"Generalised Calculation of Software Safety Integrity"
HSE PES seminar presentation, Wrightington, Feb 1998
- K. A Ford and A. E. Summers (1998)
"Are your instrumented safety systems up to standard?"
Chemical Engineering Progress, Measurement and Control, Nov 1998
- S. Frost (1998)
" Current Technology and Applications "
HSE PES Seminar presentation, Wrightington, Feb 1998
- B. Fischhoff, S. Lichtenstein and others (1981)
"Acceptable Risk"
Cambridge University Press, ISBN 0521241642
- V. Hamilton and C. Rees (1999)
"Safety Integrity Levels: An Industrial Viewpoint"
Proceedings of the 7th Safety-critical Systems Symposium, Huntingdon, UK
- Hazards Forum (1995)
Safety-related Systems, Guidance for Engineers
- K. M Hobley, P. H. Jesty and others (1995)
"Framework for Prospective System Safety Analysis"
Volume 1 - "Preliminary Safety Analysis"
Volume 2 - "Detailed Safety Analysis"
PASSPORT II, DRIVE II Project V2058
- N. J. Holloway and R. Williams (1990)
"An Assessment of Risks at Fairground Rides" , SRD/HSE/R 522
- HSE (1987)
"PES Programmable Electronic Systems in Safety Related Applications:
Part 1 "An Introductory Guide, Part 2 General Technical Guidelines", Out of print
- 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", ISBN 0118859773
- HSE (1992)
"The Tolerability of Risk from the Nuclear Power Stations", ISBN 0118863681
- HSE (1993)
"Quantified Risk Assessment: Its Input to Decision Making", ISBN 0118854992

HSE (1995/1)

"Out of Control: Why Control Systems go Wrong", C50, ISBN 0717608476

HSE (1995/2)

"5 Steps to Risk Assessment, A Step by Step Guide to a Safer and Healthier Workplace"
IND(G)163L 6/95 C500

HSE (1997)

"Fairgrounds and Amusement Parks: Guidance for Safe Practice"
HS(G) 175, ISBN 0717611744

HSE Video (1998)

"Thrills Not Spills"

HSE (1998)

"The Use of Computers in a Safety-Critical Applications", ISBN 0717616207

HSE (1999)

"Reducing Risks, Protecting People ", Discussion Document DDE11 C150 5/99

N. W. Hurst, C. Nussey and R. P. Pape (1989)

" Development and Application of a Risk Assessment Tool (RISKAT) in the HSE "
Chem Eng Res Des, Vol 67, July 1989

IEE

"Safety-related Systems: a Professional Brief for the Engineer"

IEC (1998)

Draft IEC Standard 61511: "Functional Safety: Safety Instrumented Systems for the process industry sector "

-Part 2 Guidelines in the application of Part 1

-Part 3 Guidelines in the application of Hazard and Risk Analysis

-Part 4 Overview of techniques and measures

IEC (1999)

IEC Standard 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

IGE (1994)

"Programmable Equipment in Safety Related Applications"

IGE/SR/15:1994, Institute of Gas Engineers Communication 1581

HEALTH AND SAFETY LABORATORY

An agency of the Health and Safety Executive

IGE (1999)

"Risk Assessment Techniques

IGE/SR/24:1999, Institute of Gas Engineers Communication 1655

A. Ioannides and N. Worsell (2000)

"Safety Integrity Levels of Fairground Ride Control Systems - Analysis of Accidents"

HSL Internal Report IR/RAS/00/03

ISO/IEC Guide 51 (1999)

"Safety aspects - Guidelines for their inclusion in standards"

P. H. Jesty and others (1992)

"DRIVE Safely - Towards a European Standard: the Development of Safe Road Transport Informatic Systems, Draft 2", DRIVE Project V1051

P. H. Jesty, K. M. Hobley and others (1995)

"Functional System Safety and Electromagnetic Compatibility"

Workpackage "Safety Aspects of Advanced Transport Telematic Systems"

Electromagnetic Compatibility of Advanced Transport Telematics (EMCATT)

DRIVE II project V2064.

P. H. Jesty and K. M. Hobley (1996)

"Integrity Levels and their Application to Road Transport Systems"

SafeComp96, Vienna, Austria.

P. H. Jesty (1996)

"Safety, Security and Speculation"

Traffic Technology International Oct/Nov 96

P. H. Jesty (1997)

"As Safe as Necessary"

Traffic Technology International June/July 97

P. H. Jesty, J. Giezen, M. Fowkes (1998)

"Co-Ordinated Dissemination in Europe of Transport Telematics: System Safety Guidelines"

CODE TR 1103.

P. H. Jesty (1998)

"Safety Issues for Future Intelligent Transport Systems"

Safety Systems, the Safety-Critical Club Newsletter, Summer 1998

Frank P. Lees (1996)

"Loss Prevention in the Process Industries", ISBN 0750615478

R. W. Macbeth (1998)

"A Study into the Use of the Approximate Risk Integral as a Representation of Societal Risk in Toxic RISKAT", HSL Internal Report IR/RAS/98/10

D Masters (1996)

"Machine Guarding - an Australian View", Safeguard Jan/Feb

MISRA (1994)

"Development Guidelines for Vehicle Based Software"

ISBN 0952415607

MISRA (1995)

"Report 2 - Integrity"

A. Nolan (1999)

"Independent Verification Magic or Myth?"

Proceedings of the 7th Safety-critical Systems Symposium, Huntingdon, UK

S. T. Parry (1986)

"A Review of Hazard Identification Techniques and Their Application to Major Accident Hazards", SRD/R/379

H. Raafat (1995)

"Machinery Safety: The Risk Based Approach, Practical Guidelines on Risk Assessment, Standards and Legislation", Technical Communications (Publications) Ltd.

ISBN 1859530060

RAPU (1995)

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

B. Rasmussen and C. Whetton (1997)

"Hazard identification based on plant functional modelling"

Reliability Engineering and System Safety

Felix Redmill (1999)

"IEC 61508 - An Influential Safety Standard"

The Safety and Health Practitioner, Feb 1999

T. Schneider, K. Weber and R. Locher (1994)

"Risque, acception des risques du point de vue technique et sociologique, approche du dialogue sur les risques", study of the Swiss academy of science, SUVA, CNA, INSAI (also available in German and Italian)

Summary and conclusions translated into English (Ref 16110/9900 20002)

Mark G. Stewart and Robert E. Melchers (1997)

"Probabilistic Risk Assessment of Engineering Systems", ISBN 0412805707

Neil Storey (1999)

"Design for Safety"

Proceedings of the 7th Safety-critical Systems Symposium, Huntingdon, UK

A. E. Summers (1997)

"Techniques for assigning a target safety integrity level"
Instrument Society of America, ISA

G. C. Tuff and C. J Beale (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

G. Wells (1996)

"Hazard Identification and Risk Assessment"
IChemE, ISBN 0852953534

M. Wilson (1997)

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

N. Worsell and J. Wilday (1995)

"The Application of Risk Assessment to Machinery Safety, Hazard Identification Techniques", HSL Internal Report IR/L/RAM/95/01

N. Worsell and J. Wilday (1997)

"The Application of Risk Assessment to Machinery Safety, Review of Risk Ranking and Risk Estimation Techniques", HSL Internal Report RAS/97/12

J. Wilday and N. Worsell (1997)

"The Application of Risk Assessment to Machinery Safety, Risk Estimation and Risk Evaluation", HSL Internal Report RAS/97/13

N. Worsell and J. Wilday (1997)

"The Application of Risk Assessment to Machinery Safety, Final Report"
HSL Internal Report RAS/97/14