HSE
Health & Safety
Executive

A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines

Prepared by **Innovation Electronics (UK) Ltd** and the
Health & Safety Laboratory (HSL) for the
Health and Safety Executive 2004

RESEARCH REPORT 216

HSE
Health & Safety
Executive

A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines

Mark Charlwood BSc
Innovation Electronics (UK) Ltd
21 Dean Lane
Hazel Grove
Stockport
SK7 6DH

Shane Turner BSc MSc PhD CPhys MInstP
Health & Safety Laboratory
Broad Lane
Sheffield
S3 7HQ

Nicola Worsell BSc MSc
Health & Safety Laboratory
Broad Lane
Sheffield
S3 7HQ

This contract research report describes the development by the authors, with funding from HSE, of a methodology for the assignment of required Safety Integrity Levels (SILs) of safety related electrical control systems of machinery. The rationale behind the methodology and how to use it in practice are also explained in some detail. The methodology has been developed and accepted for inclusion in an informative annex of the International Electrotechnical Committee standard IEC 62061: “Safety of Machinery Functional Safety of Electrical, Electronic and Programmable Electronic Control Systems for Machinery” currently being drafted.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

HSE BOOKS

First published 2004

ISBN 0 7176 2832 9

ACKNOWLEDGEMENTS

The authors would like to acknowledge the considerable input to this project from the rest of the project team: Steve Frost from HSE, Colin Chambers and Jill Wilday from HSL. The authors would also like to acknowledge the help from Tom Treble in putting together and running the workshop presented to members of the IEC/TC44/WG7 when work first began on the development of this methodology.

CONTENTS

EXECUTIVE SUMMARY

Objectives

This contract research report describes the development by the authors, with funding from HSE, of a methodology for the assignment of required Safety Integrity Levels (SILs) of safety related electrical control systems of machinery. The rationale behind the methodology and how to use it in practice are also explained in some detail.

The methodology has been developed and accepted for inclusion in an informative annex of the International Electrotechnical Committee standard IEC 62061: "Safety of machinery Functional safety of electrical, electronic and programmable control systems for machinery" currently being drafted.

Main Findings

A quantified, structured and systematic methodology has been developed for assigning SILs to SRECS safety functions in machinery. This has been developed and accepted for inclusion in IEC 62061 as an informative annex. Appendices in this report provide draft copies of the instructions for use for this methodology and the associated forms that are intended for inclusion in the informative annex.

The methodology encourages the documentation of assumptions and takes into account the risk reduction measures provided by other technologies. This methodology is only one route to the decision as to the most appropriate SIL and is available for use when there are no machinery specific standards or codes of practice upon which to base this decision.

From the validation carried out and the workshop held for members of Technical Working Group IEC/TC44/WG7 the following conclusions could be drawn about use of the methodology:

- it is difficult to use to assign SILs to functions related to emergency stops. An addendum to the methodology is required to explain both types of use of emergency stop equipment (in an emergency and as a high integrity manual stop) and to provide additional guidance in assigning SIL to the related functions.
- the paper format, in the use of forms, can appear unwieldy and inefficient. This is also out-of-date in modern CAD based design offices, which may make put off commercial users. The methodology needs to be developed into a self-documenting software based system to overcome these issues.
- the methodology appears complex which may also put users off. However, the complexity is necessary in ensuring that people think properly about the way an accident develops. Additionally, the methodology captures the full range of harm outcomes without being overly pessimistic. This adds some complexity, but avoids over-estimation of the risk and an onerous SIL being assigned.
- the guidance on the datum event for NFS type accidents is insufficiently clear.
- overall, the methodology was fount to be fit-for-purpose and usable, and generated SILs that appeared sensible.

The complexity of the methodology is offset by clear step-by-step instructions that lead the user through the completion of the forms. If followed carefully whilst completing the forms the task is not too onerous. But if the user attempts to fill in the forms without proper reference to the instructions mistakes can easily be made. A number of minor changes to the instructions and from box descriptors have, however, been identified in the process of writing this report that would improve their clarity.

This SIL allocation methodology assists the machinery sector to assign SILs using a rigorous, structured and transparent risk based approach. The forms also provide a detailed audit trail. The benefits of the technique outweigh the disadvantages, namely its apparent complexity.

Although the methodology has been developed for SIL assignment in the machinery sector, there is no reason why this cannot be expanded to cover SIL assignment in other sectors. The basic approach should be generic across all industries, although some limited development would be required. Certain concepts developed in this work would also be very useful in other areas. For example, the concept of involvement time has application in other sectors, and the combination of person type and involvement time has value for both overall installation risk assessment and deriving individual risk.

Recommendations

1. Further validation of the methodology is required as this has been very limited to date. Validation needs to look at its usability and also the output from the methodology. The SILs derived need to be checked for consistency, sense and accuracy. Having regard to the general lack of structured, documented risk assessment in the sector, it is recommended that the usability of the methodology by target groups be validated.

2. The forms should be updated to include boxes for dates, persons responsible, list reference documents and to improve management of change control.

3. Minor changes to the instructions and form box descriptors should be made to improve their clarity before the standard is published for next committee or public comment.

4. The flow diagrams presented in this report may usefully be added to annex A of the standard.

5. The methodology should be expanded to cover the emergency stop function, and associated guidance produced.

6. The scope of the methodology should be extended to include damage to health, especially from cumulative effects, and to include hygiene to satisfy an Essential Health and Safety Requirement of the Machinery Directive for food processing machines (this would also require expanded scope for IEC 62061 as this is not a risk arising directly at the machine)

7. The concepts of involvement time and Person Type Use Type combinations should be extended and applied more widely in the field of machinery risk assessment, for example in the revision to ISO 14121 (formally EN 1050), or outside the machinery sector, in risk assessment more generally.

8. The methodology should be developed further and applied to other sectors.

1 INTRODUCTION

This contract research report describes the development by the authors, with funding from HSE, of a methodology for the assignment of required Safety Integrity Levels (SILs) of safety related electrical control systems of machinery. The rationale behind the methodology and how to use it in practice are also explained in some detail.

The methodology has been developed for inclusion in an informative annex of the International Electrotechnical Committee standard IEC 62061: "Safety of machinery Functional safety of electrical, electronic and programmable control systems for machinery" (Ref. 1) currently being drafted.

Section 2 of this report first puts the methodology into context by describing the purpose and scope of IEC 62061 and its relationship with other standards. This section then goes on to describe key concepts, such as Safety Integrity Level, and where they come from, explains the need for such a methodology, and describes previous work in the area of machinery risk assessment upon which its development has drawn. Section 3 of the report describes the objectives of the methodology. Section 4 of the report explains the use of the methodology describing the models and mathematical rationales on which it is based. Section 5 describes the assumptions implicit in the methodology. The results of a limited validation exercise are given in Section 6. Conclusions and recommendations for further work are found in Sections 7 and 8 respectively. Finally, the step-by-step guidance and forms used by the methodology, as they will appear in IEC 62061, current at the time of the writing of this report, are given in Appendices A and B respectively.

2 BACKGROUND

2.1 IEC 62061 AND ITS RELATIONSHIP WITH IEC 61508

Historically, the machinery sector has been wary of the use of electronics, particularly programmable electronics, for safety related applications. One reason is the uncertainty regarding the performance of such technology. Another reason is that the sector has many small and medium sized enterprise (SME) suppliers and it has been felt that the measures necessary for the design of safety-related control systems based on programmable electronics were incompatible with the resources of an SME.

ISO 14118 "Safety of Machinery - Prevention of Unexpected Start-Up" (Ref. 2) and IEC 60204-1: "Safety of Machinery, Electrical Equipment of Machines" (Ref. 3) both state that reliance on a single channel programmable electronic system (PES) is not recommended for safety. The IEC 60204-1 recommendation in particular is interpreted by many as an absolute ban on safety functions being implemented by PES in the sector.

However, in the recent past there has been a substantial increase in machine automation due to the demand for increased production and reduced operator involvement. Machinery control systems are therefore increasingly employing complex electronic technology. In automation, the electrical control system that is used to achieve correct operation of the machine process often has an element of safety by virtue of the generation of hazards arising directly from control system failures. By default, electronic control has therefore become common in safety related electrical control system (SRECS) applications, although generally avoided in the design of safeguards and other protective measures with the specific purpose of increasing safety, i.e. reducing risk. Nevertheless, there are now many situations on a machine where protective measures are an integral part of the electrical control systems. A typical case is the use of an interlocking guard where, when it is opened to allow access to moving parts of the machinery, it signals the electrical control system to stop hazardous machine operation.

IEC 61508: "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" (Ref. 4) has been published in recognition of the increasing use of this technology throughout a wide range of industrial sectors. The standard is sector independent in seven parts, the first four of which have been assigned basic safety publication status. It is the first international standard to quantify the safety performance of an electrical control system that can be expected by conforming to specified requirements for not only the design concept but also the management of the design process, operation and maintenance of the system throughout its whole lifecycle from concept to decommissioning. These requirements thereby control failure to function safely resulting from both random hardware failure and systematic faults. Consequently, the standard represents a bold step, as a proactive approach to quantified, objective safety by design. It has already proved of substantial value to designers, users and enforcement authorities in managing safety in an increasingly complex world.

International standards are sometimes regarded as less representative of the technical 'state of the art' than national or regional standards because of their less demanding acceptance procedures and lack of linkage to legislation. Adoption of the principles of IEC 61508 within Europe is shown by its adoption as EN 61508 in 2001.

IEC 61508 can be applied directly or as the basis for writing shorter, sector-specific standards. However, as Redmill points out (Ref. 5) "because of its volume and the lack of widespread understanding of its principles IEC 61508 will be, for many, difficult to use directly" and that for direct use “numerous decisions need to be taken on such matters of relevance and interpretation of various parts of the standard”.

As stated in the scope to part 1 of IEC 61508, a major objective of the standard is to “facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors, associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector.” The progress made in various application sectors such as nuclear, rail and process is outlined in section 2.5.

In the machinery sector ISO 13849-1: “Safety of Machinery – Safety Related Parts of Control Systems – Part 1. General principles for design” (Ref. 6) gives guidance on the design of machinery control systems in order to comply with the essential health and safety requirements (EHSRs) of the Machinery Directive [98/37/EC]. This standard is not specific to electrical control systems, also being applicable to those based on hydraulic, pneumatic and mechanical technologies. It describes well-established strategies for designing systems to avoid (reliability), detect (monitoring and testing) and/or tolerate faults (redundancy and diversity) in order to minimise failure to danger situations. ISO 13849-1 also categorises parts of control systems in terms of their behaviour under fault conditions, from the situation where no single fault can lead to a failure to danger to the situation where a single fault can lead to an unrevealed failure to danger. It is aimed more at traditional electrical technology rather than complex electronic and programmable electronic control systems. It was the intention to publish a part 2 of this standard to take into account the requirements of IEC 61508 but this has never to the authors’ knowledge materialised even as a draft. Clause 4.2 mandates the use of risk assessment according to ISO 14121 (Ref. 7) but does not give guidance on how to establish the required amount of risk reduction provided by a safety-related part of a control system nor how to ensure that this would be achieved. It does not use the concept of functional safety in any depth and categories are not defined in terms of safety integrity. The need for a comprehensive but flexible machinery sector functional safety standard has therefore been apparent for some time.

IEC 62061 is being drafted to fulfil this role. A limited number of specialised product standards, such as the IEC 61496 “Electro-Sensitive Protective Equipment” family (Ref. 8), are now also becoming available. In its own words (Ref. 1) IEC 62061 “sets out an approach to safety-related considerations of electrical, electronic and programmable electronic control systems of machines and provides requirements to achieve the necessary performance.” It is “machine sector specific within the framework of the IEC 61508”.

The purpose of IEC 62061 is given as (Ref. 1) the facilitation of “the specification of the performance of electrical control systems in relation to the significant hazards…”. IEC 62061 seeks to provide guidance for the design and implementation of safety-related electrical control systems employing all electrical technologies from simple electro-mechanical to complex programmable electronics. Linkage to ISO 13849-1 (described above) and IEC 60204-1: “Safety of Machinery, Electrical Equipment of Machines”, to avoid introducing electrical hazards, is provided to ease adoption of the new standard. Finally IEC 62061 gives requirements and guidance on how to “verify that the electrical control system meets its specifications”.

2.2 FUNCTIONAL SAFETY AND SAFETY INTEGRITY LEVELS

Of particular relevance to the methodology described in this contract research report are the key concepts of functional safety and safety integrity levels. These are therefore described here with reference to their source standard IEC 61508: “Functional Safety of Electrical/Electronic/

Programmable Electronic Safety-Related Systems". The relationship of this standard with IEC 62061 has already been explained in some detail in Section 2.1.

There are slight differences in the formal definitions of functional safety in the international standards, but a broad meaning may be summarised as the safety that depends on correct function of components or systems. So far, only detailed requirements for electrical control systems have been specified, although the overall functional safety of risk reduction measures is considered in IEC 61508. There is no inherent limitation to electrical technology and functional safety standards for other technologies and even systems of work may be developed in the future by the appropriate bodies.

The intrinsic differences between the machinery and the other sectors concerned with functional safety lie in the attributes of the protective measures and the supplier-user relationship. Other sectors are primarily concerned with the control of overall risk from the process under control. The principle risks that determine the design generally concern projected outcomes of at least several fatalities or equivalent harm. The maximum projected level of harm from an accident arising directly at the machine, caused by failure of a safety-related electrical control function, is a single fatality. The difference in potential harm severity is reflected in the implementation of protective measures; process risks often use multiple layers of independent protection. This is not the case for machinery where safety generally relies on a single measure. Many machine types are series produced and distributed across the world. The distances, restricted cost and large numbers bias against a close supplier-user relationship and tend to restrict supplier involvement to the early stages of the product lifecycle. Conversely the machine maintenance, repair and modification activities are conducted in the context of limited understanding of the safety design. This situation is reflected in standardised practices for implementing protective measures and their functional safety performance.

Derived from the concept of functional safety is that of a safety function, defined in IEC 61508 as a "function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the Equipment Under Control (EUC), in respect of a specific hazardous event". In the machinery sector standard prEN ISO/FDIS 12100-1 (Ref. 9), a safety function is simply defined as the "function of a machine whose failure can result in an immediate increase of the risk(s)". The definition used in IEC 62061 is taken from the machinery sector standard. Safety functions can be implemented by any technology. IEC 61508 is concerned only with those that are implemented by Electrical/Electronic or Programmable Electronic (E/E/PE) systems either as an integral part of a control system or as an independent system dedicated to safety that interfaces with the equipment under control. IEC 61508 requires the definition of safety performance criteria for safety functions implemented by safety-related E/E/PE systems in terms of safety integrity levels (SILs). Since this concept is dealt with in the parts of IEC 61508 that have basic safety publication status it is necessary for the machinery sector application standard IEC 62061 to also specify safety performance in terms of SILs. Safety integrity is defined in IEC 61508-4 as "the probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time. The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the required safety functions." A safety integrity level (SIL) is defined in IEC 61508-4 as "a discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems, where level 4 has the highest level of safety integrity and level 1 has the lowest."

IEC 62061 refers exclusively to safety-related electrical control systems (SRECS) of machinery as being the electrical part of a control system, that implements safety functions, whose failure can result in a hazard. IEC 62061 requires the SRECS to be specified in terms of the safety functions that it implements and the SILs assigned to them. SIL 4 is not considered in IEC 62061 as it is not relevant to the risk reduction requirements normally associated with machinery because, as explained above, the projected harm in the machinery sector is rarely more than one fatality, whereas IEC 61508 applies to sectors that can credibly result in multiple fatalities.

Although a SIL is derived from an assessment of risk, it is not a measure of risk. It is the intended reliability of a safety function or system required to achieve the necessary amount of risk reduction that needs to be provided taking into account the amount of risk reduction provided by other measures. For example, even though a risk posed by a certain hazard may be high, the contribution of risk reduction measures by other means may also be high; hence, the SIL of the associated SRECS safety function is in fact quite low. For high consequence risks it is in fact not normally a good idea to have an over reliance on a control system for safety.

SRECS safety requirements must therefore be described in terms of the safety functions that they perform (i.e. what it does) and an associated SIL (i.e. how well it does it).

Whilst IEC 61508 contains a wealth of information on how to achieve a specific SIL, it contains only limited guidance, in part 5, on how to decide what the appropriate SIL should be. It is fundamental to IEC 61508, and hence IEC 62061, that safety requirements are based on a thorough analysis and understanding of the risks posed by the equipment under control (for IEC 62061 read machinery) and its control system. A requirement of the standard is therefore that hazard and risk assessment be carried out, but it is left up to the user how to do this.

2.3 RISK ASSESSMENT AND RISK REDUCTION IN THE MACHINERY SECTOR STANDARDS

In the machinery sector the principle standards for risk assessment and risk reduction are ISO 14121: “Safety of Machinery, Principles for Risk Assessment” and ISO 12100-1: “Safety of Machinery, Basic Concepts, General Principles for Design – Part 1 Basic terminology, methodology”. As stated in the introduction of IEC 62061 it is intended to be used within the framework of systematic risk reduction as described in prEN ISO/FDIS 12100 (formally EN 292-1:1991) and in conjunction with risk assessment according to the principles described in ISO 14121: 1999 (formally EN 1050:1997). Unfortunately, there is some conflict between the requirements of these standards and IEC 61508.

ISO 12100 parts 1 and 2 provide a clearly structured, systematic methodology for designing safe machines that has universal acceptance in the sector. Protective measures are applied by the designer according to a strict hierarchy, in accordance with annex 1 of the Machinery Directive (98/37/EEC). This is done taking many factors into account including: the safety of the machine during all the phases of its life, the ability of the machine to perform its function, the usability of the machine, the manufacturing, operational and dismantling costs of the machine, technological development and maintainability. The first part mandates an iterative process using risk assessment in accordance with ISO 14121, but does not specify precise methodologies for estimating the risk from individual hazards and combining these to give an overall risk for the machine. Neither does it give criteria against which to evaluate the risk taking into consideration the other risks that individuals are exposed to. The second part gives practical guidance on designing protective measures to reduce the risk from specific hazards.

ISO 14121 in its own words “establishes general principles for risk assessment by which the knowledge and experience of the design, use, and accidents related to machinery is brought together in order to assess the risks during all phases of the life of the machinery. It is not intended to provide a detailed account of methods for analysing hazards and estimating risks." However, it requires:

- the systematic identification of the various hazards that can be generated by the machine;
- the estimation of the risk for each hazard taking into account the exposure of persons to the hazard, the probability of occurrence of a hazardous event and the possibilities to avoid or limit harm;
- the evaluation of the risk to decide whether further risk reduction is required; and
- the repetition of all of the above once risk reduction in accordance with ISO 12100 has been carried out.

Both standards favour a quantitative approach when practicable but accept estimation by persons having a good knowledge of the machine use and other relevant factors. ISO 14121 gives exacting requirements for the documentation of risk assessment (Clause 9) requiring that "risk assessment shall be conducted so that it is possible to document the procedure which has been followed and the results which have been achieved".

IEC 62061 interprets these requirements so as to be able to conform with the IEC 61508 concepts of functional safety and safety integrity levels as follows:

- identification of hazards;
- initial risk estimation and evaluation to decide whether risk reduction is required;
- a decision as to whether any of this will be provided by a SRECS safety function; and
- specification of the amount of risk reduction the SRECS safety function needs to provide in terms of assignment of a SIL, taking into account the amount of risk reduction provided by other means.

Other than a limited overview of a few methods for hazard identification and risk estimation there is no guidance on the practical estimation of risk in ISO 14121. There is no mention of the assignment of SILs to safety-related control systems in either ISO 14121 or ISO 12100.

Although IEC 61496: "Safety of Machinery - Electro-Sensitive Protective Equipment" gives detailed design requirements for devices of different integrities it does not incorporate guidance on their appropriate use and the assignment of safety integrity. IEC 62046 (Ref. 10) is currently being drafted to cover these aspects.

2.4 EMERGING RISK ASSESSMENT METHODOLOGIES FOR MACHINERY

ISO/IEC Guide 51:1999 – "Safety Aspects – Guideline for their Inclusion in Standards" (Ref. 11) defines risk as the "combination of the probability of occurrence of harm and the severity of that harm". This can be interpreted as risk being made up of two elements, severity and probability and forms the basis of techniques for risk estimation that are popular in the assessment of workplace risks. The risk assessor is required to select the probability of occurrence of harm and the severity of harm from a fixed number of alternatives or categories. There are generally three or four categories for each element but the authors of this contract research report have come across a few with five categories for one or both of the elements.

The two elements of risk above are described in the terms given in ISO Guide 51. However the techniques themselves use a variety of phrases to describe the elements some referring to them as risk components or factors. For example BS 8800:1996 – "Guide to Occupational Health and Safety Management Systems" (Ref. 12), in informative annex D, states that "risks are classified according to their estimated likelihood and potential severity of harm" and gives Table 1 to show "one simple method for estimating risk levels and for deciding whether risks are tolerable". As can be seen, in this case, there are five different levels of risk for different combinations of likelihood and severity. There are numerous techniques that take this form requiring the risk level to be read from a table similar to this one, often referred to as a matrix. There are many others that assign numbers to each risk element and then combine them by multiplication or summation to give a value of risk that is then banded into risk levels. These can also be represented in the form of a matrix. These types of techniques, where risk is made up of two elements, are therefore often referred to by the generic name 'matrix'. The number of risk levels also varies between techniques from three to six.

Table 1 Risk level estimator from BS 8800 annex D

	Slightly harmful	***Harmful***	***Extremely Harmful***
Highly unlikely	Trivial risk	Tolerable risk	Moderate risk
Unlikely	Tolerable risk	Moderate risk	Substantial risk
Likely	Moderate risk	Substantial risk	Intolerable risk

Note the authors of this report are not advocating this technique over any other. It has been used because of the ease of reference to it and availability to the reader.

The vast majority of techniques have been developed specifically for the assessment of workplace risks to help the duty holder comply with the Management of Health and Safety at Work Regulations 1992 that enact the EU Framework Directive [89/391/EEC]. They have been found very useful for ranking these types of risks to prioritise action in the workplace irrespective of the industrial sector. There is therefore a strong temptation to make use of them, either directly or with little alteration, for many other applications including machinery. One such matrix is described in Reference 13.

There is also the added attraction that the two risk elements underlying matrix techniques are firstly consistent with the ISO/IEC Guide definition of risk and secondly they appear to be very simple to use. However, there are a number of difficulties associated with using matrix techniques for risk estimation as an aid to machinery design decisions. There is the tendency to overestimate the severity of harm; as in most situations it is possible to establish how someone can be severely injured or even killed. The terms for probability of harm are often poorly explained and open to different interpretations. The context in which probability is being considered is often unclear. For example, a protective measure may be unlikely to fail each time a demand is placed upon it but becomes more likely if considered in terms of the number of demands in a year and even more likely in the lifetime of a machine and more likely still if considered in terms of the industry as a whole. Matrix techniques also tend to oversimplify how a hazard leads to the realisation of harm. It is difficult to select an appropriate term or category for the probability of harm without making assumptions and properly considering what contributes to this likelihood.

In drafting ISO 14121 it was recognised that the probability of occurrence of harm was, itself made up of a number of elements. These were frequency and duration of exposure, probability of occurrence of hazardous event and possibility to avoid or limit the harm. Since the publication of ISO 14121 a number of techniques for the estimation of machinery risk based on this model have emerged. These follow two formats. One is the use of tables to select a category for each of the four elements. Each category has a numerical value associated with it. These are then combined by addition or multiplication to give a numerical value for risk. Normally, the higher the value, the higher the risk. The other more common format is diagrammatic where a path is taken according to the choice of categories for each risk element considered in a specific order. These are generally referred to as risk graphs. A number of examples, for illustrative purposes only, are given in IEC 61508-5 annex D. It is made clear that these would have to be calibrated for specific sectors.

However, most techniques only consider exposure in terms of frequency without taking into account duration. They can also be very subjective such that it is quite difficult to choose between the categories. Changing a factor by one category can result in a change in SIL. Another problem is that they do not encourage a full consideration of the chain of events leading up to an accident. This can lead to over or under-estimation of risk. Furthermore, without a good understanding of how an accident develops, risk reduction measures may be less effective.

The Health and Safety Laboratory (HSL), an in-house agency of the UK Health and Safety Executive (HSE), has undertaken research and development in machinery risk assessment for many years. A succession of projects (Ref. 14) has led to the on-going development of a risk assessment tool kit of techniques for all the stages of risk assessment as described in ISO 14121. When estimating risk, a technique is provided to first screen out any trivial risks. All other risks are then estimated quantitatively using a set of forms that lead the assessor to consider all elements of risk, taking into account the range of possible severities that could result, and the chain of events that lead up to an accident, including the contribution of existing protective measures, in order to decide whether other measures for risk reduction are required. The technique is based on underlying generic accident causation logic, the arithmetic for which is given on the forms. Lookup tables to aid in the choice of values are provided. Risk criteria are given that are a function of severity, and the result of evaluation is the amount of risk reduction required to be provided by additional measures. If all this risk reduction is to be supplied by a SRECS safety function then this is equivalent to a SIL.

2.5 SIL ASSIGNMENT METHODOLOGIES IN OTHER SECTORS

The machinery sector is not the only one for which IEC 61508 application standards have found to be required. Other sectors have written or are in the process of writing sector application standards. For example, IEC 61511 (Ref. 15) (not yet available for public comment) in the process sector, IEC 61513 (Ref. 16) in the nuclear sector, prEN 50129 (Ref. 17) in the railway sector, and IEC 60601 (Ref. 18) in the electromedical sector. IEC 60601 contains no mention of safety integrity levels. IEC 61513 does not follow the SIL approach and instead a deterministic approach is used to categorise the safety significance of a system pointing out that “the highest practicable integrity is generally deemed necessary for any system that prevents or mitigates the consequences of radioactive releases”. prEN 50129 uses the concept of SIL to specify safety requirements and recommends taking an approach similar to that used in IEC 62061. That is, calculating individual risk by forecasting accidents, taking into account the proportion of near misses and comparing this risk with a target individual risk to obtain the tolerable hazard rate for a safety function for which equivalent SIL is given in a table. However prEN 50129 does not specify what this target risk should be, nor go into details of how to go about the individual risk calculations.

In the process sector IEC 61511 gives various examples of how to assign safety integrity levels. One is based on the calibration of a risk graph with process specific guidance of the selection of factors. Also in the process sector, the Dow Chemical Company have developed a practical, spreadsheet based, system for SIL selection. A safety target factor value, an integer from 1 to

10, is first calculated using a simple matrix that relates the hazard index and quantity involved of the chemical being processed. One page of the spreadsheet contains a list of chemicals for which hazard indices have already been specified along with a facility to automatically calculate a hazard index when various specified properties of the chemical are input. An initiating event factor, another integer, is then found for the hazardous event under consideration. This is taken from another page of the spreadsheet and is based on generic failure rates for the type of event. This factor is the order of magnitude of the hazardous event frequency per year so if the event is not listed this factor is found by first estimating or calculating the event frequency. Credit factors, also integers, can then be allocated to various standard independent protective layers (IPLs) of a chemical process. These are looked up from various other pages of the spreadsheet. In addition, various listed rules need to be applied to check that each layer for which credit is given is truly independent. These factors are all input to the top level of the spreadsheet and a SIL is calculated for the control safety-function associated with the event being analysed.

In the automotive sector MISRA (Ref. 19) has developed three possible ways of allocating SILs to safety-related systems. These are referred to as the pragmatic, controllability and standards based or systematic approaches.

The pragmatic approach is qualitative and consequence based carefully avoiding any mention of accident frequencies or rates. It relies on a rigidly defined classification scheme that may be difficult to apply to novel applications. Integrity levels are selected by associating each level with a given severity as follows:

> **SIL 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 that follow good practice.
> **SIL 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.
> **SIL 3** - represents the integrity required to avoid serious incidents involving a number of fatalities and/or serious injuries.
> **SIL 4** - represents the integrity level required to avoid disastrous accidents.

This would appear to be quite quick and simple but suffers from the usual problem of a lack of clear guidance and being open to interpretation. For example, there is some overlap between the descriptions for SIL levels 2 and 3 and what is meant by disastrous in the description for SIL 4 is not defined.

The controllability approach is also qualitative and consequence based but gives qualitative terms for the acceptable failure frequency associated with each SIL (see Table 2). Each safety-function is classified according to the controllability of the motor vehicle should the safety-function fail.

Table 2 Assignment of SILs according to controllability categories (Ref. 19)

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

The selection of the appropriate controllability category is based upon a consideration of various severity and influencing factors such as reaction time compared to human capabilities, provision of backup systems and levels of system interactions. Guidance is given in the source document on what to take into account in considering these. Some of the guidance is quite general but a significant proportion is specific to motor vehicles such as vehicle stability, controllability of acceleration, braking and visibility impairments etc.

The standards based or systematic approach relies on either the use of quantified risk assessment (QRA) and the existence of industry agreed risk criteria or the availability of industrial standards that allocate SILs to various aspects of a design.

2.6 RECOGNISED DEFICIENCIES IN MACHINE RISK ASSESSMENT PRACTICE

The distribution of severity of harm outcomes resulting from a hazardous situation is an area that has caused practical difficulties for a considerable time. ISO 12100-1 when originally published as EN292-1:1991 set the scene by establishing the normative requirement: '*The risk associated with a particular situation or technical process is derived from the combination of both the following factors: a) Probability of occurrence of an injury or damage to health b) Highest foreseeable severity of this injury or damage to health* (sub-clause 6.2 'Factors to be taken into account when assessing a risk'). This can result in the ***probability of any harm*** being combined with the ***highest severity harm outcome*** to give an overestimation of the risk to be assessed. It is human nature to think the worst, and very low probability but high severity outcomes tend to be focussed upon. However, if the selected severity of harm is relatively unlikely it runs counter to instinct and experience to relate that outcome only to the probability of occurrence of the hazardous situation, despite trying to follow the standard. This may result in the probability being adjusted to fit the worst-case only leading to an underestimation of the risk. Alternatively the severity of harm is adjusted subconsciously to fit the probability of occurrence, resulting in a feeling that the worst case is not being taken into account.

Both the definition of risk and the requirement have been changed in ISO 12100-1 FDIS2002. Limiting the efforts expended in the sector on risk analysis, evaluation, assessment and reduction to this invalid combination of factors has not led to optimum safety engineering. The issue of the range of possible outcomes from a hazardous situation and the corresponding probability of each severity (including no harm) has been dealt with comprehensively by HSL in the development of the Machinery Risk Assessment methodology (Ref. 14).

There is a popular misconception that the risk reduction required of a protective measure when operating as intended is the sole determinant of the safety integrity of the functions implementing the measure. The relationship holds in some circumstances but fails dismally in others. Machines incorporate measures to reduce the risk induced by human error or deliberate, foreseeable misuse. Although the risk reduction achieved can be small because the risk without the measure is not large, a large shift in attitude can result from elimination of hazard awareness. Failure to danger of the function engenders a high probability of harm occurring as a result in the change in behaviour interacting with the machine brought about by the attitude shift. A machine having a failed to danger function is not equivalent to one without the measure incorporated into the design. The risk from a failed protective measure can be two orders of magnitude greater than if the protective measure had not been incorporated into the design in the first place because of the different behaviours of both the machine and the person(s) interacting with it. A low integrity function can be worse than none at all.

There is a culture of minimal user input both in the development of safety standards and in undertaking risk assessments. This can lead to an idealised view of machine operation with significant interventions ignored or seriously underestimated. Foreseeable misuse tends not to be adequately foreseen by designers and application engineers, although often the supplier maintenance personnel are well aware of user practices. In general, persons trained and qualified in 'hard' technical disciplines fail to accord sufficient importance to human factors in risk assessments.

Raafat and Nicholas (Ref. 13) have shown that inadequate or absence of risk assessments are a significant root cause of non-compliance with the EC Machinery Directive and the underlying reason was a poor understanding of how to conduct machinery risk assessment.

3 OBJECTIVES

To facilitate the use of the SIL concept within the normative part of IEC 62061 a methodology for SIL assignment is required that can be applied to the machinery sector bearing in mind the constraints due to existing legislation, standards and design approach in the sector. The authors found no internationally accepted generic methodology or anything in other sectors that could be easily modified. As they were familiar with the HSL Machinery Risk Assessment methodology risk estimation tool it was decided to modify this for the specific purpose of SIL assignment and attempt to avoid the recognised deficiencies in current machinery risk assessment practice.

Once hazards have been identified the designer first has to ensure that the protective measures selected are appropriate; that is, when functioning correctly, they reduce the risk sufficiently, are not easy to defeat, do not introduce new risks and permit efficient productive operation. The designer then has to evaluate the risk in terms of the likelihood of the protective measure failing in some way to operate as intended. If the protective measure is a safety related electrical control system (SRECS) this second step is the assignment of an appropriate SIL to the functions of the SRECS. The methodology described in Section 4 has been designed to fulfil this second step. It takes as a starting point the assumption that hazard and risk assessment has already been carried out in accordance with IEC 14121 such that the SRECS safety function, if operating as intended, along with all other protective measures, reduce the risk to a tolerable level. Ensuring that the safety functions are appropriate is dealt with in the normative part of IEC 62061.

Prior to the start of development, some broad guidelines were established in order to maintain a direct linkage to the ISO 12100 approach and to limit complexity of the methodology. This involved:

estimating only the risk relating to malfunction conditions;

- addressing the risk associated with the failure of one safety function at a time;
- making no attempt to estimate the risk from the machinery as a whole; and
- taking proper account of the risk reduction contributed by other protective measures to the risk associated with a specific safety function.

Professional users are the population most at risk from machine accidents, so offering the greatest potential for improvement. The methodology is therefore aimed at, and optimised for, professional use. However, it does not prevent the methodology from giving useful results for machines used domestically or for recreation, but detailed guidance relevant to these situations has been omitted for simplicity.

A decision was also taken to prioritise accuracy over simplicity. The methodology is intended to be sufficiently robust, transparent and well documented to be used to develop good practice for the sector. Conversely, its inherent complexity renders it unsuitable for routine use by machine designers. The foreseen principle users are:

- Working Groups developing standards for a type of machine or group of machines, specifying SRECS functions;
- developers of horizontal standards for a particular aspect of safety or protective measure [B standards in CEN], which could provide simplified SIL assignment specific to the particular standard; and

- designers of novel or special type machines where good practice based on comparison with other machines or horizontal standards is insufficient to assign SILs. There will always be a need for designers leading the development of new technologies to have a generic methodology to address new situations.

4 SIL ASSIGNMENT METHODOLOGY

This section provides a detailed description of the design of the SIL assignment methodology. Appendix A includes the instructions for use and Appendix B includes the forms that are used with the methodology. The methodology is described in the same order as that in the instructions for use, and cross-references to the instructions are made. This section repeats and/or elaborates on some of the guidance in the instructions for use found in Appendix A. However, it is not intended as a substitute for the instructions and should not be used as such.

4.1 INTRODUCTION

The SIL assignment methodology takes a quantified approach to the estimation of SILs for each of the identified SRECS safety functions on a machine. The methodology can be broken down into a number of discrete stages:

- preparation;
- safety function analysis and mapping;
- identification of potential accidents;
- accident scenario frequency estimation;
- harm frequency estimation;
- harm frequency summation; and
- SIL assignment.

Each of these stages is described in detail in Sections 4.3 to 4.10.

SIL assignment is in effect highly specific risk assessment with one risk reduction measure available. SIL is used to define only the ‘safety reliability’ of a SRECS safety function, the rate of failure to danger of the function per unit time. For risk estimation, a rate of dangerous failure is assumed, deemed to correspond to the worst case of a function designed to meet only basic requirements. Within this methodology it is assumed that the only applicable measure to improve safety is to increase the SIL.

Systematic and guided risk estimation constitutes the bulk of the user guidance and forms. Estimation is sufficiently detailed to prompt a thorough analysis of the machine behaviour and human behaviour in hazardous situations. The uncertainty and confidence issues relating to the numerical estimates are discussed in Section 4.1.2. Two distinct models are used to accommodate the different logic that distinguishes those accidents from functions whose failure immediately generates a hazard from others. The ‘lifecycle’ of a malfunction from its instigation to its elimination is considered. This influences risk where fault detection possibilities other than a dangerous occurrence exist. The concept may have future potential in estimating health damage risks from dangerous failures that are currently excluded from this methodology.

The machine SRECS related risks are a sub-set of all the machine risks applying to a person interacting with the machine. Sector practice is to treat separately the risk related to each combination of a particular hazard, intervention procedure and operating mode etc; each risk being reduced to insignificant if practicable. The method is well proven and its structure is the only pragmatic way to address the many and varied risks that typify machines. However, it does not output an estimate of the integral risk either in terms of individual risk to persons of various types or in societal risk terms. There is currently no accepted, detailed method of relating machine risks to persons. This methodology follows the sector structure but sets a value at which the risk from a significant hazard(s) is deemed to be reduced sufficiently. The SIL is assigned so that the risk to any type of person from a specific function is below the significant limit.

4.1.1 Ability to foresee and estimate

All risk assessment relies on the ability to foresee future situations, both routine ones and low probability occurrences. The three factors known to improve the quality of this foresight are a systematic approach, several overlapping techniques, and multiple persons of relevant but diverse experience. All the factors serve to minimise oversights by the screening effect, but multiple persons are also required to facilitate team brainstorming. Methods and techniques are given in the informative Annex A of ISO 14121. Design in accordance with ISO 12100, which mandates the use of ISO 14121 for risk assessment, is established good practice in the sector.

Following IEC 62061, the functional specification is established prior to commencing the integrity specification. For a control function to be specified as safety-related, at least one risk that can increase as a result of malfunction must be identified. This information, together with any information relating to a protective measure of which the function is a part, provides the starting point for the risk analysis in the SIL assignment methodology. A machine design in accordance with ISO 12100-1 will have available the information required by Clause 5 of that standard with all the information and documentation specified in Clauses 4-9 inclusive of ISO 14121. SIL assignment is thus less arduous than comprehensive machine risk assessment and consequently the team recommended in the methodology may be drawn from those that undertook the main machine risk assessment tasks.

As yet there is no authoritative guidance available to assist in selecting the range of environmental occurrences to be taken into account when seeking to identify low probability events. Events such as lightning strikes, tsunamis and major seismic disturbances may be dismissed as improbable (will not occur) for normal purposes but assume significance when dangerous failure rates of less than once per 10 million equipment hours are to be achieved.

4.1.2 Quantified estimates

The problems that arise when estimates are to be expressed quantitatively rather than qualitatively are directly attributable to the precision associated with the two modes of description in everyday life. People are comfortable with qualitative terms for indicating orders of magnitude but move immediately to qualified numerical descriptions to indicate a greater degree of confidence in the data. The converse is equally true; there is reluctance to be held personally responsible for numbers if the uncertainty is large. The reticence to provide numbers that cannot be justified benefits the risk estimation process by compelling the evaluation to be more rigorous.

Estimation generally seeks an average or most likely value. The greater the variability of the parameter the less comfortable people become about settling on an estimated average. It is difficult to justify the derivation of an average in such circumstances without a documented mathematical process that opposes the spirit of estimating. Discomfort rises disproportionately rapidly with the number of independent variables influencing the result. Established practice for estimating project costs and timescales decomposes the total work into component parts, each of which is capable of being estimated comfortably if hard specification information is available. There is also a reassuring feeling that over and underestimates will cancel to some extent. This same approach is followed in the SIL methodology.

4.2 OVERVIEW OF THE METHODOLOGY

The methodology is based around separately calculating the summed risk to different groups of people from all hazards protected by a specific SRECS safety function. The failure to danger rate of each SRECS safety function required for the risk from these safety function associated hazards to meet some target acceptable risk level is calculated for each of the identified groups of people. Each SRECS safety function is considered separately and the total risk from a machine is not calculated; this potential optimism is factored in, however. The failure to danger rate is used in this methodology as a *quantified surrogate* for SIL.

Sections 4.3 to 4.11 below describe in detail the design of the methodology and its fundamental attributes. An overview of the methodology is shown in Figure 1. Section 4.12 then discusses the forms that have been developed to take users of the methodology through each step.

4.3 PREPARATION – STEP 1

Step 1 of the methodology (instructions for use, Section 9.1.2.3) is primarily about gathering all the background information about the machine and its uses that are relevant for functional safety of the machine. Information gathered at this stage is utilised by the rest of the analysis. The range of information collected at this stage includes:

- the list of SRECS safety functions;
- the Use Types that are possible within the constraints stated in the machine specification and instructions for use;
- the Person Types that could interact with the machine; and
- the activities associated with the machine and Person Types.

This stage is critical to the success of the methodology. It needs to be as comprehensive as possible as omissions discovered later may result in substantial re-analysis. It is essential that a thorough hazard analysis for the intended finished machine has been carried out so that this wealth of information can be utilised. The scope of the methodology was limited to SIL assignment and not risk assessment and therefore hazard analysis is outside this method. However, a thorough hazard analysis is assumed to have been completed before application of this methodology, in accordance with ISO 12100-1:2001.

The methodology separates groups of people according to the nature of their interaction with the machine. These different groups, or Person Types (see Section 4.3.1), for example specialist maintenance technician, production operator and cleaner, are identified because they have such different hazard perception, time spent with the machine and interactions. Indeed, trying to estimate risk in one calculation that is representative for all these groups is virtually impossible. Similarly significantly, different types or circumstances of intended use (Use Types – see Section 4.3.2), are also identified separately for a similar reason. The concepts of Person Type and Use Type are fundamental to this methodology.

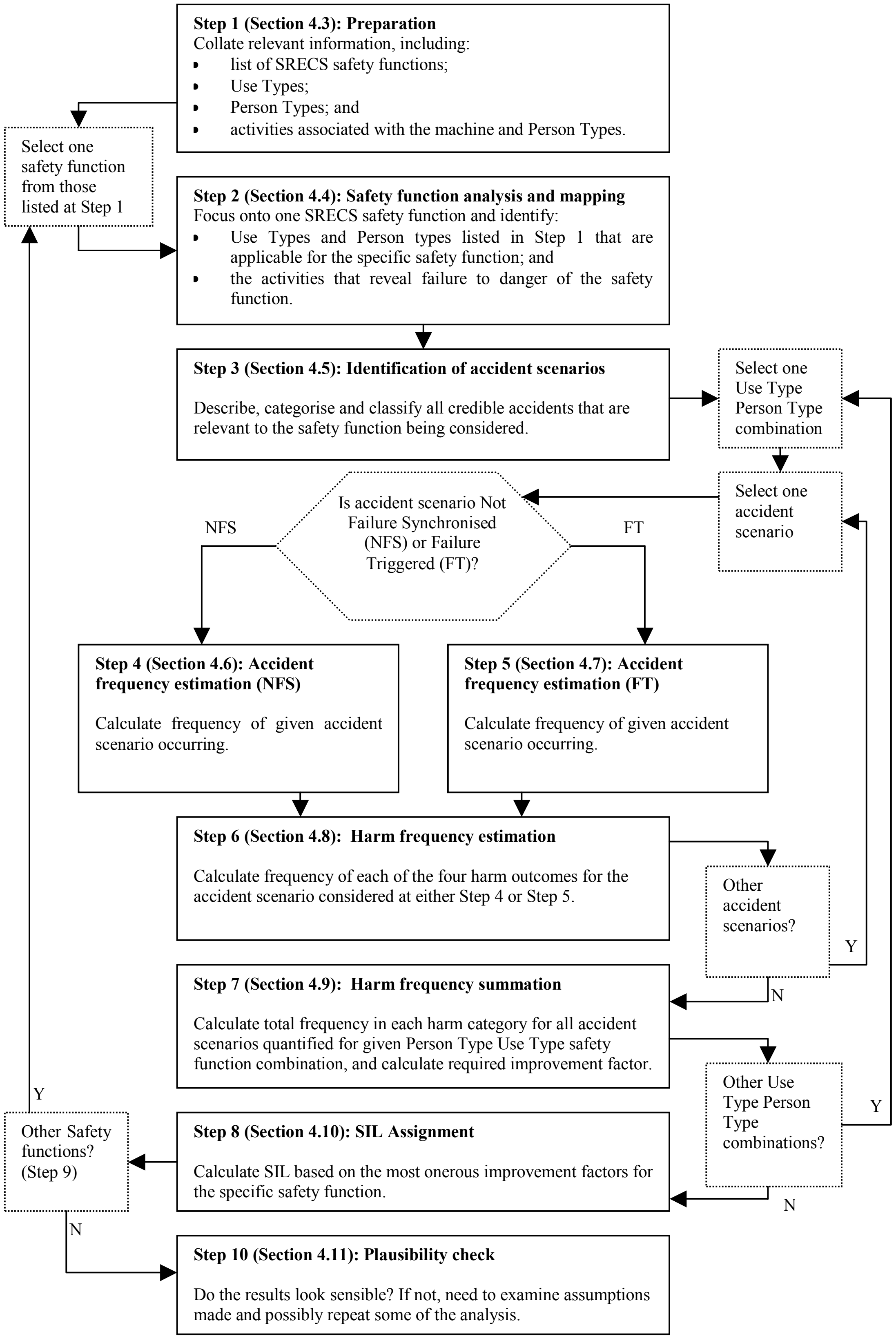

Step 1 (Section 4.3): Preparation
Collate relevant information, including:
list of SRECS safety functions;
Use Types;
Person Types; and
activities associated with the machine and Person Types.
Select one safety function from those listed at Step 1
Step 2 (Section 4.4): Safety function analysis and mapping
Focus onto one SRECS safety function and identify:
Use Types and Person types listed in Step 1 that are applicable for the specific safety function; and
the activities that reveal failure to danger of the safety function.
Step 3 (Section 4.5): Identification of accident scenarios
Describe, categorise and classify all credible accidents that are relevant to the safety function being considered.
Select one Use Type Person Type combination
Select one accident scenario
Is accident scenario Not Failure Synchronised (NFS) or Failure Triggered (FT)?
NFS
FT
Step 4 (Section 4.6): Accident frequency estimation (NFS)
Calculate frequency of given accident scenario occurring.
Step 5 (Section 4.7): Accident frequency estimation (FT)
Calculate frequency of given accident scenario occurring.
Step 6 (Section 4.8): Harm frequency estimation
Calculate frequency of each of the four harm outcomes for the accident scenario considered at either Step 4 or Step 5.
Other accident scenarios?
Y
N
Step 7 (Section 4.9): Harm frequency summation
Calculate total frequency in each harm category for all accident scenarios quantified for given Person Type Use Type safety function combination, and calculate required improvement factor.
Other Use Type Person Type combinations?
Y
N
Y
Other Safety functions? (Step 9)
Step 8 (Section 4.10): SIL Assignment
Calculate SIL based on the most onerous improvement factors for the specific safety function.
N
Step 10 (Section 4.11): Plausibility check
Do the results look sensible? If not, need to examine assumptions made and possibly repeat some of the analysis.

Figure 1 Schematic of SIL assignment methodology

4.3.1 Person Type

A Person Type is defined by the nature and range of interaction with the machine undertaken. In the context of professional use, the individual humans interchangeable within a Person Type are likely to have a closely similar role, job description and title. For example, there may be several operators that use a machine, but as they all do basically the same thing, and are exposed to the same hazards, a single Person Type, the operator, can represent them.

The concept of Person Type helps ensure that the most onerous SIL requirement is found such that the risk from hazards associated with a specific SRECS safety function to the most at risk Person Type is acceptable. The SIL requirements for the safety functions are effectively calculated for each of the Person Types and the highest SIL for each safety function taken to be the required SIL. The user of the methodology is then forced to consider for example a machine operator differently to a maintenance technician. Without taking this explicitly into account the risk to Person Types such as maintenance technicians would be computed incorrectly, as is often the case.

4.3.2 Use Type

The intended uses of the machine, the Use Types, are considered separately because the risks from a machine depend very much on how it is to be used. For example, the risks from a general purpose machine will differ according to the nature of the work and the conditions in which it is used. A different SIL may be required for a specific safety function in each case. Using this concept forces SILs to be calculated for each of the relevant Use Types and the final SIL allocation made based on the most onerous foreseeable use. Use Types must not be confused with activities or phases of use as defined by ISO 12100 (formally EN 292). For example, maintenance of a machine is an activity associated with a Use Type not a Use Type itself. One example of a machine that may have different uses is a conveyor underground that can be used to transport miners to and from the coal face at the beginning and end of a shift and coal during the shift. A crucial safety function associated with the use in transporting miners is to protect them from ending up in the coal crusher.

Use Types are not considered in isolation, however, but are considered in combination with Person Types. SILs are calculated for each combination of Person Type - Use Type that is relevant to a given SRECS safety function. It is the most onerous SIL from these combinations that gives the required SIL for the safety function.

4.4 SAFETY FUNCTION ANALYSIS AND MAPPING – STEP 2

The purpose of Step 2 of the methodology (instructions for use, Section 9.1.2.4) is to focus on one SRECS safety function to identify the Person Types and the Use Types that are relevant to the specific SRECS safety function. Indeed, this is repeated for each of the SRECS safety functions identified in Step 1 (Section 4.3). This is done to focus the risk estimation to those groups of people protected by the particular safety function being considered and those circumstances of use that are relevant.

Also identified in this step are the activities that reveal failure to danger of the SRECS safety function. This may be a functional test, loss of utility of the machine, or an accident or near miss. Revealing failure to danger does not necessarily involve danger. It is imperative that all possible ways that failure to danger of the safety function can be revealed are identified as the frequencies with which these occur of this influence (for unrevealed failures) the probability that a safety function is found failed when demanded. A representative frequency of these activities is used in the accident scenario frequency estimation stage (Section 4.6.2.1).

4.5 IDENTIFICATION OF POTENTIAL ACCIDENTS – STEP 3

The purpose of Step 3 (instructions for use, Section 9.1.2.5) is to describe, categorise and classify those credible accidents that can result in significant risk. Again, this would be repeated for each of the SRECS safety functions identified in Step 1 (Section 4.3). The frequency estimation in latter steps requires there to have been a detailed description of the accident, including the chain of events that led to the accident. This assists in the identification of each precondition (see Section 4.6.3).

Each identified accident is classified as being either failure triggered (FT) or not failure synchronised (NFS). These are dependent on whether the time of the accident is directly related to the time at which the safety function fails to danger. These classifications were developed in order to cope with the full range of accident scenarios; different logic is applied at the frequency estimation stage depending on which classification is relevant. Section 4.5.1 explains these classifications in greater depth.

As well as classifying each accident as failure triggered or not failure synchronised the Use Type - Person Type combinations that are relevant for each accident description are identified. This ensures that risk is estimated for each combination, if significant, thus capturing all risk that a given Person Type is exposed to associated with a single safety function.

4.5.1 Safety function failure classification

One of the initial objectives in the production of this SIL allocation methodology was to have a single model for the underlying accident causation logic. However, it soon became apparent during the development of this methodology that a single model would be insufficient to represent the full range of accident scenarios. From considering the detail of how accidents occur following failure to danger of a SRECS safety function it emerged that the vast majority of accident scenarios fell into one of two categories, either that the timing of the accident has a direct relationship to the time at which the safety function failed, or that the time of the accident was not related to the time at which the safety function failed. These two categories have been named as failure triggered (FT) and not failure synchronised (NFS) respectively and are defined as:

FT: The failure to danger event is the trigger event. The accident follows the failure to danger event either within a few minutes on continuous process machines or within one operating cycle. On continuous process machines the hazard normally occurs instantly but there can be a delay if, for example, a ‘bang-bang’ controller (with hysteresis like a bimetallic strip thermostat) has to change state. The accident occurs without any change to the activities, or cycle of activities, being performed by the machine or persons. The timing of the accident is determined by events that are a predictable, integral part of the on-going activities. There is no other event, in the activities of the machine and the persons, that controls the timing of the accident. The greater the duration the less likely this is to be true. Careful consideration must be given to whether a problem may be identified and rectified if, for non-continuous process machines, the operating cycle is over an hour in duration. Safety functions capable of giving rise to FT accidents are usually functions required for machine utility.

NFS: The failure to danger event is not the final event that triggers the accident. The change to the fault state does not directly control the timing of the accident. The fault is present prior to the accident and the exact timing of the accident is determined by an unrelated event.

FT accidents are much more prevalent for automatic than they are for conventional machines. Some safety functions cannot be associated with FT accidents. For example, the failure of a trip system cannot cause an accident to take place at the time of failure. The fault condition must be present prior to some other unconnected event occurring for an accident to take place. The fault state, perhaps with other preconditions, is analogous to arming a torpedo; firing it, which is equivalent to triggering the potential accident, is a different event which is not time related.

A safety function having FT accidents associated with it must also have at least one potential NFS accident. For example, a failure that occurs while the function is inactive, (e.g. power disconnected), will produce a NFS potential accident when next active. The trigger event is the start of an activity or change of state of the machine. The potential NFS accident for this event(s) must also be considered as a separate accident.

4.6 ACCIDENT SCENARIO FREQUENCY ESTIMATION FOR NFS ACCIDENTS – STEP 4

The purpose of step 4 (instructions for use, Section 9.1.2.6) is to estimate the frequency at which NFS accident scenarios, identified in Step 3 (Section 4.5), occur, if averaged over a long period of time. The frequency is calculated separately for each NFS accident scenario, Person Type, Use Type combination identified at Step 3. The frequency of the accident scenario that has the potential to cause harm of any severity is calculated without taking into account human possibilities to avoid or limit the harm. The range of different harm outcomes from no injury (including near misses) to fatalities is taken into account later where the frequencies calculated at this stage are split between four defined harm outcomes (see Section 4.8).

Each accident is decomposed into a chain of events, where each of these events must occur for the potential accident to occur, and a probability is assigned to each of these events. The SRECS safety function is assumed to fail to danger at a frequency of once every 10000 hours ($1x10^{-4}$ per hour). The basis of this assumption is explained later in Section 4.6.2. Using these data this stage facilitates the systematic calculation of the frequency of each potential accident for each Person Type – Use Type combination and for each SRECS safety function. A number of other assumptions underlying the accident scenario frequency estimation steps are described in Section 5.

The frequency of a given accident scenario is calculated from the product of the frequency of the datum event (Section 4.6.1), the probability that the safety function fails when required (Section 4.6.2) and the probabilities of each of the defined preconditions (Section 4.6.3). The instructions for use and Form 4 (see Appendix B) take users of the methodology through this process.

4.6.1 Datum event

The datum event is some regular repetitive feature of the machine or use of the machine to which each of the events in the accident causation logic can be correlated. This concept was introduced to make it easier to derive probabilities for each of the preconditions as estimation is often simpler if made relative to something. The average datum event frequency for the time the Person Type under consideration is involved with the machine is estimated as the total number of events (the repetitive feature) divided by the total involvement time of the specific Person Type taking into account machine downtime and any time spent away from the machine. The concept of involvement time causes most difficulty and is discussed below in Section 4.6.1.1. A number of detailed examples of how to calculate the datum event in different circumstances can be found in the instructions for use in Appendix A. Different users of the methodology may use different datum events for the same accident scenario and Person Type Use Type combination. This does not matter as probabilities for the preconditions will differ in each case, estimated relative to the specific datum event, such that the accident scenario frequencies would be the same.

4.6.1.1 Involvement time

Involvement time should be interpreted as time for which a person of that type is performing activities directly or indirectly related to their intended use of (or interaction with, in the case of an onlooker) the machine and is time not available for the corresponding activities on another similar machine. This will usually include some time that is not spent at the machine.

Involvement Time is a construct to limit the time over which risk is averaged. Only workers using the same machine continuously for their employment have a straightforward relationship between risk from the machine and the risk in their lives. Other workers such as specialist maintainers move from machine to machine, and some machines are used only seasonally. For professional use, the designer must assume that a person's work-time not involved with a particular machine will be spent on activities of equivalent risk. Only in this way can the overall work related risk of a person be limited whilst fairly allocating fractions of the 'risk budget' to independent sources. The methodology limits the average risk per hour during the involvement time of the Person Type for each SRECS safety function. The machine related risk over a year may be estimated as an abstract individual risk or a hypothetical worker by summing all risks attributable to the work-time.

4.6.2 Failure on demand of SRECS safety function

A base failure to danger rate for the SRECS control function of 1x10^{-4} per hour is assumed. The basis of the methodology is to determine by how much this failure to danger rate must be improved by to reduce the risk to a given Person Type Use Type combination from accident scenarios associated with a single safety function to a target risk level. From this improvement factor a SIL is inferred (see Section 4.10 which discusses this in depth). The base failure to danger rate equates to an order of magnitude greater than the highest target failure to danger rate specified for SIL 1 (SRECS safety function operating in high demand or continuous mode of operation). The magnitude of the assumed base failure to danger rate is not critical, it basically defines the starting position from which relative changes can be measured.

For NFS type accidents, failure of the safety function does not lead directly to an accident, other events have to happen as well. The status of the safety function is unrevealed until an activity that reveals failure to danger, or shows that the function is working occurs. The probability that the safety function has failed when required depends on both the failure to danger rate of the function and the frequency of the activities that reveal failure to danger.

Assuming random failures of the safety function, failures that are unrevealed and a constant failure to danger rate for the SRECS safety function, then the basic 'saw-tooth' reliability model (Ref. 20) can be used. Thus the probability that the safety function is found failed when demanded is given by:

$$\frac{\lambda}{2f} \qquad (1)$$

where λ is the failure to danger rate of the SRECS safety function and f is the frequency at which failures of the safety function would be revealed (see Section 4.6.2.1). Following realisation of any activity that could potentially reveal a safety function that had failed to danger it is assumed that the reliability of the SRECS safety function in the instant immediately after is 1, i.e. as good as new. This assumption adds some optimism to the methodology, although the effect is judged to be negligible.

This relationship breaks down for f less than ½ λ, as nonsensical probabilities would be calculated (values greater than 1). Therefore, the guidance associated with the methodology limits the frequency at which failures of the safety function would be revealed to $1\text{x}10^{-4}$ per hour, i.e. twice the maximum failure to danger rate of the SRECS safety function. This leads to a maximum probability that the safety function is found failed on demand to 0.5. In reality, it is likely that probabilities significantly less than this will be calculated.

The base probability that the SRECS safety function is failed when demanded can therefore be calculated by using Equation 1 and substituting $1\text{x}10^{-4}$ per hour for the failure to danger rate of the SRECS safety function, λ, and the frequency calculated in Section 4.6.2.1 for the frequency of the activities that reveal failure to danger, f.

4.6.2.1 Frequency of activities that reveal failure to danger

Step 2 of the methodology identifies various activities that could reveal the failure to danger of the safety function. These could include:

- functional test, either user initiated or automatic (such as at start-up);
- loss of utility of the machine which may or may not lead to danger;
- recognised abnormal behaviour or exposure to a hazard; and
- other accidents or near misses.

To be able to take into account other accidents care is needed to analyse the accident scenarios in an appropriate order. A rough estimate of the frequency of the accident under consideration can also be included but may need iteratively altering if found to be different to the result recorded at the bottom of the form.

The frequency at which these opportunities occur will dictate how likely the safety function is found to have failed when required. These are assumed to be the only ways in which a failed safety function is revealed as for these NFS type of accidents, failure of the safety function does not directly trigger an event. It is important that claims made here about frequency are justifiable, for example the frequency of a functional test must be practicable, it must be required in the machine's instructions for use and the test results must be recorded. Any frequency assumed must be a formal requirement and not just an assumption or hope on behalf of the designer. If this is not the case there is the potential for fiddles such that an unrealistically low SIL is allocated.

At this stage, the aim is to estimate the frequency of opportunities to reveal failure to danger for the Use Type under consideration. Various activities may be relevant to a given Use Type, therefore the most frequent of the various activities must be selected and a frequency estimated for this. If one activity occurs at a much higher frequency than the others, then this is a reasonable approximation. However, if a number of opportunities occur at similar frequencies then the frequency at which failure to danger is revealed will be underestimated if the opportunities are fully staggered. This may lead to a small pessimism being introduced in the calculation of the probability that the safety function is found failed when demanded. This small pessimism offsets to some extent the uncertainties associated with the estimation of the frequency of a given activity, the natural variation of this frequency over for example a five-day workweek and the optimism with assuming that when a failure has been revealed it is repaired to be “as good as new”.

Once the most frequent activity has been identified, the average frequency must be estimated. The frequency of a specific opportunity to reveal failure to danger can vary a great deal, even on the same machine.

4.6.3 Preconditions

Preconditions are any events that have to occur in addition to the SRECS safety function failing to danger and in addition to the datum event occurring. They include things such as foreseeable misuse, unexpected or expected behaviour of persons or equipment, actions of a third party, faults or failures. The identified preconditions all must happen or be in place for the accident to occur. If a single precondition does not occur it is not possible for the accident scenario to occur. Conversely, if the accident will happen irrespective of something that is listed as a precondition, then it is not in fact a precondition. The probability that a given precondition occurs must have an impact on the accident frequency. For example, doubling the chance of a given precondition must double the accident frequency.

It is obviously necessary for there to be someone exposed to the hazard at some point for there to be an accident. Someone being in the vicinity of the hazard may be thought of as a precondition. However for this type of accident this exposure is incorporated into the datum event through the concept of involvement time and should NOT be listed as a separate precondition.

It is necessary to identify preconditions such that the chain of events making up the accident scenario can be broken down into small enough steps that probabilities can be estimated with greatest confidence. Table A.G1 in Appendix B provides examples of different preconditions. The aim of these examples is not to provide a checklist, but aid thinking, as the examples given are non-exhaustive and on their own generally insufficient to fully define the preconditions for a given accident scenario. Without considering preconditions, estimation of the frequency at which a given accident is predicted to occur would be extremely difficult and any result subject to huge uncertainty.

The preconditions are identified by referring to the description of the accident scenario in Step 3 (Section 4.5). From this description it is possible to list all the events that make up the chain of events. The number of preconditions can vary massively for different accident scenarios. For example, if the accident will happen every time the safety function fails then there are minimal preconditions. The level of detail required is not the most important factor, but preconditions should be resolved to sufficient detail to make probability estimation less uncertain. Similarly, there may be different ways of defining the preconditions. Providing the definitions are clear and no precondition is duplicated, it is not important which way is used.

4.6.3.1 Common cause failure

It is imperative that common cause failure (CCF) is considered. If an event can occur that can cause two or more of the preconditions to occur, then if this were not taken into account the frequency of the accident scenario would be underestimated. This includes where there is any dependence between preconditions. The methodology does not go into the detail of modelling common cause failures, i.e. estimating the independent probability of the preconditions, and separately estimating CCF probabilities. Instead, the preconditions must be analysed and those susceptible to CCF identified. If any are found to be susceptible to CCF either a single precondition must be defined that incorporates the CCF or the probability of each precondition must be limited.

IEC 62061 normative text and the design of the SIL assignment methodology presuppose that dangerous failure of a SRECS control function will lead directly to a hazardous situation when a safety demand is placed on the function. Clause 5 of the standard requires that a SRECS control function is specified as one function to define the behaviour of the machine required to achieve reduction of a risk. This is to prevent the temptation to respecify one function as two or more functions contributing to reduction of a risk so that a low-cost logic unit having limited SIL capability can implement the SRECS. Hence, self-monitoring cannot be specified as a sub-function of another. This requirement seeks to ensure that one SIL defines the safety performance of the SRECS with respect to malfunction when a protective measure is reliant on the SRECS. Measures to control systematic faults provide redundancy and fault detection etc. to achieve the needed safety performance are dealt with in a co-ordinated manner within one function and its corresponding SIL. The coordination is a necessary safeguard for a safety architecture that does not employ independent layers of protection. By this means safety performance is not compromised by an uncoordinated approach to the realisation of the SRECS and a foreseeable abuse is discouraged.

However, there can be circumstances in which two independent SRECS functions do contribute to reduction of the same risk. The situation may arise because one function alone controls a different risk e.g. an energy limiting function alone may reduce risk during a particular intervention, but act in conjunction with a further function to reduce a different risk during another activity. If another function of the Electrical Control System is included as a precondition, the CCF or similar systematic faults affecting both functions must be carefully considered. In this case the methodology limits the failure to danger probability that can be claimed to a minimum of 0.1 if the function(s) included as a precondition is safety related and 0.35 if not. It is judged by the authors of this report that this restriction is required to accommodate the likelihood of CCF or similar systematic faults that, in such circumstances, are not controlled by the requirements of Clause 6 of IEC 62061 (Ref. 1).

4.6.3.2 *Quantification of preconditions*

Once preconditions have been identified, the probability of their occurrence must be estimated. This is a difficult step and potentially subject to large uncertainty. Where data is available this should be used. The probability should be taken as an average over many occasions and many different examples within the Use Type, Person Type and precondition combination under consideration. The probability should represent the likelihood of the state or event taking place out of all possible occasions. It is neither the worse case nor best case that is wanted. For those preconditions where there is insufficient specific or generic data then expert judgement should be used. To reduce the uncertainty associated with expert judgment, guidance is provided to facilitate good estimates with tables appended to the forms in Appendix B to support this. Table A.G2 provides probabilities for a range of qualitative descriptors and Table A.G3 provides probabilities of human error for a range of tasks with varying complexity and time constraint. These tables were developed as part of the development of the Machinery Risk Assessment methodology (Ref. 14).

4.7 ACCIDENT SCENARIO FREQUENCY ESTIMATION FOR FT ACCIDENTS – STEP 5

The purpose of step 5 (instructions for use, Section 9.1.2.7) is to estimate the frequency at which FT accident scenarios, identified in Step 3 (Section 4.5), occur, if averaged over a long period of time. The frequency is calculated separately for each FT accident scenario, Person Type, Use Type combination identified at Step 3. It is the frequency of the accident scenario that has the potential to cause harm of any severity that is calculated without taking into account human possibilities to avoid or limit the harm. The range of different harm outcomes from no injury (including near misses) to fatalities is taken into account later where the frequencies calculated at this stage are split between four defined harm outcomes (see Section 4.8).

Each accident is decomposed into a chain of events (exactly as for NFS accidents described in Section 4.6), where each of these events must occur for the potential accident to occur, and a probability is assigned to each of these events. The SRECS safety function is assumed to fail to danger at a frequency of once every 10000 hours ($1x10^{-4}$ per hour). Using these data this stage facilitates the systematic calculation of the frequency of each potential accident for each Person Type – Use Type combination and for each SRECS safety function.

The frequency of a given accident scenario is calculated from the product of the frequency of the datum event (Section 4.7.1), the probability that the Person Type is in range of the hazard (Section 4.7.2) and the probabilities of each of the defined preconditions (see discussion on preconditions for NFS accidents, Section 4.6.3). The instructions for use and Form 5 (see Appendix B) take users of the methodology through this process.

4.7.1 Datum event

The datum event for FT accidents is the actual failure to danger rate of the SRECS safety function as this triggers the accident. The failure to danger of the SRECS safety function is immediately[1] revealed, unlike NFS accidents where failure to danger of the safety function and the timing of the accident are unrelated, and the failure is not immediately revealed. The failure rate is initially assumed to be $1x10^{-4}$ per hour, consistent with the NFS accidents. The choice of this value was not critical, but defines a starting failure rate from which improvement must be made such that the risk limit can be met.

4.7.2 Person in range of hazard

Unlike for NFS type accidents the likelihood that a person is in range of the hazard is explicitly taken into account. This is because a person may be within range of a hazard for only a small amount of time. In this case, on most occasions the failure of the safety function will only result in a harmless loss of utility. However, an accident is possible if the failure occurs when a person is in range of the hazard. The probability that a person is in range of the hazard is estimated. This is calculated as the probability over the time the specific Person Type is involved with the machine, not over all time (the concept of involvement time is discussed in Section 4.6.1.1).

4.8 HARM FREQUENCY ESTIMATION – STEP 6

The purpose of Step 6 (instructions for use, Section 9.1.2.8) is to split the frequency of the accident leading to any harm outcome between possible harm severity categories, from no injury including near miss, through to fatality and permanent disability. A frequency is calculated for each of the harm outcomes.

A particular benefit was gained by separating the consequences (or outcome) of a hazardous situation from its occurrence. As previously described, selection of a single severity of harm outcome in line with sector guidance tends to derange the estimation as explained in Section 2.6.

[1] *within a short period of time*

Four severity of harm categories are used in the methodology as defined below:

Fatality and permanent serious disability: little chance of ever returning to near an accustomed quality of life (personal / work tasks that before the injury were taken for granted are now difficult to carry out).

Irreversible injury (major): some loss in the quality of life but could eventually lead a near normal life. Generally, these are those injuries that are immediately incapacitating.

Reversible injury (minor): no loss in the quality of life. On recovery no tasks would be any more problematic than before the injury. Generally, injuries where the victim is able to depart from the scene of the accident with the minimum of assistance usually fall into this category.

No injury (including near miss): this also captures the possibility of avoidance.

Table 3 (also Table A.G4 in Appendix B) gives examples of injuries that would be classified as each of the harm categories.

Table 3 Severity level definitions

Severity level	***Example injuries***
Fatality and permanent serious disability	Quadriplegia Paraplegia Prolonged unconsciousness (coma) Permanent brain damage
Irreversible injury (major)	Any fracture (other than to fingers, thumbs or toes) Burns causing permanent scarring Damage to sight partial or total Any amputation Loss of consciousness (not prolonged) Dislocation of the shoulder, hip, knee or spine Treatment required due to fume exposure Anything requiring resuscitation
Reversible injury (minor)	Minor broken bones (fingers, toes) Cuts and bruises Minor burns, temporary scarring Anything else requiring first aid only
No injury and near misses	No injury including the possibility of avoidance

The harm categories have been developed based on work carried out previously in this area in Reference 14 and with reference to:

- Classification of Motor Vehicle Traffic Accidents, 5th Ed, National Safety Council, Illinois, USA, ANSI D16.1-1989;
- Coding of Work Injury or Disease Information, Z795-96, Canadian Standards Association;
- International Recommendations on Labour Statistics, ILO, Geneva, 1976;
- Swedish Injury Reporting Regulations;

- Australian workplace injuries compensation guide; and
- UK Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995.

The harm categories essentially represent order of magnitude steps in consequence; this is discussed in greater depth in Section 4.9.1.3.

The way in which the harm frequencies are calculated is to first estimate the probabilities of a given accident leading to each of the four harm outcomes. The sum of these probabilities must add up to one. Multiplying each of these probabilities by the accident frequency (i.e. that calculated in either Step 4, Section 4.6, or Step 5, Section 4.7) gives the harm frequencies. The most onerous part of this step is the estimation of the probabilities. However, use of accident statistics, for example, should help reduce some of this uncertainty.

4.9 HARM FREQUENCY SUMMATION – STEP 7

The purpose of Step 7 of the methodology (instructions for use, Section 9.1.2.9) is to compare the total risk to a given Person Type Use Type combination, generated by different potential accident scenarios associated with a single SRECS safety function, with a risk limit. The factor difference between the total risk and the risk limit, the improvement factor, gives an indication by how much the failure to danger rate assumed for the SRECS control function ($1x10^{-4}$ per hour) must be improved by such that the total risk associated this safety function, for the Person Type Use Type combination, is sufficiently low.

To compare the risk, total frequencies for each harm category are calculated for accidents associated with a Person Type Use Type and SRECS safety function combination. In other words, the directly related risks from one function, generated by different potential accident scenarios, are summed. These summed frequencies are compared with the relevant frequency limit for the specific harm category. It is the factor difference in these frequencies that gives a measure of how much the assumed failure to danger rate for the SRECS control function must be improved by. The highest factor across the harm categories, neglecting the no injury category, is used, which represents the improvement that must be made to the failure to danger rate of the control function such that the risk associated with the dominant harm category is sufficiently low. By default, the risk associated with the other categories will then be lower. This factor is for the specific Person Type Use Type combination, and it may be that other Person Type Use Type combinations yield higher factors, that will ultimately dictate the SIL for the specific safety function. The relationship between improvement factor and SIL is discussed in greater depth in Section 4.10.1.

Summation is only carried out across the accident scenarios associated with a single Person Type Use Type combination, and a single SRECS safety function. Summation across the safety functions is not carried out. The total risk to a Person Type from all hazards associated with a machine, including those not associated with one of the safety functions, is not calculated. It is important to remember that the methodology is not a risk assessment method but is solely a SIL assignment methodology. However, these aspects are accounted for in the choice of the risk limits.

Crucial to this methodology and in the discussion above is the risk target and what is considered to be a risk that is sufficiently low. These areas are, therefore, explored in much greater depth in Section 4.9.1.

4.9.1 Risk criteria

4.9.1.1 Introduction

Risk criteria are required in order to determine the amount of risk reduction that needs to be provided by the safety function. Reference 21 states that "a fundamental requirement to comply with the standards (IEC 61508 and ANSI/ISA S84.01) is a clear and careful identification of target risk level". It goes on to say that these targets vary with industry and that they can be expressed in terms of losses such as injuries and fatalities to employees or the public, etc.. Quantitative risk criteria are usually in the form of the maximum tolerable frequency of a given level of consequence. Such consequence levels could, for example, include a single fatality, multiple numbers of fatalities or injuries.

The philosophy behind risk criteria is that society, or individuals within it, take risks of various kinds in order to obtain benefits. For example, in deciding to undertake a car journey, the benefit of getting to the destination is weighed against the risk of accident. This example is of a voluntary risk, but some risks may be involuntary and, if so, the tolerable frequency would be expected to be lower than for a voluntary risk. This is summarised in Reference 22 that ethically "if a hazard might kill or catastrophically injure someone and we know how to prevent it, and that solution does not cost too much, we should prevent it".

Determining what these criteria should be is far from a simple task. The approach proposed by HSE in 'Reducing Risks Protecting People', R2P2, (Ref. 23) is described in Section 4.9.1.2 below. Section 4.9.1.3 develops this approach and applies it to the harm categories and, finally, Section 4.9.1.4 discusses the risk criteria used in the SIL assignment methodology.

4.9.1.2 HSE's tolerable risk framework

HSE published information regarding risk criteria (Reference 24) as a result of a public consultation exercise. This introduces a framework for the tolerability of risk, referred to as the TOR framework. There is a level of risk that is so high as to be intolerable and a lower level of risk that can be considered broadly acceptable because it is low in comparison with the background risk. Between these two levels is the so-called "ALARP" region, in which a risk is only tolerable if it has been reduced as low as is reasonably practicable. Comparison with current best practice and/or cost/benefit analysis may be used to determine whether ALARP has been achieved.

The TOR framework was originally aimed at risks from nuclear power stations however the underlying philosophy has quickly gained acceptance among both regulator and industry as having wider applicability. However data and resources are not necessarily available in other sectors to enable a fully quantitative approach to be taken. As a result HSE recently published R2P2, which sought to comment on the wider applicability of HSE's quantitative risk criteria and procedures for reducing risks in the workplace and also on the application of the TOR framework where only qualitative not quantitative estimates of risk are available. This framework is illustrated in Figure 2 below.

Within this framework the word tolerable has a very specific meaning and does not mean the same thing as acceptable. Tolerability 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 it is not regarded as negligible or something that might be ignored, but rather as something that needs to be kept under review and reduced still further as and when possible (Ref. 24). R2P2 goes further stating that risks are also expected to be assessed using the best available scientific evidence.

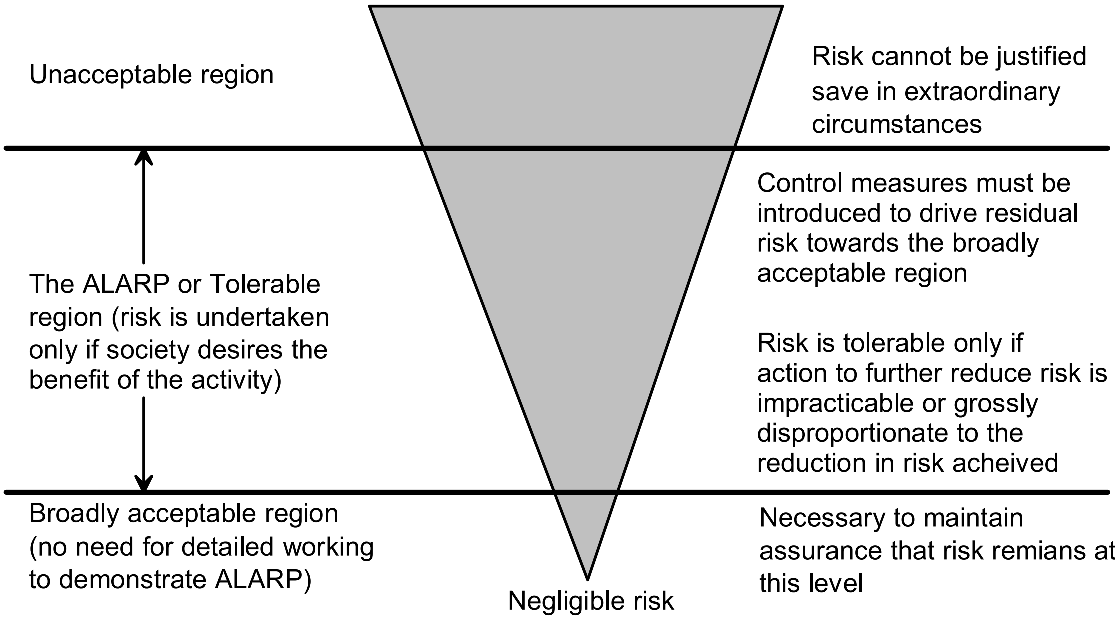

Unacceptable region
Risk cannot be justified save in extraordinary circumstances
Control measures must be introduced to drive residual risk towards the broadly acceptable region
The ALARP or Tolerable region (risk is undertaken only if society desires the benefit of the activity)
Risk is tolerable only if action to further reduce risk is impracticable or grossly disproportionate to the reduction in risk acheived
Broadly acceptable region (no need for detailed working to demonstrate ALARP)
Necessary to maintain assurance that risk remians at this level
Negligible risk

Figure 2 Tolerability of risk framework

HSE has published quantitative risk criteria for individual risk (the risk of death to one individual) in terms of the framework. These criteria were developed for nuclear power stations (Ref. 24) and major hazard installations (Ref. 25). The criteria state that a risk of death of $1x10^{-3}$ per year would be intolerable for a worker (whilst a risk of $1x10^{-4}$ per year would be intolerable for a member of the public, involuntarily exposed to a risk from the same source). A risk of $1x10^{-3}$ per year corresponds to that which is tacitly accepted by workers in the riskiest occupations in the UK, e.g. deep sea diving. A risk of death of $1x10^{-6}$ per year would be considered broadly acceptable, as it would be difficult to distinguish it from the background risk. The region in-between $1x10^{-6}$ and $1x10^{-3}$ per year, is referred to as the ALARP region. In this region the risk would be tolerable only if reduced as low as is reasonably practicable (ALARP). It is important to understand that it is the lower boundary of this region that any creator of risk is expected to strive towards.

R2P2 seeks to make these criteria more widely applicable throughout all types of workplace and to qualitative as well as quantitative risks. There is therefore no fixed boundary to the ALARP region. However 1 in a million ($1x10^{-6}$) per year is still suggested as being the most suitable boundary for broadly acceptable risk as this continues to be small in comparison with the risk a person is typically exposed to from day to day activities. The upper boundary is considered to be less fixed and likely to be more variable between industries however again a risk of 1 in 1000 ($1x10^{-3}$) per year is suggested as being a suitable starting point.

4.9.1.3 Extension of the TOR framework to the harm categories

The discussion above described risk criteria for fatality and not for the other less severe harm categories defined in Section 4.8. Therefore, criteria were developed for each of the harm categories using the fatality criteria as the starting point. The criteria discussed above for fatality have been assumed to be applicable for the fatality and permanent serious disability harm category.

As part of the development of the Machinery Risk Assessment methodology (Ref. 14) a number of risk ranking methods were reviewed, some of which gave some information about relative values of criteria for fatality and other severity levels. Two methods, Rafaat's Risk Calculator (Ref. 26) and Baseline (Ref. 27) allow numerical frequency criteria to be inferred for different severity levels. From these, the upper bound of the ALARP region for a worker sustaining a reversible injury (minor) could be set at 0.1 per year. This was also found to be broadly consistent with the UK accident statistics for different injuries that indicate that the frequency of greater than 3-day loss time accidents is between two and three orders of magnitude higher than the frequency of fatality within any given industry.

The upper bound of the ALARP region for a worker sustaining an irreversible injury (major) can be set as intermediate between the criteria for fatality and permanent serious disability and the reversible injury (minor), i.e. at 1x10^{-2} per year. Again this was found to be consistent with the accident statistics analysed as part of the development of the Machinery Risk Assessment methodology (Ref. 14).

The broadly acceptable level for fatality (and permanent serious disability) is 1x10^{-6} per year. By analogy, the broadly acceptable level for the lower severity levels, irreversible and reversible injury, could be set at 3 orders of magnitude lower than their respective upper bound ALARP values. This therefore giving decade steps in broadly acceptable frequency between the adjacent harm categories.

These criteria across the three harm categories are illustrated in Figure 3.

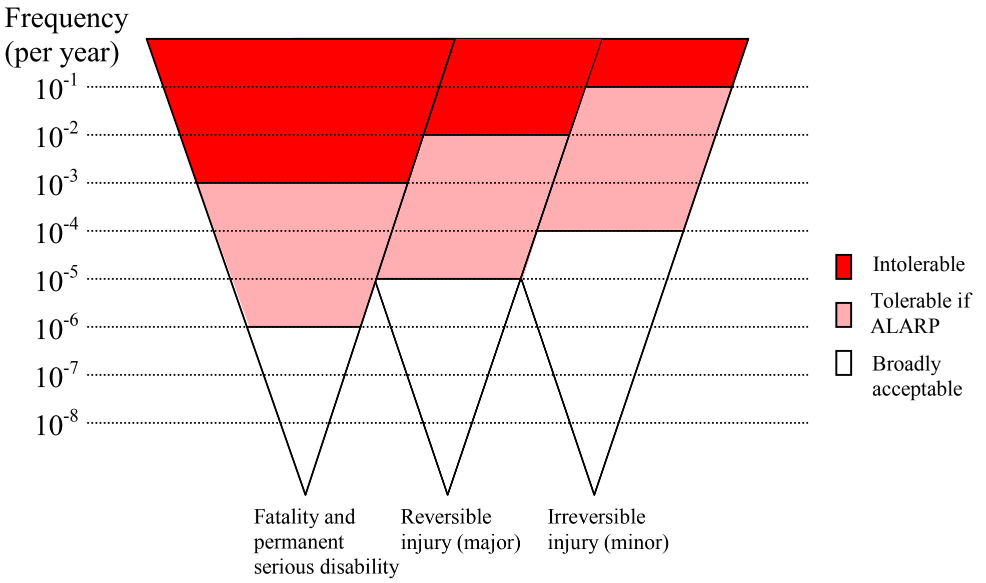


Figure 3 Individual risk criteria

4.9.1.4 Criteria used in this methodology

The criteria used in the SIL assignment methodology, the frequency limit values used in Step 7, are based on those shown in Figure 3, and are shown below in Table 4.

Table 4 Criteria used in SIL assignment methodology

Harm category	*Target maximum frequency*	
	(per year)	(per hour)
Fatality and permanent serious disability	10^{-6}	10^{-10}
Irreversible injury (major)	10^{-5}	10^{-9}
Reversible injury (minor)	10^{-4}	10^{-8}

As can be seen, by comparing the values in Table 4 with Figure 3 it is the 'broadly acceptable' ALARP boundary that is being used as the risk limit for the risk associated with a given SRECS safety function. The methodology derives the improvement factor needed in the base failure to danger rate of a specific SRECS safety function that gives a risk from accidents associated with that function for a given Person Type Use Type that is just below the limit value.

The limit incorporated in the methodology appears on the face of it to be extremely restrictive for the machinery industry and appears to reduce risk further than may commonly be thought both necessary and practical. However, the real risk to a given Person Type will be significantly higher than the limit level for a number of reasons:

1. each SRECS safety function is treated separately and the risk is not summed across all the SRECS safety functions; and

2. risk from the other machine hazards not associated with the SRECS safety functions are not taken into account.

Consequently, each SIL assignment to a SRECS function addresses only a fraction of the overall risk to a person using machinery. This follows accepted practice in the sector and no risk summation is undertaken. Taking these factors into account explicitly would have over complicated the methodology. A value corresponding to the maximum broadly acceptable risk level has been used as a limit value for individual functions in order to accommodate the increase in overall risk that results from the accumulation of numerous contributory risks from other hazards. In this way the risk associated with the hazard protected by a SRECS should not make a significant contribution to the overall risk. The SILs derived from this methodology should be inline with expectations and established good safety engineering practice.

4.10 SIL ASSIGNMENT – STEP 8

The purpose of step 8 (instructions for use, Section 9.1.2.10) is to assign a SIL to the SRECS safety function. This is done by finding the greatest improvement factor across all Person Type Use Type combinations considered for the SRECS safety function under consideration. An improvement factor was calculated at Step 7 for each combination of Person Type Use Type and safety function. From this improvement factor a SIL can be inferred as shown in Table 5. Section 4.10.1 explains the relationship between improvement factor and SIL.

Table 5 Relationship between improvement factor and SIL

Improvement factor	*SIL*
≥1 to <10	1
≥10 to <100	2
≥100 to <1000	3

4.10.1 Link between improvement factor and SIL

The basis for the relationship between improvement factor and SIL can be understood by considering the target failure measures for the different SILs given in IEC 61508-1 (Table 3 from paragraph 7.6.2.9), reproduced in Table 6 below, and the base failure to danger rate assumed for the safety function ($1x10^{-4}$ per hour). However, it is important to visualise the base failure to danger rate as not representing a point but the limit of an order of magnitude range in failure to danger rate (from $1x10^{-5}$ to $1x10^{-4}$ per hour). It can be visualised conceptually as representing the limit of SIL 0[2]. The methodology is based around calculating the degree that this range in failure to danger rate must be improved by in order that the frequency targets shown in Figure 3 are met. But as each SIL represents a decade range in failure to danger rate, any improvement required in the base failure to danger rate from a factor 1 to 10 will mean that the next range of failure to danger rate will be required, i.e. SIL 1. It is then easy to see that an improvement factor of between 10 and 100 infers SIL 2 and 100 to 1000, SIL 3. As an example, if the methodology gave an improvement factor of two from the assumed $1x10^{-4}$ base failure to danger rate, this means that a failure to danger rate of between $5x10^{-6}$ and $5x10^{-5}$ is required. As this range falls across both SIL 1 and SIL 0, a SIL 1 must be assigned to this safety function.

This methodology essentially calculates the required maximum failure to danger rate for a SRECS safety function such that the risk from the accidents to the most dominant Person Type Use Type combination is just below the risk limit. The allocated SIL will result in a failure to danger rate within the range of 0.01-1.00 of this risk limit value as the result of two factors; decade steps in the maximum failure to danger rate between adjacent SIL and the decade band of failure to danger rate within a SIL.

Table 6 SILs: target failure measures for a safety function, allocated to an E/E/PE safety-related system operating in high demand or continuous mode of operation

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

4.11 PLAUSIBILITY CHECK AND SENSITIVITY

The final step in the methodology (step 10 in the instructions for use, Section 9.1.2.12) is to do a plausibility check. This essentially means that the users of the methodology should ask themselves whether the derived SILs make sense. It is also prudent at this stage to see if any

[2] *SIL 0 is introduced here to aid understanding and is not recognised in IEC 61508.*

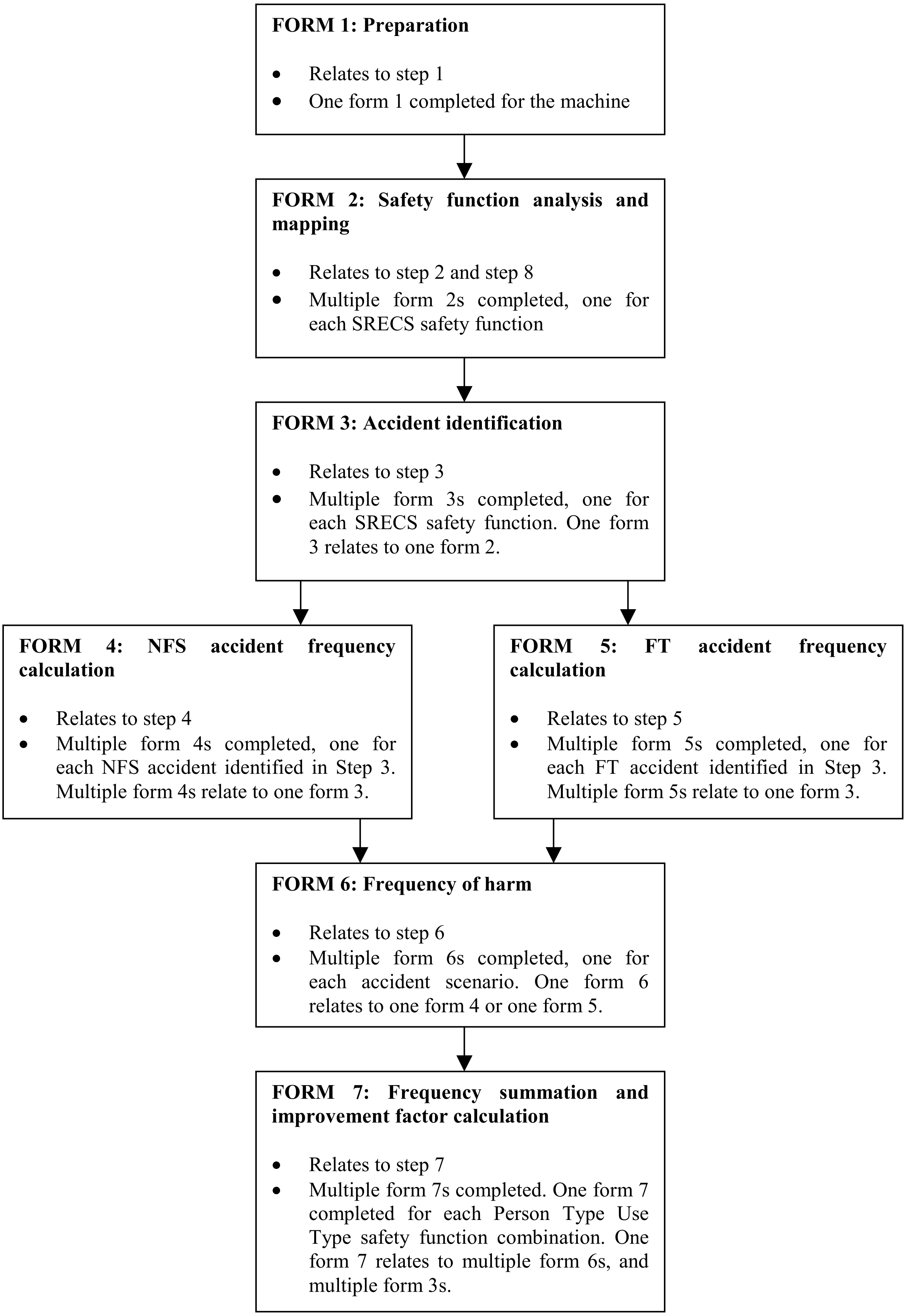
accident scenario dominates the derived SIL. This area can then be examined in more depth and a sensitivity analysis of the assumptions carried out.

4.12 FORMS

A series of user forms (shown in Appendix B) have been developed to facilitate use of the SIL assignment methodology by taking users of the methodology through each step in a methodical and structured way. The purpose of these forms were twofold:

1. to simplify application of this seemingly complex methodology; and
2. to provide a way of ensuring sufficient detail is recorded giving an audit trail, thus ensuring that the basis for the derived SILs stand up to scrutiny.

The forms also provide basic guidance on how to use them, supported by the detailed instructions for use (Appendix A). The flowchart in Figure 4 shows how the forms link together and their relationship with the various steps in the methodology.



FORM 1: Preparation

- Relates to step 1
- One form 1 completed for the machine

FORM 2: Safety function analysis and mapping

- Relates to step 2 and step 8
- Multiple form 2s completed, one for each SRECS safety function

FORM 3: Accident identification

- Relates to step 3
- Multiple form 3s completed, one for each SRECS safety function. One form 3 relates to one form 2.

FORM 4: NFS accident frequency calculation

- Relates to step 4
- Multiple form 4s completed, one for each NFS accident identified in Step 3. Multiple form 4s relate to one form 3.

FORM 5: FT accident frequency calculation

- Relates to step 5
- Multiple form 5s completed, one for each FT accident identified in Step 3. Multiple form 5s relate to one form 3.

FORM 6: Frequency of harm

- Relates to step 6
- Multiple form 6s completed, one for each accident scenario. One form 6 relates to one form 4 or one form 5.

FORM 7: Frequency summation and improvement factor calculation

- Relates to step 7
- Multiple form 7s completed. One form 7 completed for each Person Type Use Type safety function combination. One form 7 relates to multiple form 6s, and multiple form 3s.

Figure 4 Relation between forms and steps in methodology

5 ASSUMPTIONS IMPLICIT IN THE SIL ASSIGNMENT METHODOLOGY

This section cites the assumptions explicit in this SIL allocation methodology that were not made explicit in Section 4 and outlines their limitations. There are many assumptions implicit in any risk assessment. Not all the assumptions in IEC 62061 relevant to faults, failures and system behaviour are made explicit.

A constant rate of failure to danger: The time considered is elapsed time as opposed to time in operation. This represents a simplification of reality that is used consistently through the IEC functional safety standards. The majority of applications in other sectors (process, railways, nuclear) have nearly equal elapsed time and energised/operating time. Functional failures from both random and systematic causes can be induced by operation, non-operation and cycling power. The assumed failure rate may be over-stated for machines used only a few times distributed over the year but is generally a reasonable simplification given the number of influences.

Random hardware failures lead to stable faults: This assumption ignores intermittent faults, a well-known behaviour of electrical systems. There is an analogous problem with systematic faults; functional failure may occur only under specific conditions, e.g. environmental or combination of parameters and may thus remain undetected. Necessary but undesirable assumptions.

Functional failure to danger results in worst case behaviour: Any failure to perform the intended function to specification is assumed to produce the worst case unless the fault reaction function is performed. This equates response time just out of specification with total loss of the safety function. A conservative assumption that is offset by the next two items.

Functional tests have complete coverage: Never true under any circumstances. Neither functional tests needing 'safety margin' for a pass nor even 'proof' tests [an unknown concept in the machinery sector] provide full coverage and full confidence.

As good as new following testing or repair: All aspects of performance, including the rate of failure to danger, meet specification following repair. This assumption is less realistic than in sectors where maintenance is managed more formally.

No reliability improvement programme: A reasonable assumption in most circumstances. No systematic monitoring of the circumstances of use by the supplier and no information for safe use requiring monitoring and the related risk management by the user.

No change in the characteristics of the foreseen use environment over the lifecycle: This assumption has been shown to be unrealistic for EMC because of the rapid proliferation of electronics including deliberate emission of electromagnetic energy, e.g. wireless communications. Taken in conjunction with the previous two items, the ability to foresee the lifecycle sufficiently to confidently claim failure to danger rates of less than once per 10 million equipment years appears unreasonably optimistic.

6 VALIDATION

The work on validation was separated into two parts: comparison with other methods and user tests.

6.1 COMPARISON WITH OTHER METHODS

Initially, attempts were made to compare the SIL allocated to a example control functions with the risk estimates obtained or measures recommended using the techniques within ISO 14121, ISO 13849 and BS 5304:1988 (Ref. 28), now obsolete. The qualitative textual guidance, the risk graph of ISO 13849-1 Annex B and the nomogram of BS 5304 Appendix B were used. In each case severe difficulties were encountered in applying these other methods. The guidance in IEC 61508-5 was applied to assign SIL to the example functions. Again, major difficulties were experienced. The only method that relates directly to the dangerous failure condition is that of BS 5304 in which the state is the starting point for application of the nomogram. The method has relevance to the interlocking functions for which it is intended, but does not deal with functions that generate a hazardous situation immediately upon failure, as duration of exposure is not included. The difficulties encountered correspond to the characteristics of the methods reported in Reference 14. No conclusion could be drawn from this attempt at validation.

6.2 USER TESTS

Three industrial machine sector companies volunteered to pilot the methodology, applying it to example SRECS safety functions as part of new machine development projects. However, one of the companies was obliged to withdraw, prior to testing the methodology, as a result of major re-structuring following a change of ownership. Initial feedback from one of the other two companies was very useful in exposing a key deficiency in the methodology, in relation to handling emergency stop functions, and highlighting the importance of a correct and complete functional specification as an input to SIL assignment process.

The methodology risk model cannot accommodate a true emergency stop function provided solely as a complementary protective measure as defined in ISO 12100-2 Clause 4.5.1. A true complementary protective measure is neither inherently safe design nor safeguarding. It is difficult to predict the detail of the circumstances in which its malfunction creates risk and thus the data needed by the methodology cannot be estimated. However, emergency stop equipment is often used to provide a high integrity manual stop control that is intended to be used routinely. An addendum to the methodology is required to explain both types of use of emergency stop equipment and to provide additional guidance in assigning SIL to the related functions.

Although a copy of IEC 62061 CD2 was provided to the companies piloting the methodology, the engineers had difficulty in drawing up the functional specification that the SIL was to be assigned to. A clear functional specification is needed to design an implementation, irrespective of the SIL assignment methodology employed. It is recommended that Clause 5 of IEC 62061 (Ref. 1) incorporate further guidance on functional specification.

No substantive additional feedback was received from the other company within the timescale of this contract.

6.3 SUMMARY OF VALIDATION

A very limited amount of validation was carried which found no significant flaws with the methodology. However, further validation is required. It is recommended that the methodology undergo further validation in a number of countries. In may be beneficial for this to be a two stage process with the first stage involving the authors of this report facilitating use of the methodology and the second stage left for companies or C-standard writers to use alone. In this way fundamental problems can be separated from problems of usability.

7 CONCLUSIONS

A quantified, structured and systematic methodology has been developed for assigning SILs to SRECS safety functions in machinery. This has been developed and accepted for inclusion in IEC 62061 as an informative annex. Appendices A and B of this report provide draft copies of the instructions for use for this methodology and the associated forms that are intended for inclusion in the informative annex.

This report has explained the need for such a methodology, given a detailed description of the design of the methodology and the assumptions implicit within it, and discussed the limited validation carried out.

The methodology encourages the documentation of assumptions and takes into account the risk reduction measures provided by other technologies. This methodology is only one route to the decision as to the most appropriate SIL and is available for use when there are no machinery specific standards or codes of practice upon which to base this decision.

From the validation carried out and the workshop held for members of Technical Working Group IEC/TC44/WG7 the following conclusions could be drawn about use of the methodology:

- it is difficult to use to assign SILs to functions related to emergency stops. An addendum to the methodology is required to explain both types of use of emergency stop equipment (in an emergency and as a high integrity manual stop) and to provide additional guidance in assigning SIL to the related functions.
- the paper format, in the use of forms, can appear unwieldy and inefficient. This is also out-of-date in modern CAD based design offices, which may make put off commercial users. The methodology needs to be developed into a self-documenting software based system to overcome these issues.
- the methodology appears complex which may also put users off. However, the complexity is necessary in ensuring that people think properly about the way an accident develops. Additionally, the methodology captures the full range of harm outcomes without being overly pessimistic. This adds some complexity, but avoids over-estimation of the risk and an onerous SIL being assigned.
- the guidance on the datum event for NFS type accidents is insufficiently clear.
- overall, the methodology was fount to be fit-for-purpose and usable, and generated SILs that appeared sensible.

The complexity of the methodology is offset by clear step-by-step instructions that lead the user through the completion of the forms. If followed carefully whilst completing the forms the task is not too onerous. But if the user attempts to fill in the forms without proper reference to the instructions mistakes can easily be made. A number of minor changes to the instructions and from box descriptors have, however, been identified in the process of writing this report that would improve their clarity.

This SIL allocation methodology assists the machinery sector to assign SILs using a rigorous, structured and transparent risk based approach. The forms also provide a detailed audit trail. The benefits of the technique outweigh the disadvantages, namely its apparent complexity.

Although the methodology has been developed for SIL assignment in the machinery sector, there is no reason why this cannot be expanded to cover SIL assignment in other sectors. The basic approach should be generic across all industries, although some limited development would be required. Certain concepts developed in this work would also be very useful in other areas. For example, the concept of involvement time has application in other sectors, and the combination of person type and involvement time has value for both overall installation risk assessment and deriving individual risk.

8 RECOMMENDATIONS

1. Further validation of the methodology is required as this has been very limited to date. Validation needs to look at its usability and also the output from the methodology. The SILs derived need to be checked for consistency, sense and accuracy. Having regard to the general lack of structured, documented risk assessment in the sector, it is recommended that the usability of the methodology by target groups be validated.

2. The forms should be updated to include boxes for dates, persons responsible, list reference documents and to improve management of change control.

3. Minor changes to the instructions and form box descriptors should be made to improve their clarity before the standard is published for next committee or public comment.

4. The flow diagrams found in Figures 1 and 4 of this report may usefully be added to annex A of the standard.

5. The methodology should be expanded to cover the emergency stop function, and associated guidance produced.

6. The scope of the methodology should be extended to include damage to health, especially from cumulative effects, and to include hygiene to satisfy an Essential Health and Safety Requirement of the Machinery Directive for food processing machines (this would also require expanded scope for IEC 62061 as this is not a risk arising directly at the machine)

7. The concepts of involvement time and Person Type Use Type combinations should be extended and applied more widely in the field of machinery risk assessment, for example in the revision to ISO 14121 (formally EN 1050), or outside the machinery sector, in risk assessment more generally.

8. The methodology should be developed further and applied to other sectors.

9 APPENDICES

9.1 APPENDIX A: INSTRUCTIONS FOR USE

This appendix includes the latest version of the instructions for use as developed for inclusion in Annex A of IEC 62061. This version was current as of February 2003.

9.1.1 Limits of this methodology

The methodology deals with risks of injury from an accident resulting from a fault or failure of a SRECS safety-related control function. The methodology is not suitable for risks of harm to health that are not immediately detectable and where the harm does not occur and become apparent within a period of 15 minutes or less.

NOTE: A period of 15 minutes has been estimated to be the time of exposure of a single person to a hazardous situation that includes the response of a user to prevent its recurrence. After this period the effects of the exposure will be evident.

9.1.2 Use of the SIL Assignment Methodology

9.1.2.1 Introduction

The optimal SIL assignment is determined by increasing the safety function integrity, thus reducing the likelihood of harm, sufficiently to restrict the risk arising from failure of a SRECS safety function to a broadly acceptable level. Broadly acceptable risk corresponds to a level similar to the background level of risk in ordinary life away from work.

Risk is systematically screened, and calculated as necessary, for each combination of usage characteristics, person type, and machine operating mode in order that the target risk is achieved for all foreseen circumstances. Attainment of the target risk is intended to ensure that each hazard resulting from a SRECS failure is evaluated as a “relevant hazard” (ISO 12100-1:2001 E 3.7) and not as a “significant hazard” when the risk estimation step of ISO 12100-1 Clause 5.3 is carried out after implementation of the SRECS.

The methodology employs a quantitative approach, combining the quantified target failure to danger rates with defined data and quantified estimates. The techniques used are generic but the forms used are specific to the machinery SRECS SIL assignment methodology described below and are not suitable for any other purpose.

9.1.2.2 Overview

A detailed description of each step that needs to be followed to use the methodology is given below. It is recommended that this be followed systematically until confidence in the methodology is gained. The methodology requires the completion of a series of seven forms which themselves contain some basic guidance so that an experienced user of the methodology need not continuously refer back to these instructions. Their understanding is also improved when they are used in conjunction with the lookup tables G1 to G4, which provide readily accessible supplementary guidance. Each form has space for notes. These should be used to record any additional relevant information such as the thinking behind what has been entered onto the form, in particular when it has been decided that something is not applicable.

The methodology requires a team of suitably experienced people to be applied correctly as described. This team should comprise persons with knowledge and skills covering the following topics:

- design and technology of the machine (e.g. designer);
- detail of the use of the machine. All phases, all aspects of use (e.g. operator and maintainer);
- safety engineering or, as a minimum, experience of applying ISO 12100-1/2;
- experience of the different types and conditions of use that may be encountered (e.g. application engineer).

9.1.2.3 Step 1: Preparation (Form 1)

The purpose of Form 1 is to record background information about the machine and its uses that are relevant to the functional safety of the machine. Information recorded in this form will be drawn upon during the rest of the analysis. It is important to be as comprehensive as possible in gathering this information and considering all factors relevant to the safe operation of the machine. Omissions discovered later will result in substantial rework if many safety functions have to be re-evaluated.

It is, therefore, essential that a thorough hazard identification for the intended finished machine, as deliverable to the user, is carried out in accordance with ISO 12100-1:2001. Much preliminary and useful detailed information will be available from prior hazard identification used to specify the functions of the SRECS.

It is important that all the information regarding the machine capabilities, options, accessories, variants and limitations are available together with the user instructions.

1) At the top of Form 1, record a description of the machine model in box 1.1 and version in box 1.2.

2) Insert the name of all the SRECS safety functions given in the Safety Requirements Specification (Clause 5) in boxes 1.3.11 to 1.3.20. Check that the functional specifications are aligned with 5.2.3. Give each a unique reference and insert this in boxes 1.3.1 to 1.3.10.

3) If there are more than ten safety functions an additional Form 1 will need to be filled in as a continuation sheet. Clearly, mark any continuation sheets as such. Indicate at the bottom of the form if it has a continuation Form 1 associated with it.

4) Identify all the Use Types that are possible within the constraints stated in the machine specification and instructions for use. Insert up to four Use Types in boxes 1.4.5 to 1.4.8. If there are more than four Use Types, an additional Form 1 will need to be filled in as a continuation form. Clearly mark any continuation sheets as such, and indicate at the bottom of the form if it has a continuation Form 1 associated with it.

General-purpose machines may have a broad range of intended types and circumstances of use, leading to several Use Types being defined. For example, a machine may be intended to produce repetitive identical products; “one-off” items widely differing and items for use with a specified accessory. The circumstances may include training and varying environments. Use Types should not be confused with the phases of use as defined in ISO 12100. For example start-up, shutdown, maintenance are not in this methodology Use Types but activities as described below. The Use Type is what the machine is used for and enables multi-purpose machines or machines that may foreseeably be used for uses other than that intended by the designer to be comprehensively analysed. As a change in the type or circumstances of use may affect risk considerably, e.g. by changing the conditions or frequency of an activity. In some cases, further persons, e.g. second operators, may be introduced. Use of a machine 24/7, i.e. continuously, is a different Use Type to using the machine five shifts a week. It is imperative that such Use Types are captured here to ensure issues such as start-up, which only relate to one of these Use Types, are accounted for later.

5) Identify all the types of person who could interact with the machine. Be comprehensive; include unintended but foreseeable persons and those apparently at marginal risk such as passers-by. Insert up to five Person Types in boxes 1.5.6 to 1.5.10. If there are more than five Person Types an additional Form 1 will need to be filled in as a continuation sheet. Clearly, mark any continuation sheets as such. Indicate at the bottom of the form if it has a continuation Form 1 associated with it.

Person Type is the formal way of defining persons by their characteristics and activities they perform in relation to the machine, such as ‘operator’, 'maintenance technician' or 'onlooker'. Person Types differ according to the machine and its usage. For example, 'unauthorised child' is an unlikely Person Type for a factory machine but may be relevant to retail outlet, open site industry and domestic machines. A particular Person Type (e.g. second operator) may only be relevant to certain types of use. Other Person Types to consider are supervisor, trainee, and installation engineer.

6) List all the activities associated with the machine and Person Types, for all the phases of use as defined by ISO 12100 relevant to functional safety in boxes 1.6.11 to 1.6.20. Consider: productive operation, setting, adjustment, cleaning, maintenance, fault-finding, product/process changeover, start-up, shut-down, clearing blockages, restoration after power loss if different from normal start-up, stopped, hold, waiting and watching. Loss of power is not an activity, but is part of possible chain of events leading to an accident and should be considered in Step 3. Give each a unique reference and insert this in boxes 1.6.1 to 1.6.10. If there are more than ten activities an additional Form 1 will need to be filled in as a continuation sheet. Clearly, mark any continuation sheets as such. Indicate at the bottom of the form if it has a continuation Form 1 associated with it.

7) List any special features, that could affect the operation of the machine and hence its functional safety, in boxes 1.7.6 to 1.7.10. Give each a unique reference and insert this in boxes 1.7.1 to 1.7.5. Examples are co-ordination with other machines and interaction with higher level systems. For example, is there a supervisory control system, which is able to affect the machines operation, remotely?

8) Record initial ideas regarding possible accident scenarios based on the hazard identification used to specify the safety function(s) in boxes 1.8.9 to 1.8.16. Consider the behaviour(s) of the machine that is controlled by the safety function. Give each a unique reference and insert this in boxes 1.8.1 to 1.8.8.

9) For each safety function listed in boxes 1.3.11 to 1.3.20 of Form 1, write the safety function reference given in 1.3.1 to 1.3.10 respectively in box 2.1 of a Form 2.

9.1.2.4 Step 2: Safety Function Analysis and Mapping (Form 2 – Part 1)

The purpose of Part 1 of Form 2 is to record which Use Types and what Person Types are relevant to each specific safety function and information on the activities that reveal a failure to danger of a that safety function. Part 2 of Form 2 is not completed at this stage but is used later in the analysis to identify the combination of Use Types and Person Type that generates the highest risk and assign a SIL appropriate to this risk.

A separate Form 2 needs to be completed for each of the safety functions listed in boxes 1.3.2 to 1.3.20 of Form 1.

1) Take one of the Form 2's (prepared at the end of step 1 above), putting the rest on one side for later.

2) Write a clear description of what the safety function does in box 2.2.

3) List those Use Types given in form 1 that are relevant to the safety function under consideration, inserting the reference given in boxes 1.4.1 to 1.4.4 of form 1 in boxes 2.3.1 to 2.3.3 of form 2.

4) List the Person Types given in form 1 that are relevant to the safety function under consideration, inserting the reference given in boxes 1.5.1 to 1.5.5 of form 1 in boxes 2.3.4 to 2.3.6 of form 2.

5) If any Use Type or Person Type listed in Form 1 does not apply make a note of its reference(s) and briefly give the reasons why in the notes boxes 2.4.1 to 2.4.6 on Form 2.

6) List all events/activities, which could lead to a revealed failure to danger in boxes 2.5.11 to 2.5.20 reference the Use Type in boxes 2.5.1 to 2.5.10.

Assume complete failure to danger of the safety function with all other functions of the machine operating as intended. Analyse the behaviour of the machine, with the safety function in the failed to danger condition, for all activities and events, as recorded in Form 1, in order to identify potential events and activities that would reveal a failure to danger. Consider the failure event, taking place before and during each activity. No assumptions should be made about how the safety function is implemented.

Revealing a failure to danger does not necessarily involve danger. Ways in which failure is revealed include:

- functional test failed, user initiated or automatic (such as on start-up);
- loss of utility of the machine, which may or may not lead to danger;
- recognised abnormal behaviour or exposure to a hazard;
- accident or near miss.

For example, loss of control of an axis movement of a robot will probably result in loss of utility. This may be known even before a person approaches the robot, perhaps by throughput monitoring. It is unusual to have a formal test of such a function. Failure to danger of a hazardous motion access interlock type safety function will not usually affect the utility of the machine, however formal test of such a function is frequently specified. A safety function may have both utility values as well as being a direct protective measure by reducing risk. This combination often occurs with functions for speed reduction, single stepping etc. used for setting or adjustment.

The failure of a safety function may not be known until a specific trigger event occurs. This trigger event may, require the unintended operation of the machine or a person. Reaction on overload functions and many access interlocks are of this type.

Failure of other safety functions, such as process control type functions, may become evident as soon as the failure of the safety function occurs. Therefore, it is important to consider any unintended behaviour, which can result from failure to danger. For example, unexpected start up, change of mode or setting may be possible.

If there is doubt or confusion, the safety function may need to be redefined. Also consider if the task would be easier if the safety function is sub-divided into a small number of more precisely defined functions, but see also A.5.5.

9.1.2.5 Step 3: Define Potential Accidents (Form 3)

One Form 3 needs to be completed for each Form 2. The purpose of Form 3 is to describe, characterise and classify those credible accidents that can result in significant risk.

1) Record the safety function reference from box 2.1of Form 2, in box 3.1 at the top of Form 3.

2) Using the information generated in Step1 and Step 2, identify the circumstances in which accidents resulting from failure to danger of the safety function can occur. Initially concentrate on the physical interaction(s) between the machine and the person, which could result in harm.

3) Describe each accident as fully as possible in boxes 3.2.2 to 3.5.2.

Several different accidents may be possible resulting from the failure of one safety function. Try to foresee all eventualities. In some cases, correlation with specific interventions is easiest, whilst in others it is better to consider each state of the machine or each step in a process. Free ranging thinking, “brainstorming”, is the best way to identify potential accidents. Do not make any assumptions about the way that the safety function is implemented. Consider failure to danger of the function occurring both prior to and during each activity of the person and of the machine. Human error needs to be taken into account when postulating accidents, refer to Table A.G1 for examples. In circumstances where a credible accident can only take place if another function of the SRECS has an undetected fault, then consider redefinition of the safety function to encompass both functions. For example a “backup” overspeed cut-out could be combined with the basic speed limiting function. If this is not appropriate or helpful, make a note of what this other function is and that it needs to fail for the accident to occur in the notes boxes provided.

Consider each Person Type, Use Type and the activities that are being performing. Eliminate the combinations, which are obviously not relevant to this safety function. For each accident, identify the activity of the person and the mode/state/setting of the machine and the activity it is performing, if any. If the presence of a person in a particular place is required for the accident to occur, define the three-dimensional space and record the details on Form 3. Changes in the definition of the space will affect both the probability of a person being there and the probabilities of the outcomes when a potential accident occurs. A clear written definition of the space, which may be entered in the 'notes' boxes provided, is essential to ensure consistency of assumptions.

4) Record those Use Type and Person Type combinations associated with a credible Accident #1 having a non-trivial risk in boxes 3.2.5 to 3.2.9 for a credible Accident #2 in boxes 3.3.5 to 3.3.9, #3 in boxes 3.4.5 to 3.4.9 etc.

5) Once it is certain that all significant potential accidents have been characterised, classify each potential accident as either NFS or FT, in boxes 3.2.4 to 3.5.4, according to the following definitions.

NFS – not failure synchronised. The failure to danger event is not the final event that triggers the accident. The change to the fault state does not directly control the timing of the accident. The fault is present prior to the accident and the exact timing of the accident is determined by an unrelated event.

FT – failure triggered. The failure to danger event is the trigger event. The accident follows the failure to danger event either within a few minutes on continuous process machines or within one operating cycle. On continuous process machines the hazard normally occurs instantly but there can be a delay if, for example, a 'bang-bang' controller (with hysteresis like a bimetallic strip thermostat) has to change state. The accident occurs without any change to the activities, or cycle of activities, being performed by the machine or persons. The timing of the accident is determined by events that are a predictable, integral part of the on-going activities. There is no other event in the activities of the machine and the persons, which controls the timing of the accident. The greater the duration the less likely this is to be true. Careful consideration must be given to whether a problem may be identified and rectified if, for non-continuous process machines, the operating cycle is over an hour in duration. Safety functions capable of giving rise to FT accidents are usually functions required for machine utility.

FT accidents are much more prevalent for automatic than they are for conventional machines. Some safety functions cannot be associated with FT accidents. For example, the failure of a trip system cannot cause an accident to take place at the time of failure. The fault condition must be present prior to some other unconnected event occurring for an accident to take place. The fault state, perhaps with other preconditions, is analogous to arming a torpedo; firing it, which is equivalent to triggering the potential accident, is a different event which is not time related.

A safety function having FT accidents associated with it must also have at least one potential NFS accident. For example, a failure that occurs while the function is inactive, (e.g. power disconnected), will produce a NFS potential accident when next active. The trigger event is the start of an activity or change of state of the machine. The potential NFS accident for this event(s) must also be considered as a separate accident.

9.1.2.6 Step 4: Frequency of potential NFS accidents (Form 4)

The purpose of Form 4 is to record and facilitate the systematic calculation of the frequency of an NFS accident scenario. This form should not be used for any FT type accident scenarios – for these types of accident see step 5 below.

Accident scenario is used in these forms methodology to describe the potential accident situation, which is specific to one combination of Safety Function, Accident number, Person Type, Use Type and precondition set.

Work through all the potential NFS accidents in Form 3 before looking at the FT type accidents. A separate Form 4 will need to be completed for each combination of Person Type and Use Type for each Accident #number. Depending on the chain of events leading to the accident, there may be more than one Form 4 for each accident.

1) Insert the safety control function reference given in box 3.1 of form 3 (and also 2.1 of form 2) in box 4.1.

2) Insert the use and person type reference numbers being considered in the space provided in box 4.2 and the accident # number in box 4.3

NFS accident frequency is controlled by many different parameters. Therefore, the risk of each combination needs to be estimated using the systematic approach described here. Ensure that irrelevant Person Types and Use Types have been screened out in Form 3 in order to reduce the number of combinations to be addressed.

Estimates of frequency, duration and probability need to be made in this and subsequent steps. Members of the team with first hand experience of use of the type of machine under consideration are those best qualified to make realistic estimates. Aim to be realistic, as opposed to idealistic or unduly pessimistic (e.g. pessimism based on the most unfavourable combination of factors). In particular, the low levels of intervention specified in design are generally not consistently achieved in practice because of unforeseen circumstances including changes in the requirements of the user. Estimates should reflect the situation most likely to occur in practice and should not be based on favourable projections unproven by operational experience.

This step contains the following elements:

- Accident causation logic
- Datum event frequency estimation
- Precondition probabilities
- Demand event frequency estimation
- Scenario frequency estimation

Accident causation logic

1) Taking as a starting point the description of the accident scenario and associated notes given in Form 3, carefully consider the chain of events that leads to the accident. List anything including foreseeable misuse, unexpected or expected behaviour of persons or equipment, actions of a third party, faults or failures that must happen or be in place for the accident to occur. Also if the machine has a number of operating states include the state that the machine has to be in at the time of the accident. Be comprehensive and write everything down at this point even if unsure whether true preconditions or not. The guidance below should then be followed in order to identify which should be included.

2) Choose as the datum event, a routine repetitive event that is also an integral part of the chain of events leading to the potential accident.

An operation of the machine or the person should be fairly easy to associate with the potential accident scenario. The datum event must not rely on faults, failures or unexpected behaviour of persons or equipment. Examples of specific interventions used as datum events are “draining the tank” or “setting the traverse rate”. Datum events relating to normal productive use may be the machine cycle or a specific element of normal use, e.g. “starting up after a tool change”.

3) Insert a brief description of this datum event in box 4.4.1. Everything else in the list can be considered as a precondition.

4) Delete any precondition that will occur directly because of another. Watch out for common cause failure, for example between the normal control system function and safety function.

5) Check that a precondition must occur in addition to all the other preconditions to make the accident possible.

For example, access door open AND stop button not pressed prior to intervention. If an OR condition exists between any two preconditions, for example machine in automatic mode OR manual mode, a new potential accident scenario must be defined and an additional Form 4 prepared i.e. one form to cover automatic and one to cover manual mode. It may be found that there is more than one way of defining the preconditions; providing the definitions are clear and no precondition is actually duplicated it does not matter which way is used.

Take care that a precondition actually has an impact on the event and is not just incidental i.e. simply the state the machine happens to be in or the activity that happens to be going on at the time. For example if the accident will happen irrespective of something that is listed as a precondition then it is not in fact a precondition and should be deleted from the list.

If the accident will happen every time the safety function fails then there are minimal preconditions, for example power on and person in range of the hazard.

6) Insert the list of preconditions remaining after this process in boxes 4.5.1 to 4.5.10.

Datum Event Frequency Estimation

1) Estimate the average rate that the datum event occurs during the time the Person Type is involved with the machine. This is the total number of events divided by the total involvement time of the specific Person Type taking into account machine downtime and any time spent away from the machine.

This process is neither intuitive nor obvious. An estimate of the average rate the datum event occurs during the time the Person Type is involved with the machine is required. It is the second aspect, the involvement time of the Person Type, which causes most difficulty. Involvement time should be interpreted as time for which a person of that type is performing activities directly or indirectly related to their intended use of (or interaction with, in the case of an onlooker) the machine and is time not available for the corresponding activities on another similar machine. This will usually include some time that is not spent at the machine.

A number of examples are given below:

Example 1: An operator of a manual load/unload production machine has a contractual working time of 36 hours each week, and a single shift is worked. The uninterrupted production rate is one component per minute. The first estimate of the machine load event is one per minute, i.e. 60 per hour. Although this is a simple case, the result is an overestimate as will be seen.

For a contractual working time of 36 hours, typically 15% will not be worked on the machine because of washing, breaks, administration, training, meetings etc. Not all the time at the machine is uninterrupted production; time is lost on batch changes, jams and breakdowns, machine setting, cleaning, checking and other similar activities. Typically, 20% of the remaining potential cycles are not performed. Note, all 36 hours count as time performing activities directly or indirectly related to the intended use of the machine by the designated Person Type. However, the average datum event frequency per minute has been adjusted to 1 x 0.85 x 0.8 = 0.68i.e 40.8 per hour. This example is included to show that it is the number of events divided by the actual uninterrupted working time that is important, not the easily observed frequency of the datum event. Information about throughput or component use may be a helpful input in such circumstances.

Example 2: A waste compacting machine is on a public access waste collection site. The Person Type is a member of the public disposing of household waste. Typically, six public disposals are made between compacting cycles. Only 1 in 6 typical individuals of this Person Type will in fact experience the datum event. However, if the compacting occurs, say 4 times a day the Person Type is exposed 4 times per day. This example is included to show the importance of considering the Person Type not individuals. One Person Type may be made up of many individuals. The most obvious case is when the Person Type is ‘passer-by’.

Example 3: Consider as the datum event, 'harvester screen cleaning'. The Person Type considered is 'agricultural worker'. The Use Type considered is that of a worker from the farm being harvested instructed to assist the specialist harvester operator/driver with screen cleaning and other tasks for the duration of the work on the farm. In such a case the actual person allotted to do this task may change every few days. However, as in the example above, all these separate individuals are in fact the same Person Type. Screen cleaning varies with the plant variety harvested, the ground characteristics and the immediately preceding weather conditions. The frequency can vary by at least 10:1. The result from a single farm is, therefore, not appropriate. An average over many farms is needed. This example is included to show the importance of having at least one team member with broad experience and not taking worst case examples as equivalent to the average probability.

Example 4: The operation of automatic machines can require little human intervention and may permit one person to operate many similar machines, for example in the production of textile yarns. This case is an exception to the general rule given above. The person is both behaving as intended as a user of a machine and is simultaneously available to perform similar activities on a similar machine. Because in this special case the intended activity is to attend to a group of machines, the production operator has involvement with all the machines for all of the working time similarly to Example 1. It is also possible, but rare, to be involved with two very different machines simultaneously, such as using one machine to clean another sort of machine. The involvement time for the two machines may be different.

Example 5: A specialist maintenance technician may deal with 100 similar machines in the course of a year. The event under consideration, sensor alignment during power-on diagnostics, may be performed three times in a year on the machine under consideration. The technician spends 10 hours actually working on this machine in the year. The datum event frequency is therefore apparently 3/10 per hour. However, the technician is available for work over the whole year (total hours 1750) and not more than 100 similar machines can be dealt with in a year's work. The involvement per machine is in fact 1750/100 = 17.5 hours, not the 10 hours actually spent working directly on the machine. The datum event frequency is thus 3/17.5 = 0.17 per hour.

2) Insert the estimated datum event frequency in box 4.4.2.

Precondition Probabilities

1) Estimate the probability of each precondition listed in boxes 4.5.1 to 4.5.10. Tables A.G2 and A.G3 can help in estimating probability.

This probability should be an average over many occasions and many different examples within the Use Type, Person Type and precondition set combination under consideration. Neither best case, nor worst case, nor even most typical case is wanted. Rather a probability should represent the likelihood of the state or event, taking place out of all possible occasions.

2) Insert these values in boxes 4.5.11 to 4.5.20.

For a precondition that relates to the failure of another electrical control function restrictions are given, at the bottom of the form, of the lowest probability that can be used. This restriction is required to accommodate the likelihood of common cause or similar systematic faults that are not controlled by the requirements of Clause 6. Assume the least favourable sequence of the appearance of faults, including simultaneity.

Demand event frequency estimation

1) Multiply together the datum event frequency (box 4.4.2) and all the precondition probabilities (boxes 4.5.11 to 4.5.20) as instructed on the form to obtain the demand event frequency and insert this value in box 4.6.

2) Leave boxes 4.7 and 4.8 empty at this point.

3) Repeat the steps above to fill in Forms 4 for all the other relevant Use Types and Person Types for each NFS accident scenario.

Potential accident scenario frequency estimation

1) Identify the most frequent opportunity to reveal failure to danger for the Use Type under consideration and calculate its frequency. Insert this value in box 4.7. This must not be less than $1x10^{-4}$ per hour (once per year).

Use Form 2 to identify the ways in which failure to danger is revealed. The aim is estimate the frequency of opportunities to reveal failure to danger for the Use Type under consideration. To do this the most frequent of the different possibilities must be selected and the average frequency for this estimated. The frequency of a specific opportunity to reveal failure to danger can vary a great deal, even on the same machine. Therefore, an average must be taken.

Consider whether a fault in the safety function is revealed by reduced utility, and how the user will react. Check the frequency of formal tests. For the same safety function and Use Type, evaluate the demand rate for other combinations of Person Type, Accident number and precondition set. These situations should characterise all the instances of recognised abnormal behaviour and exposure to a hazard(s) that will be acted on by a user to correct the fault.

Initially, consider opportunities that are not potential accident scenarios. First consider opportunities that are near continuous, frequent or related to the accident scenario under evaluation on this Form 4. Is it probable an opportunity occurs each day that the machine is used? Possibilities include: continuous utility functions of automatic machines, automatic start-up tests and start of shift formal tests on some power press functions. To determine the value to enter for a continuous utility function, take the reciprocal of the time interval 't' when failure to danger is not revealed (for example, because the machine is switched off). The interval 't' is that time between the end of one period and the beginning of the next period when the failure can be revealed. This can be considered the equivalent of the reciprocal of revelation of failure to danger event frequency and can be a significant factor in the likelihood of accidents at start up. Calculate the equivalent number of the events per day by dividing 24 hours by the time interval 't' in hours.

All calculations of the frequency of events revealing failure to danger in this sub-section must use elapsed time; 24 hours per day, irrespective of the time the machine is used in the day. The same rule applies when considering longer periods; divide the number per week by 168 or the number per month by 730 or the number per year by 8766 to calculate the frequency per hour.

If the machine use is erratic or seasonal, and the opportunity to reveal failure to danger is directly related to its functioning in use, consider only the days the machine is in use. For example, if a machine is used just two days each week during a summer season of 13 weeks and there are 3 opportunities to reveal failure to danger each day it is functioning. Set the frequency as 0.125 per hour, i.e.3/24 = 0.125. If an opportunity is unlikely each day, extend the time frame to a week or a month Estimate the average number of opportunities in a given timescale. There may not be any opportunity probable even in a timescale of one year.

Also, consider all potential NFS accident scenarios that apply to this safety function in this Use Type. The demand event frequency can be taken directly from each relevant Form 4 and the involvement time per year can be derived from the involvement time notes and the pattern of use. There is an implicit assumption that all potential FT accidents are taken into account by loss of utility, so check that this is valid. If not an estimate of the number of times failure to danger is revealed per year must be made.

Multiply the demand event frequency by $1x10^{-4}$ and divide by 2 x the FTD exposure frequency, as instructed on the form, to give the frequency of the potential accident per hour and enter this in box 4.8.

9.1.2.7 Step 5: Frequency of potential FT accidents (Form 5)

The purpose of Form 5 is to record and facilitate the systematic calculation of the frequency of a FT type accident scenario. This form should not be used for any NFS type accident scenarios - these types of accident should have been considered during step 4 above. A separate Form 5 will need to be completed for each combination of Person Type and Use Type for each accident that is considered. There may, therefore, be several Forms 5 for each accident number.

For each accident described in Form 3 it is, therefore, worth attempting to first identify the combination of Person Type and Use Type that will lead to the highest risk.

The risk in these cases is primarily determined by the amount of time exposed to the potential hazard, as a fraction of the involvement time of the Person Type with the machine. Until estimation becomes familiar, select the first combination by intuition. Subsequently, after having completed one Form 5 and seen how the parameters and calculations work, select another combination. Continue until you are confident you have processed the highest risk combination.

3) Insert the safety control function reference given in box 3.1 of form 3 (and also 2.1 of form 2) in box 5.1.

4) Insert the use and person type reference numbers being considered in the space provided in box 5.2 and the accident # number in box 5.3

If there are continuation sheets having the same mapping reference because of multiple precondition sets, then ensure this is marked on the form.

This step is in two parts:

- Accident causation logic
- Scenario frequency estimation

Accident Causation Logic

1) Taking as a starting point the description of the accident and associated notes given in Form 3, carefully consider the chain of events that lead to the accident. The starting point is that the machine is in a state such that failure of the safety function leads directly to a hazard. List anything including, the operating mode and/or machine activity, the material being processed, foreseeable misuse, unexpected or expected behaviour of persons or equipment, actions of a third party, faults or failures that must happen or be in place for the accident to occur.

In some cases the operating mode or activity or material being processed are irrelevant to whether the accident occurs. In which case these should NOT be given as preconditions. In others a failure of the safety function may be completely harmless in most conditions and detected by a loss of utility except for a specific combination of activity, mode and process material. An example is the cleaning and sterilisation of food processing machinery by hot caustic liquid, where in normal operation the food is processed at room temperature. An incorrect discharge in this case only leads to a hazard during the cleaning process. Table G1 gives some examples of preconditions that, whilst not exhaustive, may be useful to refer to.

2) A person must potentially, at some time, be within range of the hazard. This may be quite different from the danger zone defined for other purposes, especially if material ejection is possible. If the three dimensional space considered to be within range of the hazard has not already been defined on Form 3 do so here and describe in the note associated with the accident scenario under consideration.

A person may be within range of a hazard for only a small amount of time. Although, on most occasions the failure of a safety function only results in a harmless loss of utility it is possible for the accident to occur if the failure occurs when a person is within range of the hazard. The form, therefore, needs to be completed taking this into account as described in the scenario frequency estimation step. An example of this is the automatic warehouse where the presence of people in the range of hazards is very limited.

3) This should give a comprehensive list of preconditions. Check that a precondition must occur in addition to all the other possible preconditions to make the accident possible. Delete any precondition that will occur directly because of another.

As an example, a failure leading to the uncovenanted activation of a laser; production hold state AND target alignment activity. If an OR condition exists between any two preconditions, for example target alignment activity OR changing work-piece activity, a new potential accident scenario must be defined and an additional Form 5 prepared i.e. one form to cover target alignment and one to cover changing work-piece.

It may be found that there is more than one way of defining the preconditions; providing the definitions are clear and no precondition is actually duplicated it does not matter which way is used.

4) Insert the list of preconditions remaining after this process in boxes 5.4.1 to 5.4.10.

Scenario Frequency Estimation

To estimate the frequency of the accident scenario, probabilities need to be assigned to all the preconditions.

Tables A.G2 and A.G3 can help in estimating probability. This probability should be an average over many occasions and many different examples within the Use Type and Person Type combination under consideration. Neither best case, nor worst case, nor even most typical case is wanted. Rather a probability should represent the likelihood of the state or event, taking place out of all possible occasions.

1) Refer to the Form 2's and 3's as well as the analysis that was used in 5.6.2. Consider the total involvement for this Person Type in the Use Type under consideration. Probabilities should relate to this involvement time.

2) Estimate the probability of the specific Person Type being in range of the hazard when it is generated. Enter this probability in box 5.4.11.

3) Estimate the probability of all other preconditions, using the guidance above and insert these values in boxes 5.4.12 to 5.4.20. For a precondition that relates to the failure of another electrical control function, restrictions are given, at the bottom of the form, of the lowest probability that can be used. These restrictions are required to accommodate the likelihood of common cause or similar systematic faults that are not controlled by the requirements of Clause 6 of the Standard. Assume the least favourable sequence of the appearance of faults, including simultaneity

4) Calculate the frequency of the potential accident (per hour) by multiplying the probability of a person being in range of the hazard (5.4.11) and all the precondition probabilities (5.4.12 to 5.4.20) together and then multiplying this figure by the assumed failure rate to danger of the safety function of $1x10^{-4}$ as instructed on the form. Enter the result in box 5.5.

5) Consider the other Use Type, Person Type and precondition set combinations for this accident. Next, decide whether any other combinations are likely to pose a similar (within one order of magnitude) or higher risk. If so, complete a Form 5 for these combinations.

6) When you are confident that the highest risk combination for this accident has been analysed, or there are no others to be analysed. Move on to the next accident scenario until at least one Form 5 has been completed for each FT accident defined in Form 3. All NFS scenarios should have been dealt with during step 4 above.

9.1.2.8 Step 6: Frequency of Different Severity Levels (Form 6)

The purpose of Form 6 is to record the range of severities and calculate the frequency of harm associated with each accident scenario. One Form 6 needs to be filled in for each completed Form 4 and Form 5.

1) Insert the safety function reference from box 4.1 of form 4 or box 5.1 of form 5 as appropriate in box 6.1 and mapping reference in box 6.2 made up of the Use Type and Person Type, accident number and type by deleting either NFS or FT as appropriate.

2) Enter the potential accident frequency from box 4.8 in Form 4 or box 5.5 in Form 5 in to box 6.3.

3) Consider the spread of outcomes that the accident scenario could give rise to for the specific Person Type, Use Type combination. Table A.G4 gives some practical examples of injury severity.

4) Consider the possible variations in factors that will affect the accident outcome. These can be timing, speed, position, machine settings, and even weather conditions if appropriate. Estimate the probability that the accident scenario will give rise to each of the severity categories defined below. Insert this probability into boxes 6.4.1 to 6.4.4.

Fatality and permanent serious disability: little chance of ever returning to near an accustomed quality of life (personal / work tasks that before the injury were taken for granted are now difficult to carry out).
Irreversible injury (major): some loss in the quality of life but could eventually lead a near normal life. Generally, these are those injuries that are immediately incapacitating.
Reversible injury (minor): no loss in the quality of life. No tasks would be any more problematic than before the injury. Generally injuries, where the victim is able to depart from the scene of the accident with the minimum of assistance usually fall into this category.

It is usually easiest to start with the no injury probability, which directs thinking towards ways in which injury is avoided or at least reduced, and then work upwards in severity. For many accident scenarios, it is possible to predict how the injury takes place in detail. Table A.G4 gives some practical examples of injury severity, but the detailed definition is given above:

5) Ensure that the total probability of all severity levels in boxes 6.4.1 to 6.4.4 add up to one. Calculate the frequency of harm for each severity level as instructed on the form and insert the answers in boxes 6.5.1 to 6.5.2. Repeat until a Form 6 has been filled in for all Form 4's and all Form 5's.

Note: The category definitions above and example injuries in Table A.G4 have been developed with reference to:
IEC 62061 CD2 © IEC 44/380/CD 64
Classification of Motor Vehicle Traffic Accidents, 5th Ed, National Safety Council, Illinois, USA, ANSI D16.1-1989
Coding of Work Injury or Disease Information, Z795-96, Canadian Standards Association
International Recommendations on Labour Statistics, ILO, Geneva, 1976
Swedish Injury Reporting Regulations
Australian workplace injuries compensation guide
UK Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995

9.1.2.9 Step 7: Harm Frequency Summation (Form 7)

One Form 7 is needed for each Use Type and Person Type combination for each safety function.

1) Insert the safety function reference from box 6.1 of form 6 in box 7.1 and mapping reference in box 7.2 made up of the Use Type and Person Type.

2) Transfer the frequency values of a fatal and permanent serious disability from all the Forms 6 relating to this use, person type combination into boxes 7.3.2 to 7.6.2.

3) Transfer the frequency values of an irreversible injury values from all the Forms 6 relating to this use, person type combination into boxes 7.3.3 to 7.6.3.

4) Transfer the frequency values of a reversible injury values from all the Forms 6 relating to this use, person type combination into boxes 7.3.4 to 7.6.4.

5) Sum the frequencies for each severity level and enter the values in boxes 7.7 to 7.9 as instructed on Form 7.

6) Calculate the required improvement factor for each severity level as instructed in Form 7 and enter the value in boxes 7.10 to 7.12.

7) Identify the highest improvement factor from boxes 7.10 to 7.12 and write this most onerous factor in box 7.13.

9.1.2.10 Step 8: SIL Assignment (Form 2 – Part 2)

1) Transfer the most onerous improvement factor from each Form 7 box 7.13 to the relevant Use Type/Person Type combination to the corresponding boxes 2.6.8 to 2.6.14 in Form 2 for the safety function under consideration. The relevant Use/Person type identifier for each improvement factor is entered in boxes 2.6.1 to 2.6.7.

2) Identify the highest value from boxes 2.6.8 to 2.6.14 and write it in box 2.7 of Form 2.

3) If the value is greater than 1, use the SIL requirement information to determine the SIL to assign and write the SIL in box 2.8.

9.1.2.11 Step 9: Continue analysis for all other safety functions

1) Repeat steps 2 to 8 until all the Forms 2, prepared at the end of step 1, have been completed.

2) Check that every safety-related control function in the Safety Requirement Specification now has a SIL assigned to it. If not modify Form 1 accordingly and repeat steps 2 to 8 as required.

9.1.2.12 Step 10: Plausibility Check

Prior to issuing the final comprehensive Safety Requirement Specification, wherever practicable check that the assigned SILs appear reasonable and in line with similar machines. Ensure that all relevant requirements appear consistent and comprehensive.

9.2 APPENDIX B: COPY OF FORMS INCLUDED IN ANNEX A OF IEC 62061

This appendix includes the latest version of forms as developed for inclusion in Annex A of IEC 62061. This version was current as of February 2003.

FORM 1: Machine and use characteristics relevant to functional safety

Machine type(s): Describe		*1.1*
Machine version: Describe		*1.2*
	Reference	**Name**
SRECS Safety Functions	*1.3.1*	*1.3.11*
	1.3.2	*1.3.12*
	1.3.3	*1.3.13*
	1.3.4	*1.3.14*
	1.3.5	*1.3.15*
	1.3.6	*1.3.16*
	1.3.7	*1.3.17*
	1.3.8	*1.3.18*
	1.3.9	*1.3.19*
	1.3.10	*1.3.20*
	Reference	**Notes**
Use type / circumstances	*1.4.1* **U1**	*1.4.5*
	1.4.2 **U2**	*1.4.6*
	1.4.3 **U3**	*1.4.7*
	1.4.4 **U4**	*1.4.8*
Person types	*1.5.1* **P1**	*1.5.6*
	1.5.2 **P2**	*1.5.7*
	1.5.3 **P3**	*1.5.8*
	1.5.4 **P4**	*1.5.9*
	1.5.5 **P5**	*1.5.10*
Activities of machine and persons:	*1.6.1*	*1.6.11*
	1.6.2	*1.6.12*
	1.6.3	*1.6.13*
	1.6.4	*1.6.14*
	1.6.5	*1.6.15*
	1.6.6	*1.6.16*
	1.6.7	*1.6.17*
	1.6.8	*1.6.18*
	1.6.9	*1.6.19*
	1.6.10	*1.6.20*
Special features: *list any special features and the relevant information*	*1.7.1*	*1.7.6*
	1.7.2	*1.7.7*
	1.7.3	*1.7.8*
	1.7.4	*1.7.9*
	1.7.5	*1.7.10*
Other: *record initial ideas of the possible accidents and the chain of events ...*	*1.8.1*	*1.8.9*
	1.8.2	*1.8.10*
	1.8.3	*1.8.11*
	1.8.4	*1.8.12*
	1.8.5	*1.8.13*
	1.8.6	*1.8.14*
	1.8.7	*1.8.15*
	1.8.8	*1.8.16*

FORM 2: Safety function Analysis

PART 1

SRECS safety function reference:	*2.1*		
Describe what the function does:	*2.2*		
	Ref.	**Notes**	
Use type / circumstances:	*2.3.1* **U_**	*2.4.1*	
	2.3.2 **U_**	*2.4.2*	
	2.3.3 **U_**	*2.4.3*	
Person types:	*2.3.4* **P_**	*2.4.4*	
	2.3.5 **P_**	*2.4.5*	
	2.3.6 **P_**	*2.4.6*	
Activities revealing failure to danger:	**Ref.**	**Description**	**Notes**
	2.5.1	*2.5.11*	*2.5.21*
	2.5.2	*2.5.12*	*2.5.22*
	2.5.3	*2.5.13*	*2.5.23*
	2.5.4	*2.5.14*	*2.5.24*
	2.5.5	*2.5.15*	*2.5.25*
	2.5.6	*2.5.16*	*2.5.26*
	2.5.7	*2.5.17*	*2.5.27*
	2.5.8	*2.5.18*	*2.5.28*
	2.5.9	*2.5.19*	*2.5.29*
	2.5.10	*2.5.20*	*2.5.30*

PART 2

Combination Reference: U_…. P_	**Required improvement factor: #**	
2.6.1	*2.6.8*	
2.6.2	*2.6.9*	
2.6.3	*2.6.10*	
2.6.4	*2.6.11*	
2.6.5	*2.6.12*	
2.6.6	*2.6.13*	
2.6.7	*2.6.14*	
SIL requirement information: Relationship between the required improvement and SIL. **Factor** **SIL** ≥1 to <10 1 ≥10 to <100 2 ≥100 to <1000 3	**Highest required improvement factor:** Write the highest of the numbers from [2.6.8 to 2.6.14] in [2.7].	*2.7*
	Assigned SIL: Compare the value in [2.7], the required improvement factor, with the information to the left to infer the SIL requirement. Write the required SIL in [2.8].	*2.8*

FORM 3: Accident Analysis and Potential Accident Scenarios

SRECS safety function reference: *3.1*				
Accident Reference:	**Accident description:**	**Notes**	**FT/ NFS**	**Combination**
3.2.1 **#1**	*3.2.2*	*3.2.3*	*3.2.4*	*3.2.5* **U_ P_**
				3.2.6 **U_ P_**
				3.2.7 **U_ P_**
				3.2.8 **U_ P_**
				3.2.9 **U_ P_**
3.3.1 **#2**	*3.3.2*	*3.3.3*	*3.3.4*	*3.3.5* **U_ P_**
				3.3.6 **U_ P_**
				3.3.7 **U_ P_**
				3.3.8 **U_ P_**
				3.3.9 **U_ P_**
3.4.1 **#3**	*3.4.2*	*3.4.3*	*3.4.4*	*3.4.5* **U_ P_**
				3.4.6 **U_ P_**
				3.4.7 **U_ P_**
				3.4.8 **U_ P_**
				3.4.9 **U_ P_**
3.5.1 **#4**	*3.5.2*	*3.5.3*	*3.5.4*	*3.5.5* **U_ P_**
				3.5.6 **U_ P_**
				3.5.7 **U_ P_**
				3.5.8 **U_ P_**
				3.5.9 **U_ P_**

FORM 4: NFS accident calculation

SRECS safety-related control function reference:	*4.1*
Mapping reference:	*4.2* **U….. P …..NFS**
Accident identification number:	*4.3* **# ……**
Datum event: *Description*	*4.4.1*
	Value
Calculated datum event frequency (per hour):	*4.4.2*
Preconditions	**Precondition probability** **Value (range 0 – 1)**
4.5.1	*4.5.11*
4.5.2	*4.5.12*
4.5.3	*4.5.13*
4.5.4	*4.5.14*
4.5.5	*4.5.15*
4.5.6	*4.5.16*
4.5.7	*4.5.17*
4.5.8	*4.5.18*
4.5.9	*4.5.19*
4.5.10	*4.5.20*
Note: When included as a precondition, the probability of another function of the Electrical Control System being failed to danger must be set to a minimum of 0.1 for functions specified as SRECS safety functions or otherwise a minimum of 0.35. This restriction is required to accommodate the likelihood of common cause or similar systematic faults that are not controlled by the requirements of Clause 6. Assume the least favourable sequence of the appearance of faults, including simultaneity.	
Calculated demand event frequency: *(A)* Multiply together the datum event frequency and all the precondition probabilities.	*4.6*

FTD maximum exposure frequency for this Use Type (per hour): (*B*)	*4.7*
Frequency of potential accident (per hour): (*C*)	*4.8*

Note: When included as a precondition, the probability of another function of the Electrical Control System being failed to danger must be set to a minimum of 0.1 for functions specified as SRECS safety functions or otherwise a minimum of 0.35. This restriction is required to accommodate the likelihood of common cause or similar systematic faults that are not controlled by the requirements of Clause 6. Assume the least favourable sequence of the appearance of faults, including simultaneity.

$$C = A \cdot \left(\frac{10^{-4}}{2 \cdot B} \right)$$ or in words:

(Frequency of potential accident (per hour)) = (Calculated demand event frequency) X (10E^{-4} / (2 * (FTD exposure frequency))

FORM 5: FT accident calculation

SRECS safety function reference	*5.1*
Mapping reference:	*5.2* **U….. P …..FT**
Accident identification number:	*5.3* **# ……**
Assumed failure rate to danger for SRECS safety-related control function (per hour):	**10^{-4}**
Preconditions	**Precondition probability Value (range 0 – 1)**
5.4.1 ***Person in range of hazard***	*5.4.11*
5.4.2	*5.4.12*
5.4.3	*5.4.13*
5.4.4	*5.4.14*
5.4.5	*5.4.15*
5.4.6	*5.4.16*
5.4.7	*5.4.17*
5.4.8	*5.4.18*
5.4.9	*5.4.19*
5.4.10	*5.4.20*
Frequency of potential accident (per hour of involvement):	*5.5*

Note: When included as a precondition, the probability of another function of the Electrical Control System being failed to danger must be set to a minimum of 0.1 for functions specified as SRECS safety functions or otherwise a minimum of 0.35. This restriction is required to accommodate the likelihood of common cause or similar systematic faults that are not controlled by the requirements of Clause 6. Assume the least favourable sequence of the appearance of faults, including simultaneity

FORM 6: Frequency of harm

SRECS safety function reference		*6.1*	
Mapping reference:		*6.2* **U….. P …..#……NFT/FT* ….. of …** *delete as appropriate	
Frequency of potential accident (per hour):		*6.3*	
Severity level	**Probability of harm of specific severity**	**Frequency of harm**	
	Value	**Instructions**	**Value**
Fatal and permanent serious disability	*6.4.1*	Multiply the value in [6.4.1] by the value in [6.3] and write the result in [6.5.1].	*6.5.1*
Irreversible	*6.4.2*	Multiply the value in [6.4.2] by the value in [6.3] and write the result in [6.5.2].	*6.5.2*
Reversible	*6.4.3*	Multiply the value in [6.4.3] by the value in [6.3] and write the result in [6.5.2].	*6.5.3*
No Injury including near miss	*6.4.4*		
Total: sum must equal 1	**1**		

FORM 7: Calculation of required improvement factor

Safety Function reference:	*7.1*		
Mapping reference:	*7.2* **U….. P …..**		
Accident Identification number	Frequency of given severity		
	Fatal and permanent serious disability: enter value from [6.5.1] into the relevant row.	**Irreversible:** enter value from [6.5.2] into the relevant row.	**Reversible:** enter value from [6.5.3] into the relevant row.
7.3.1 **#….**	*7.3.2*	*7.3.3*	*7.3.4*
7.4.1 **#….**	*7.4.2*	*7.4.3*	*7.4.4*
7.5.1 **#….**	*7.5.2*	*7.5.3*	*7.5.4*
7.6.1 **#….**	*7.6.2*	*7.6.3*	*7.6.4*
Total frequency for a given severity over all accidents:	*7.7* Sum of above	*7.8* Sum of above	*7.9* Sum of above

Severity level	**Required factor improvement in SRECS safety function failure rate to danger**	
	Instructions	**Value**
Fatal and permanent serious disability	Multiply the value in [7.7] by 10^{10} and write in [7.10]	*7.10*
Irreversible	Multiply the value in [7.8] by 10^{9} and write in [7.11]	*7.11*
Reversible	Multiply the value in [7.9] by 10^{8} and write in [7.12]	*7.12*
Most onerous improvement factor	Take the maximum value from [7.10 to 7.12] and write in [7.12]	*7.13*

Table A.G1: Examples of pre-conditions

NOTE Pre-conditions can be considered to be a part of the sequence of events that can lead to a potential accident. The examples given below are non-exhaustive and on their own are generally insufficient to fully define the pre-conditions for use in this methodology.

Category	Examples
Human (any human related action or omission) Take into account time pressures, piecework and production deadlines, which may result in a temptation to take short cuts.	Failure to isolate Machine left running Misuse Lack of/inappropriate PPE Misuse of safety systems as part of normal operation – e.g. interlock as on/off switch, or emergency stop as operational stop etc. Trips/slips and falls Inappropriate clothing Ignoring stated procedures Wrong material/work piece Inappropriate manual intervention
Environment (the type of environmental conditions in which the machine is being operated)	Adequacy of lighting Adequacy of access Extreme temperature Mechanical instability of machine Explosive atmosphere exists Noise/Vibration Weather conditions
Machine Condition	Mechanical defects Inadequately and uninsulated cables Damaged cables Cracks in pipes Poorly carried out maintenance Lack of maintenance/inspection Inadequately fitted guards
Operation of machine (the mode in which the machine must be operating)	Speed/inertia/momentum of some part of machine Stored energy e.g. mass being lifted or pipe work/hose/vessel pressurised Unexpected or aberrant machine operation - unexpected operation in wrong cycle Inadequate stopping performance
Other	Blockage in machine Anything else not in above list

Table A.G2 Proposed probability values

Probability	Description
1	Occurs continuously
10^{-1}	Frequent
10^{-2}	Probable
10^{-3}	Occasional

Table A.G3 Probability of human error

Error probability	Task
$10^{-5} – 10^{-6}$	Routine, good feedback with time to make use of it, good appreciation of hazard
0.001	Routine, simple
0.01	General error of omission
0.1	Non-routine, complicated
0.1	High stress, time constraint 30 minutes
0.9	High stress, time constraint 5 minutes
1	High stress, time constraint 1 minute
1	Error in second step, having already erred in first

Table A.G4 Severity level definitions

Severity level	Example injuries
Fatality and permanent serious disability	- Quadriplegia - Paraplegia - Prolonged unconsciousness (coma) - Permanent brain damage
Irreversible injury (major)	- Any fracture (other than to fingers, thumbs or toes) - Burns causing permanent scarring - Damage to sight partial or total - Any amputation - Loss of consciousness (not prolonged) - Dislocation of the shoulder, hip, knee or spine - Treatment required due to fume exposure - Anything requiring resuscitation
Reversible injury (minor)	- Minor broken bones (fingers, toes) - Cuts and bruises - Minor burns, temporary scarring - Anything else requiring first aid only
No injury and near misses	- no injury including the possibility of avoidance

9.3 APPENDIX C: RELATING RISK TO PERSONS

The relationship between the chosen limit values and the total work related risk exposure of a professional machine user is examined and tentatively calculated in Section 9.3.2 below. Machine risk to non-professional users is estimated using further assumptions. The assumptions and uncertainties underlying the calculations are explored.

9.3.1 Theory

The maximum value allowed for the risk from each function is not the typical or average value that is achieved in practice. As the rate of dangerous failure assumed in the risk estimation is the most pessimistic within an integrity band one decade wide, and risk reduction proceeds in decade steps, the resulting risk lies in the range of 0.01-1.00 of the limit value for the most unfavourable combination of Use Type and Person Type. A specific Person Type in a particular Use Type will not be the most unfavourable combination for every function, so will not exposed to the greatest risk from all of the SRECS safety functions. Summation of the risks to a person needs to accommodate the foregoing factors.

The risks arising from faults in the electrical control system of the machine do not constitute the integral risk to the machine user. There will always be additional risks associated with the machine itself, the location/installation and ancillary activities. The relative contribution of SRECS risks varies widely between types. In order to arrive at a meaningful result a contribution of 10% is assumed, as a conservative estimate for current, automated production machinery without significant, dominant risks. This proportion is intended to be a best estimate in circumstances where all machine risks have been made insignificant according to ISO 12100-1 and the other work related risks are of similar scale. Some machines cannot achieve such a low level of risk because of technical restrictions on protective measures and for work with such machines a higher integral risk is to be expected. Annex 4 of the Machinery Directive contains examples of such machines.

Not all SILs are set by outcome harm severity including fatality. This methodology does not sum risk of different severities so true fatality equivalent greater than that calculated by summing the values achieved for the most demanding harm outcome. The distribution of outcomes is variable between accident scenarios. In order to allow for the increase in risk when all outcomes are combined, a multiplier or 2 is selected as a conservative estimate.

It is estimated that fatal outcome represents 20% of all the risk, but is the only outcome recorded unambiguously.

9.3.2 Calculations

9.3.2.1 Professional worker

An annual work time of 1750 hours is assumed. This estimate is to accommodate holidays and sickness together with an allowance for overtime.

Machine SRECS sourced risks are estimated at one tenth of the sum of the integral risk from working.

The number of relevant SRECS functions is estimated at 25.

The factor to accommodate exposure to less than the greatest risk for a proportion of the functions is estimated at 0.85.

The distribution of SRECS safety function risk is assumed to be linear prior to mitigation.

The distribution of probability of failure to danger of a function realised in accordance with the requirements for a specific SIL is assumed to be linear within the band corresponding to the SIL.

The limit value for the risk of a single safety function for the most unfavourable combination is set by the methodology at $1x10^{-10}$ fatality equivalent harm per hour.

A factor of 2 is estimated as the multiplier to average the summation of risk from the 3 harm severity outcomes.

1750 [hours] x 25 [number of functions] x 0.8 [less than greatest risk from a proportion of the functions] x $1x10^{-10}$ [fatality equivalent risk limit] x 2 [summation of harm outcomes] x 0.55 [average limit of risk after SIL assigned] x 0.55 [average probability of failure to danger rate ⁄□ maximum for SIL] x 10 [whole work multiplier] x 0.2 [fatalities per fatality equivalent risk unit] = number of fatalities expected per year in safe industry = $4.2x10^{-6}$.

This would assume no worse than reasonably foreseeable misuse within a managed health and safety environment. Result is that overall input from machine related risk under the condition that safety is aiming for is just at boundary of broadly acceptable / ALARP boundary like fire or gas explosion at home. Fatal outcome represents 15% of all the risk, but is the only outcome rigorously recorded.

In real industry there are many more fatalities from falls and hit by objects and similar that cannot be affected by machine safety by design and relate to the users not organising the work process properly.

9.3.2.2 Casual domestic user

Applying similar assumptions other than 75 hours involvement per year, the final result is $1.8x10^{-7}$ fatalities per annum.

9.3.3 Discussion

The calculated value for fatalities in safe industry is $4.2x10^{-6}$, compared with the currently accepted value of $1x10^{-5}$ for the safest parts of industry. The calculated value assumes an idealised situation in which all risks are mitigated sufficiently to eliminate them from the significant risk category of ISO 12100-1. Given the inevitable difference between the ideal and the practicable, there is good correlation between the calculated and measured values. Examination of industrial accident statistics indicates a proliferation of fatalities from falls or persons struck by moving objects. The rate of accidents from hazards of machines, arising directly at the machines, appears to accord well with the calculations.

The increase in probability of fatality calculated for a domestic user of a safe machine 75 hours a year, $4.5x10^{-8}$ per annum. This compares with a ‘background’ level of $1x10^{-6}$, suggesting that the domestic use of machines carries a finite but not dominant risk. It has not been possible to obtain unambiguous recorded data to allow for a direct comparison of the calculated result with reality.

The calculations provide an indication that the risk limit value selected for the methodology is reasonably in accordance with the level of safety corresponding to current good practice.

10 REFERENCES

1 IEC 62061 "Safety of machinery – functional safety of electrical, electronic and programmable control systems for machinery"
Committee Draft 44/380/CD, May 2002

2 ISO 14118 (EN 1037:1996)
Safety of machinery - prevention of unexpected start-up

3 IEC 60204-1:1997
Safety of machinery. Electrical equipment of machines. General requirements

4 IEC 61508:2002 "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"

5 F. Redmill, 2000
Safety Integrity Levels - theory and problems
Proceedings of 8th Safety-critical Systems Symposium: Lessons in System Safety

6 ISO 13849-1 (EN 954)
Safety of machinery – safety related parts of control systems
Part 1. General principles for design

7 ISO 14121:1999 (EN 1050)
Safety of machinery – Principles for risk assessment

8 IEC 61496 Safety of machinery - electro-sensitive protective equipment.
-Part 1: 1997 General requirements and tests
-Part 2: 1997 Safety of machinery - Electro-sensitive protective equipment. Particular requirements for equipment using active opto-electronic protective devices (AOPDs)
-Part 3: 2001 Safety of machinery -Electro-sensitive protective equipment. Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)

9 ISO/TR 12100:1992 (EN 292)
Safety of machinery – basic concepts, general principles for design

10 IEC 62046: Safety of machinery - Application of personnel sensing protection equipment to machinery (PSPE) Committee draft 44/377/CD

11 ISO/IEC Guide 51:1999

12 BS 8800:1996
Guide to occupational health and safety management systems

13 H. Raafat and R Nicolas 2001
Root cause analysis of non-compliance with the EC Machinery Directive
Journal of the Institution of Occupational Safety and Health Vol. 5, Issue 2

14 N. Worsell, A. J. Wilday and D. Keeley 1997
The Application of Risk Assessment to Machinery Safety, Final Report
HSL Internal Report RAS/97/14

15 IEC 61511-3
Functional safety of safety instrumented systems for the process industry sector, part 3 guidance for the determination of safety integrity levels – informative, CDV July 2000

16 IEC 61513:2001
Nuclear power plants. Instrumentation and control for systems important to safety. General requirements for systems

17 prEN 50129:2000
Railway Applications - Safety Related Electronic Systems for Signalling

18 IEC 60601-1-4:1996
Medical electrical equipment. General requirements for safety. Collateral standard. General requirements for programmable electrical medical systems

19 MISRA, 1994
Development guidelines for vehicle based software
ISBN 0952415607

20 M.L. Shooman,
Probabilistic reliability: an engineering approach
McGraw-Hill (1968) pp. 170-185.

21 Bhimavarapu, K and Stavrianidis, P, 2000
Safety Integrity Level analysis for processes: issues and methodologies
Process Safety Progress, Vol 19, No 1

22 Gallagher, V A Jnr, 1999
Motivating management, when cost benefit analysis fails
Professional Safety, May, Vol 44, No 5

23 HSE Books 2001
Reducing risks, protecting people, HSE’s decision-making process
ISBN 0-7176-2151-0

24 HSE Books, revised 1992
The tolerability of risk from nuclear power stations
ISBN 0-11-886368-1

25 HSE
Risk criteria for land-use planning in the vicinity of major hazards
HMSO, 1989.

26 H. Raafat
Machinery safety: the risk based approach, practical guidelines on risk assessment, standards and legislation.
Technical Communications (Publishing) Ltd, 1995.

27 S.B. Warren and T.M. Amundson
Comprehensive baseline hazard assessments – a team approach
Professional Safety, July 1995.

28 BS 5304:1988, obsolete
British Standard Code of practice for safety of machinery.

Printed and published by the Health and Safety Executive
C1.10   04/04

HSE
BOOKS

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from booksellers

HEALTH AND SAFETY INFORMATION
HSE Infoline
Tel: 08701 545500
Fax: 02920 859260
e-mail: hseinformationservices@natbrit.com
or write to:
HSE Information Services
Caerphilly Business Park
Caerphilly CF83 3GG

HSE website: www.hse.gov.uk

RR 216

£15.00

ISBN 0-7176-2832-9

9 780717 628322