IEC 61508-5

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité

IEC 61508-5:2010

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61508-5

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 25.040.40

ISBN 978-2-88910-528-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 5: Examples of methods for the determination of safety integrity levels

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1998. This edition constitutes a technical revision.

This edition has been subject to a thorough review and incorporates many comments received at the various revision stages.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/552/FDIS	65A/576/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.

NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are given in the Bibliography (see references [1], [2] and [3]).

In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future product and application sector international standards and in revisions of those that already exist.

This International Standard

– considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, though design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
– has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
– enables product and application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
– provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
– adopts a risk-based approach by which the safety integrity requirements can be determined;
– introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 2 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

– sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in

  – a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5};

  – a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

– sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;

– introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 5: Examples of methods for the determination of safety integrity levels

1 Scope

1.1 This part of IEC 61508 provides information on

– the underlying concepts of risk and the relationship of risk to safety integrity (see Annex A);

– a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems to be determined (see Annexes C, D, E, F and G).

The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes C, D, E, F and G illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account. Those intending to apply the methods indicated in these annexes should consult the source material referenced.

NOTE For more information on the approaches illustrated in Annexes B, and E, see references [5] and [8] in the Bibliography. See also reference [6] in the Bibliography for a description of an additional approach.

1.2 IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.3 One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-5 plays in the achievement of functional safety for E/E/PE safety-related systems.

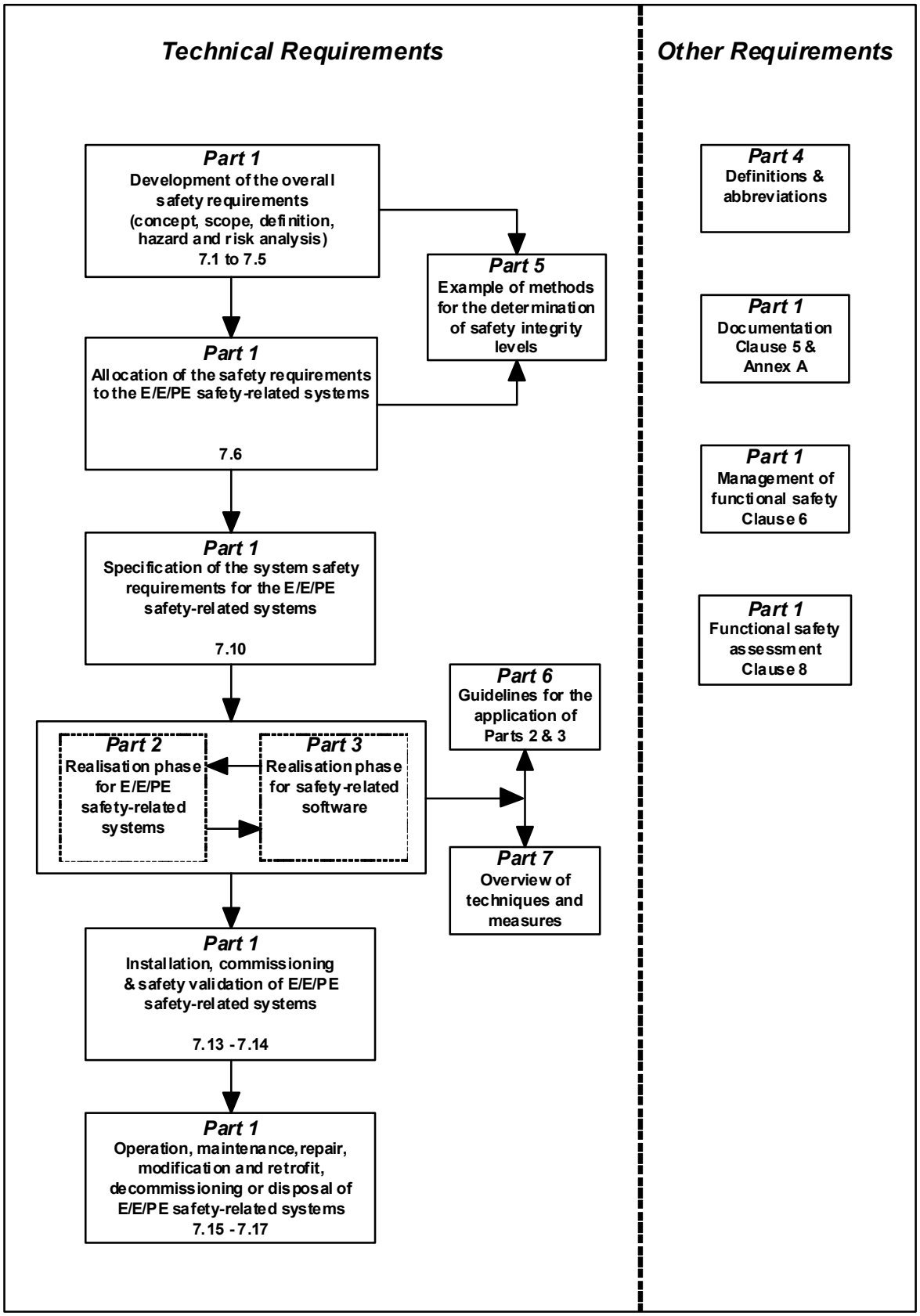


Figure 1 – Overall framework of the IEC 61508 series

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in IEC 61508-4 apply.

Annex A
(informative)

Risk and safety integrity – General concepts

A.1 General

This annex provides information on the underlying concepts of risk and the relationship of risk to safety integrity.

A.2 Necessary risk reduction

The necessary risk reduction (see 3.5.18 of IEC 61508-4) is the reduction in risk that has to be achieved to meet the tolerable risk for a specific situation (which may be stated either qualitatively[1] or quantitatively[2]). The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event.

The tolerable risk will depend on many factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). Important factors will be the perception and views of those exposed to the hazardous event. In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered. These include:

– legal requirements, both general and those directly relevant to the specific application;
– guidelines from the appropriate safety regulatory authority;
– discussions and agreements with the different parties involved in the application;
– industry standards and guidelines;
– international discussions and agreements; the role of national and international standards is becoming increasingly important in arriving at tolerable risk criteria for specific applications;
– the best independent industrial, expert and scientific advice from advisory bodies.

In determining the safety integrity requirements of the E/E/PE safety-related system(s) and other risk reduction measures, in order to meet the tolerable frequency of a hazardous event, account needs to be taken of the characteristics of the risk that are relevant to the application. The tolerable frequency will depend on the legal requirements in the country of application and on the criteria specified by the user organisation. Issues that may need to be considered together with how they can be applied to E/E/PE safety-related systems are discussed below.

---

1 In achieving the tolerable risk, the necessary risk reduction will need to be established. Annexes E and G of this document outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly by specification of the SIL requirement rather than stated explicitly by a numeric value of risk reduction required.

2 For example, that the hazardous event, leading to a specific consequence, shall not occur with a frequency greater than one in 10^8 h.

A.2.1 Individual risk

Different targets are usually defined for employees and members of the public. The target for individual risk for employees is applied to the most exposed individual and may be expressed as the total risk per year arising from all work activities. The target is applied to a hypothetical person and therefore needs to take into account the percentage of time that the individual spends at work. The target applies to all risks to the exposed person and the tolerable risk for an individual safety function will need to take account of other risks.

Assurance that the total risk is reduced below a specified target can be done in a number of ways. One method is to consider and sum all risks to the most exposed individual. This may be difficult in cases where a person is exposed to many risks and early decisions are needed for system development. An alternative approach is to allocate a percentage of the overall individual risk target to each safety function under consideration. The percentage allocated can usually be decided from previous experience of the type of facility under consideration.

The target applied to an individual safety function should also take into account the conservatism of the method of risk analysis used. All qualitative methods such as risk graphs involve some evaluation of the critical parameters that contribute to risk. The factors that give rise to risk are the consequence of the hazardous event and its frequency. In determining these factors a number of risk parameters may need to be taken into account such as a vulnerability to the hazardous event, number of people who may be affected by the hazardous event, the probability that a person is present when the hazardous event occurs (i.e. occupancy) and probability of avoiding the hazardous event.

Qualitative methods generally involve deciding if a parameter lies within a certain range. The descriptions of the criteria when using such methods will need to be such that there can be a high level of confidence that the target for risks is not exceeded. This can involve setting range boundaries for all parameters so applications with all parameters at the boundary condition will meet the specified risk criteria for safety. This approach to setting the range boundaries is very conservative because there will be very few applications where all parameters will be at the worst case of the range. If members of the public are to be exposed to risk from failure of a E/E/PE safety-related system then a lower target will normally apply.

A.2.2 Societal risk

This arises where multiple fatalities are likely to arise from single events. Such events are called societal because they are likely to provoke a socio-political response. There can be significant public and organisational aversion to high consequence events and this will need to be taken into consideration in some cases. The criterion for societal risk is often expressed as a maximum accumulated frequency for fatal injuries to a specified number of persons. The criterion is normally specified in the form of one or more lines on an F/N plot where F is the cumulative frequency of hazards and N the number of fatalities arising from the hazards. The relationship is normally a straight line when plotted on logarithmic scales. The slope of the line will depend on the extent to which the organisation is risk averse to higher levels of consequence. The requirement will be to ensure the accumulated frequency for a specified number of fatalities is lower than the accumulated frequency expressed in the F/N plot. (see reference [7] in the Bibliography)

A.2.3 Continuous improvement

The principles of reducing risk to as low as reasonably practicable are discussed in Annex C.

A.2.4 Risk profile

In deciding risk criteria to be applied for a specific hazard, the risk profile over the life of the asset may need to be considered. Residual risk will vary from low just after a proof test or a repair has been performed to a maximum just prior to proof testing. This may need to be taken into consideration by organisations that specify the risk criteria to be applied. If proof test intervals are significant, then it may be appropriate to specify the maximum hazard

probability that can be accepted just prior to proof testing or that the PFD(t) or PFH(t) is lower than the upper SIL boundary more than a specified percentage of the time (e.g. 90 %).

A.3 Role of E/E/PE safety-related systems

E/E/PE safety-related systems contribute towards providing the necessary risk reduction in order to meet the tolerable risk.

A safety-related system both

– implements the required safety functions necessary to achieve a safe state for the equipment under control or to maintain a safe state for the equipment under control; and

– is intended to achieve, on its own or with other E/E/PE safety-related systems or other risk reduction measures, the necessary safety integrity for the required safety functions (3.5.1 of IEC 61508-4).

NOTE 1 The first part of the definition specifies that the safety-related system must perform the safety functions which would be specified in the safety functions requirements specification. For example, the safety functions requirements specification may state that when the temperature reaches x, valve y shall open to allow water to enter the vessel.

NOTE 2 The second part of the definition specifies that the safety functions must be performed by the safety-related systems with the degree of confidence appropriate to the application, in order that the tolerable risk will be achieved.

A person could be an integral part of an E/E/PE safety-related system. For example, a person could receive information, on the state of the EUC, from a display screen and perform a safety action based on this information.

E/E/PE safety-related systems can operate in a low demand mode of operation or high demand or continuous mode of operation (see 3.5.16 of IEC 61508-4).

A.4 Safety integrity

Safety integrity is defined as the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time (3.5.4 of IEC 61508-4). Safety integrity relates to the performance of the safety-related systems in carrying out the safety functions (the safety functions to be performed will be specified in the safety functions requirements specification).

Safety integrity is considered to be composed of the following two elements.

– Hardware safety integrity; that part of safety integrity relating to random hardware failures in a dangerous mode of failure (see 3.5.7 of IEC 61508-4). The achievement of the specified level of safety-related hardware safety integrity can be estimated to a reasonable level of accuracy, and the requirements can therefore be apportioned between subsystems using the normal rules for the combination of probabilities. It may be necessary to use redundant architectures to achieve adequate hardware safety integrity.

– Systematic safety integrity; that part of safety integrity relating to systematic failures in a dangerous mode of failure (see 3.5.6 of IEC 61508-4). Although the mean failure rate due to systematic failures may be capable of estimation, the failure data obtained from design faults and common cause failures means that the distribution of failures can be hard to predict. This has the effect of increasing the uncertainty in the failure probability calculations for a specific situation (for example the probability of failure of a safety-related protection system). Therefore a judgement has to be made on the selection of the best techniques to minimise this uncertainty. Note that it is not the case that measures to reduce the probability of random hardware failure will have a corresponding effect on the probability of systematic failure. Techniques such as redundant channels of identical hardware, which are very effective at controlling random hardware failures, are of little use in reducing systematic failures such as software errors.

A.5 Modes of operation and SIL determination

The mode of operation relates to the way in which a safety function is intended to be used with respect to the frequency of demands made upon it which may be either:

– **low demand mode:** where frequency of demands for operation made on the safety function is no greater than one per year; or

– **high demand mode:** where frequency of demands for operation made on the safety function is greater than one per year; or

– **continuous mode:** where demand for operation of the safety function is continuous.

Tables 2 and 3 of IEC 61508-1 detail the target failure measures associated with the four safety integrity levels for each of the modes of operation. The modes of operation are explained further in the following paragraphs.

A.5.1 Safety integrity and risk reduction for low demand mode applications

The required safety integrity of the E/E/PE safety-related systems and other risk reduction measures shall be of such a level so as to ensure that:

– the average probability of failure on demand of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk; and/or

– the safety-related systems modify the consequences of failure to the extent required to meet the tolerable risk.

Figure A.1 illustrates the general concepts of risk reduction. The general model assumes that:

– there is an EUC and a control system;

– there are associated human factor issues;

– the safety protective features comprise:

  – E/E/PE safety-related systems;

  – other risk reduction measures.

NOTE Figure A.1 is a generalised risk model to illustrate the general principles. The risk model for a specific application will need to be developed taking into account the specific manner in which the necessary risk reduction is actually being achieved by the E/E/PE safety-related systems and/or other risk reduction measures. The resulting risk model may therefore differ from that shown in Figure A.1.

The various risks indicated in Figure A.1 and A.2 are as follows:

– EUC risk: the risk existing for the specified hazardous events for the EUC, the EUC control system and associated human factor issues: no designated safety protective features are considered in the determination of this risk (see 3.1.9 of IEC 61508-4);

– tolerable risk; the risk which is accepted in a given context based on the current values of society (see 3.1.7 of IEC 61508-4);

– residual risk: in the context of this standard, the residual risk is that remaining for the specified hazardous events for the EUC, the EUC control system, human factor issues but with the addition of, E/E/PE safety-related systems and other risk reduction measures (see also 3.1.7 of IEC 61508-4).

The EUC risk is a function of the risk associated with the EUC itself but taking into account the risk reduction brought about by the EUC control system. To prevent unreasonable claims for the safety integrity of the EUC control system, this standard places constraints on the claims that can be made (see 7.5.2.5 of IEC 61508-1).

The necessary risk reduction is achieved by a combination of all the safety protective features. The necessary risk reduction to achieve the specified tolerable risk, from a starting

point of the EUC risk, is shown in Figure A.1 (relevant for a safety function operating in low demand mode of operation).

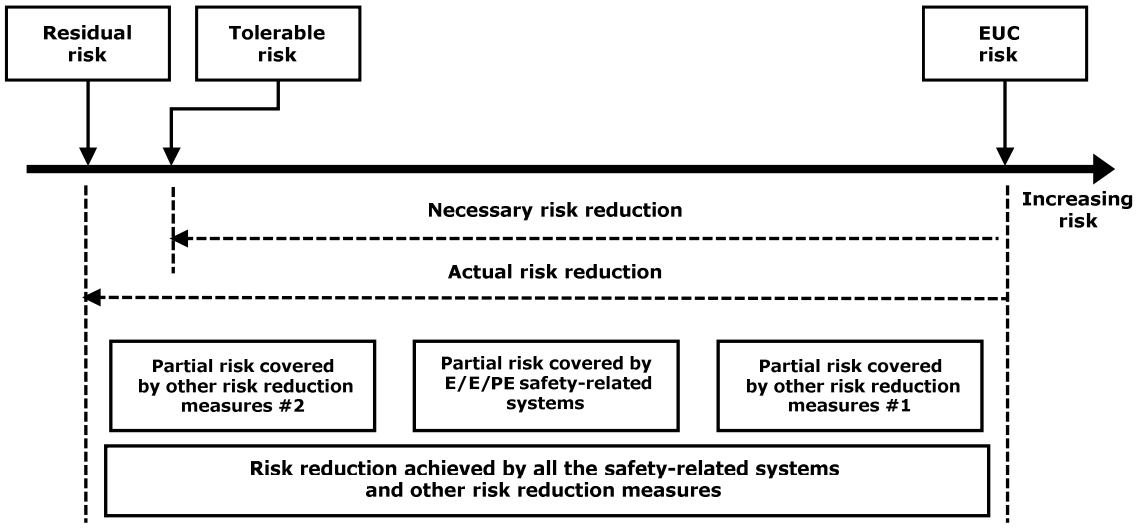


Figure A.1 – Risk reduction – general concepts (low demand mode of operation)

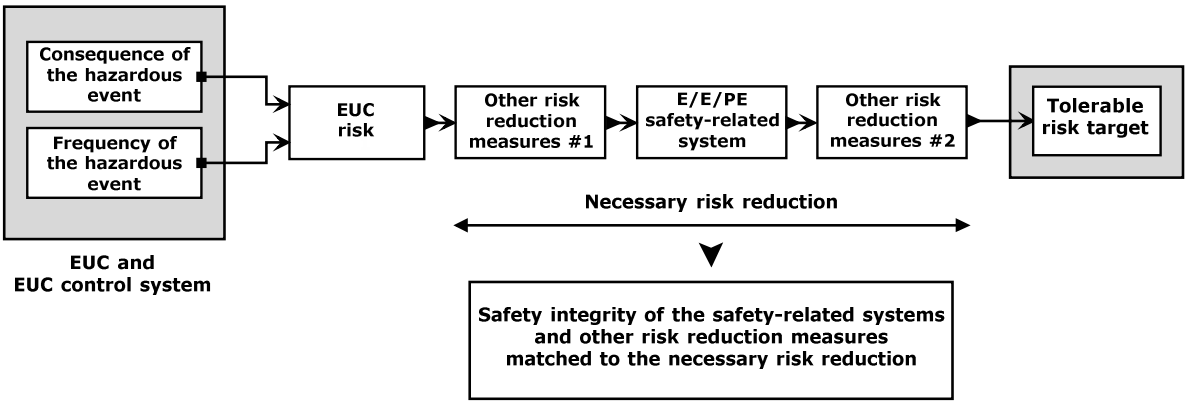


Figure A.2 – Risk and safety integrity concept

A.5.2 Safety integrity for high demand mode applications

The required safety integrity of the E/E/PE safety-related systems and other risk reduction measures shall be of such a level to ensure that:

– the average probability of failure on demand of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk; and/or

– the average probability of failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk.

Figure A.3 illustrates the general concepts of high demand applications. The general model assumes that:

– there is a EUC and a control system;

– there are associated human factor issues;
– the safety protective features comprise:
  – E/E/PE safety-related system operating in high demand mode;
  – other risk reduction measures.

Various demands on the E/E/PE safety related systems can occur as follows:

– general demands from the EUC;
– demands arising from failures in the EUC control system;
– demands arising from human failures.

If the total demand rate arising from all the demands on the system exceeds 1 per year then the critical factor is the dangerous failure rate of the E/E/PE safety-related system. Residual hazard frequency can never exceed the dangerous failure rate of the E/E/PE safety-related system. It can be lower if other risk reduction measures reduce the probability of harm.

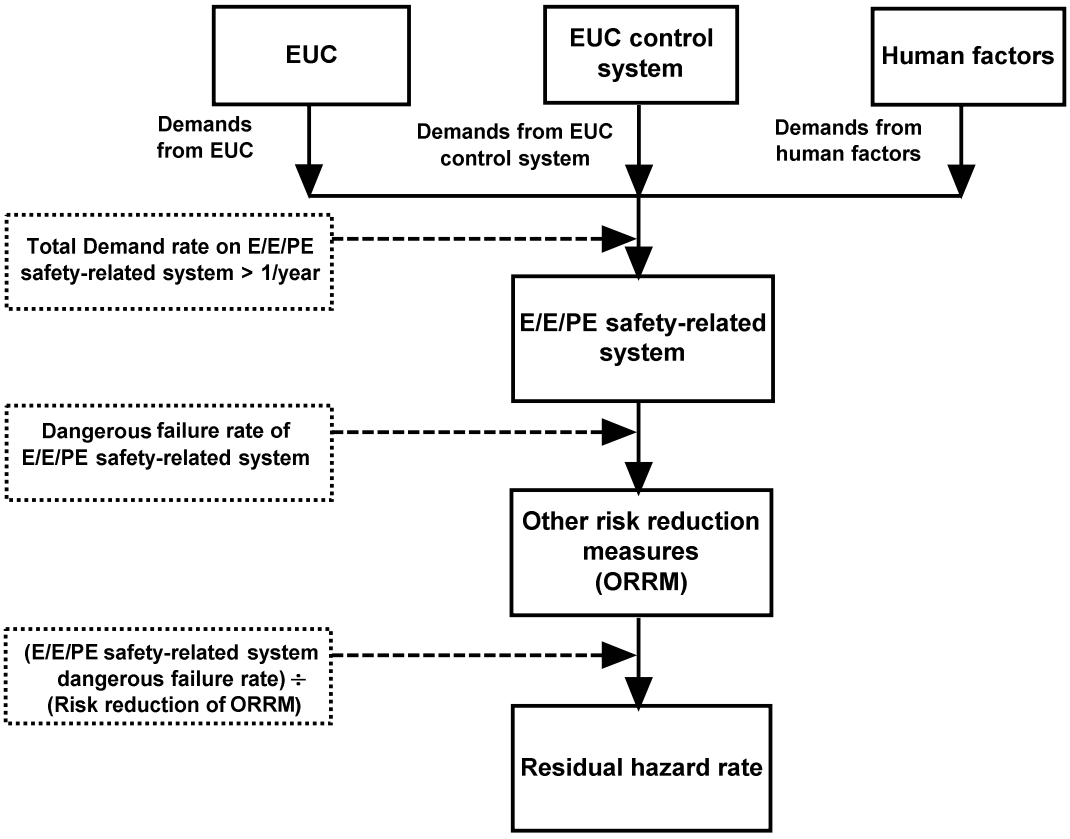


Figure A.3 – Risk diagram for high demand applications

A.5.3 Safety integrity for continuous mode applications

The required safety integrity of the E/E/PE safety-related systems and any other risk reduction measures shall be of such a level to ensure that the average probability of a dangerous failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk.

With an E/E/PE safety-related system operating in continuous mode, other risk reduction measures can reduce the residual hazard frequency according to the risk reduction provided The model is shown in Figure A.4.

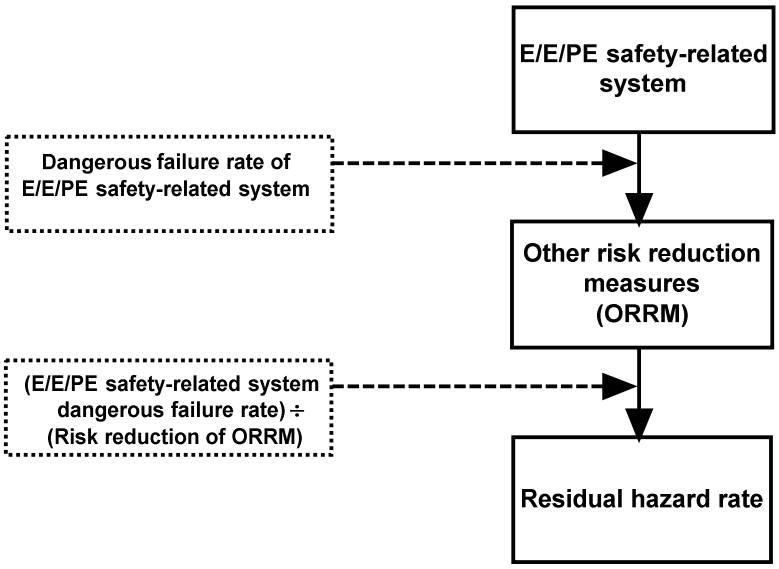


Figure A.4 – Risk diagram for continuous mode operation

A.5.4 Common cause and dependency failures

During the determination of the safety integrity levels it is important to take account of common cause and dependency failures. The models shown above in Figures A.1, A.2, A.3 and A.4 are drawn on the basis that each safety system relevant to the same hazard is fully independent. There are many applications where this is not the case. Examples include the following:

1) Where a dangerous failure of an element within the EUC control system can cause a demand on a safety-related system and the safety-related system uses an element subject to failure from the same cause. An example of this could be where the control and protection system sensors are separate but common cause could lead to failure of both (see Figure A.5).
2) Where more than one safety-related system is used and some of the same type of equipment is used within each safety-related system and each is subject to failure from the same common cause. An example would be where the same type of sensor is used in two separate protection systems both providing risk reduction for the same hazard (see Figure A.6).
3) Where more than one protection system is used, the protection systems are diverse but proof testing is carried out on all the systems on a synchronous basis. In such cases the actual PFD_{avg} achieved by the combination of multiple systems will be significantly higher than the PFD_{avg} suggested by the multiplication of the PFD_{avg} of the individual systems.
4) Where the same individual element is used as part of the control system and the safety-related system.
5) Where more than one protection system is used and where the same individual element is used as part of more than one system.

In such cases the effect of common cause/dependency will need to be considered. Consideration should be given as to whether the final arrangement is capable of meeting the necessary systematic capability and the necessary probability of dangerous random hardware failure rates relating to the overall risk reduction required. The effect of common cause failures is difficult to determine and often requires the construction of special purpose models (e.g. fault tree or Markov models).

The effect of common cause is likely to be more significant in applications involving high safety integrity levels. In some applications it may be necessary to incorporate diversity so that common cause effects are minimised. It should however be noted that incorporation of diversity can lead to problems during design, maintenance and modification. Introducing diversity can lead to errors due to the unfamiliarity and lack of operation experience with the diverse devices.

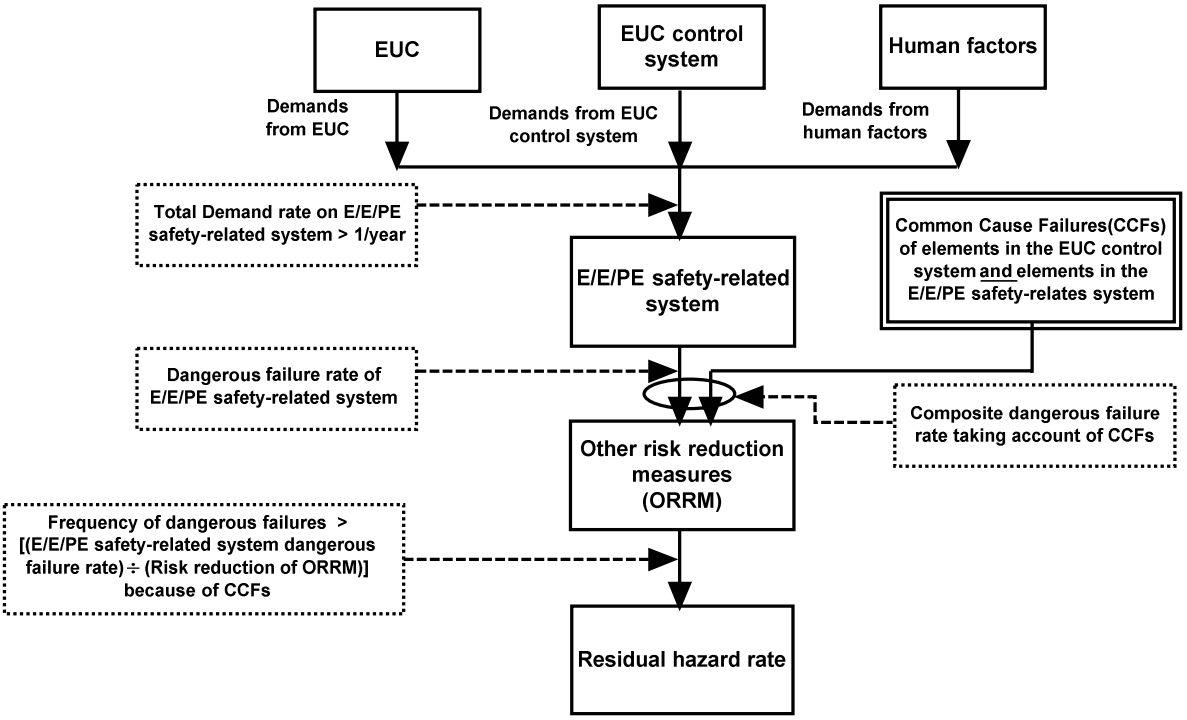


Figure A.5 – Illustration of common cause failures (CCFs) of elements in the EUC control system and elements in the E/E/PE safety-related system

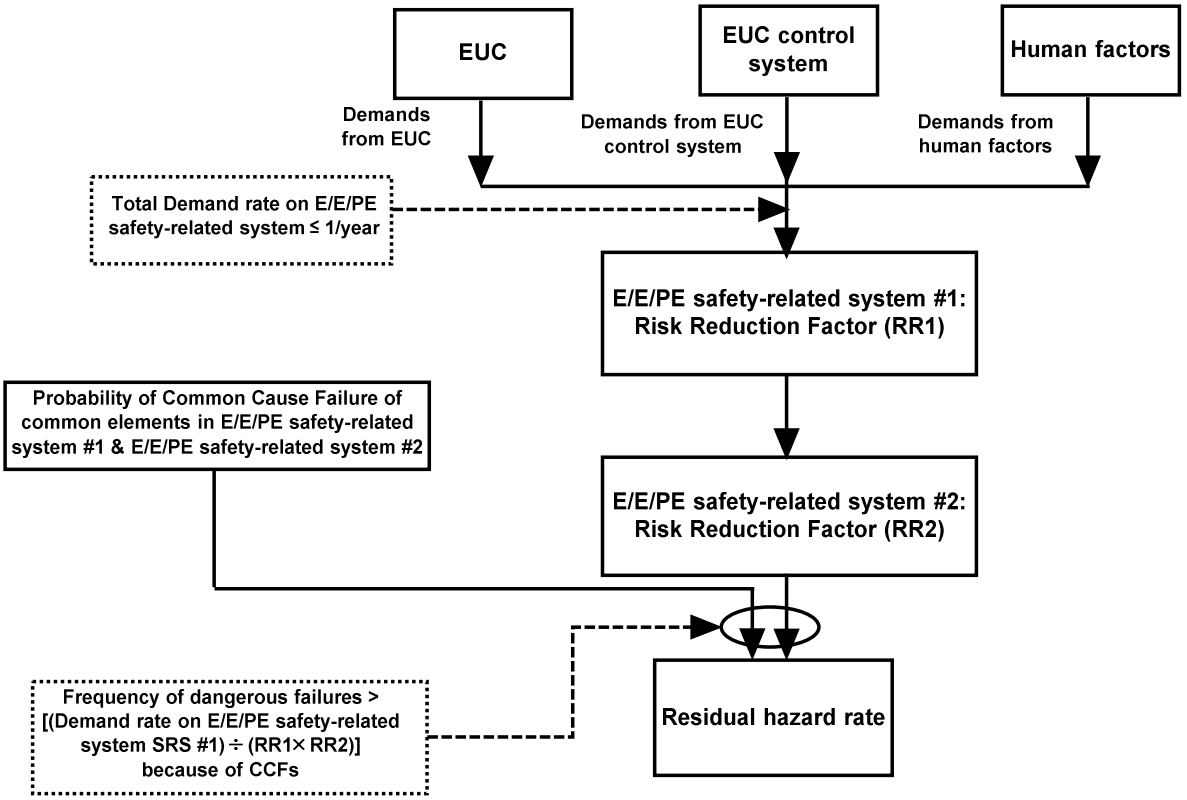


Figure A.6 – Common cause between two E/E/PE safety-related systems

A.5.5 Safety Integrity levels when multiple layers of protection are used

When multiple layers of protection are used to achieve a tolerable risk there may be interactions between systems themselves and also between systems and causes of demand. As discussed above in A.5.4 there are always concerns about test (de)synchronisation and common cause failures since these can be significant factors when overall risk reduction requirements are high or where demand frequency is low. Evaluation of the interactions between safety layers and between safety layers and causes of demand can be complex and may need the development of a holistic model (e.g. as described in ISO/IEC 31010) and based, for example on a top down approach with the top event specified as the tolerable hazard frequency. The model may include all safety layers for calculating the actual risk reduction and all causes of demand for calculating the actual frequency of accident. This allows the identification of minimal cut sets (i.e. failure scenarios), reveals the weak points (i.e. the shortest minimal cut sets: single, double failures, etc.) in the arrangement of systems and facilitates system improvement through sensitivity analysis.

A.6 Risk and safety integrity

It is important that the distinction between risk and safety integrity be fully appreciated. Risk is a measure of the probability and consequence of a specified hazardous event occurring. This can be evaluated for different situations (EUC risk, risk reduction required to meet the tolerable risk, actual risk (see Figure A.1). The tolerable risk is determined by consideration of the issues described in A.2. Safety integrity applies solely to the E/E/PE safety-related systems and other risk reduction measures and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be allocated (see 7.4, 7.5 and 7.6 of IEC 61508-1).

NOTE The allocation is necessarily iterative in order to optimize the design to meet the various requirements.

A.7 Safety integrity levels and software systematic capability

To cater for the wide range of necessary risk reductions that the safety-related systems have to achieve, it is useful to have available a number of safety integrity levels as a means of satisfying the safety integrity requirements of the safety functions allocated to the safety-related systems. Software systematic capability is used as the basis of specifying the safety integrity requirements of the safety functions implemented in part by safety-related software. The safety integrity requirements specification should specify the safety integrity levels for the E/E/PE safety-related systems.

In this standard, four safety integrity levels are specified, with safety integrity level 4 being the highest level and safety integrity level 1 being the lowest.

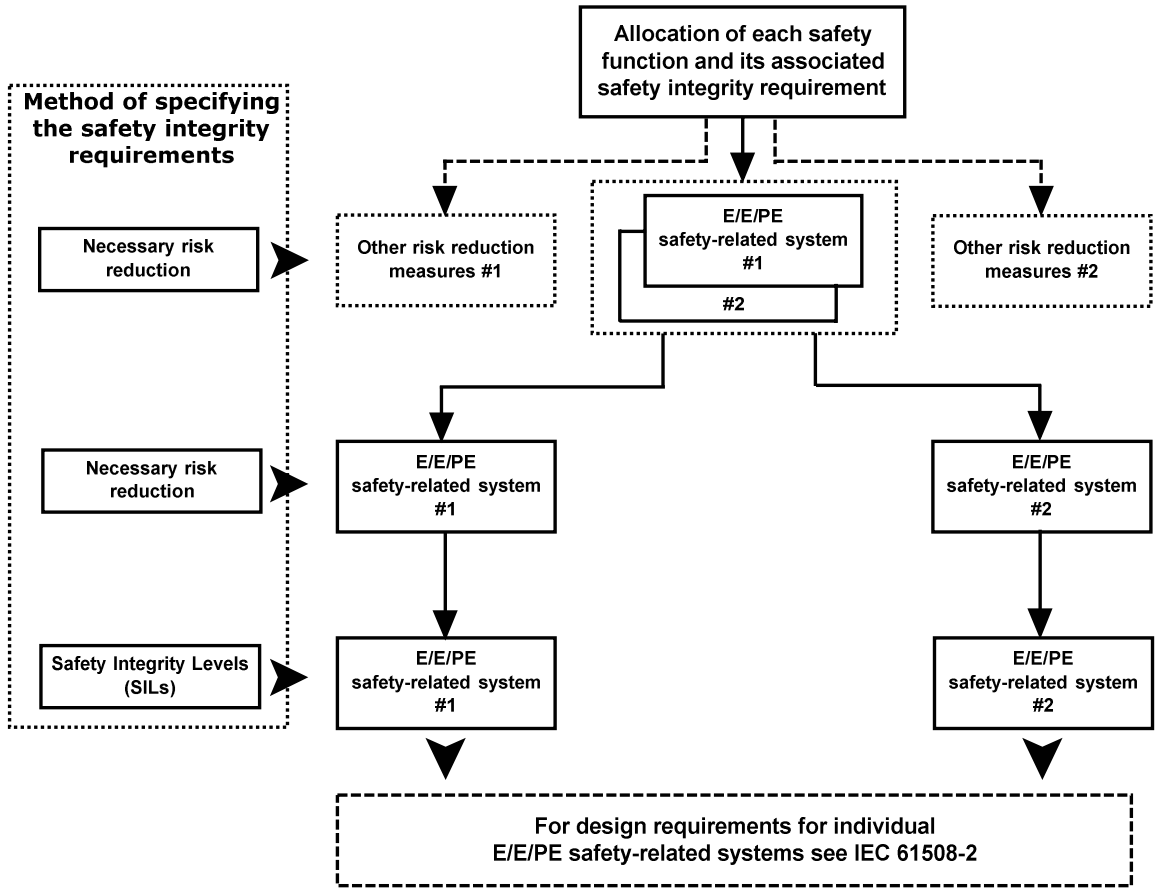
The safety integrity level target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1. Two parameters are specified, one for safety-related systems operating in a low demand mode of operation and one for safety-related systems operating in a high demand or continuous mode of operation.

NOTE For safety-related systems operating in a low demand mode of operation, the safety integrity measure of interest is the probability of failure to perform its design function on demand. For safety-related systems operating in a high demand or continuous mode of operation, the safety integrity measure of interest is the average probability of a dangerous failure per hour (see 3.5.16 and 3.5.17 of IEC 61508-4).

A.8 Allocation of safety requirements

The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the E/E/PE safety-related systems, other technology safety-related systems and other risk reduction measures is shown in Figure A.7 (this is identical to Figure 6 of IEC 61508-1). The requirements for the safety requirements allocation phase are given in 7.6 of IEC 61508-1.

The methods used to allocate the safety integrity requirements to the E/E/PE safety-related systems, other technology safety-related systems and other risk reduction measures depend, primarily, upon whether the necessary risk reduction is specified explicitly in a numerical manner or in a qualitative manner. These approaches are termed quantitative and qualitative methods respectively (see Annexes C, D, E, F and G).



NOTE 1 Safety integrity requirements are associated with each safety function before allocation (see 7.5.2.3 and 7.5.2.4 of IEC 61508-1).

NOTE 2 A safety function may be allocated across more than one safety-related system.

Figure A.7 – Allocation of safety requirements to the E/E/PE safety-related systems, and other risk reduction measures

A.9 Mitigation systems

Mitigation systems take action in the event of full or partial failure of other safety-related systems such as E/E/PE safety-systems. The objective is to reduce the consequences associated with a hazardous event rather than its frequency. Examples of mitigation systems include fire and gas systems (detection of fire/gas and subsequent action to put the fire out (e.g. by water deluge), and airbag systems in an automobile.

When determining the safety integrity requirements it should be recognised that when making judgments on the severity of the consequence, only the incremental consequences should be considered. That is, determine the increase in the severity of the consequence if the function did not operate over that when it does operate as intended. This can be done by first considering the consequences if the system fails to operate and then considering what difference will be made if the mitigation function operates correctly. In considering the consequences if the system fails to operate there will normally be a number of outcomes all with different probabilities. Event tree analysis (ETA) may be a useful tool for this.

NOTE Guidance on the determination of safety integrity levels for fire and gas and emergency shut down systems is included in Annex B of ISO 10418.

Annex B
(informative)

Selection of methods for determining safety integrity level requirements

B.1 General

This annex lists a number of techniques that can be used for determination of safety integrity levels. None of the methods are suitable for all applications and users will need to select the most suitable. In selecting the most appropriate method consideration should be given to the following factors:

1) the risk acceptance criteria that need to be met. Some of the techniques will not be suitable if it is required to demonstrate that risk has been reduced to as low as reasonably practicable;
2) the mode of operation of the safety function. Some methods are only suitable for low demand mode;
3) the knowledge and experience of the persons undertaking the SIL determination and what has been the traditional approach in the sector;
4) the confidence needed that the resulting residual risk meets the criteria specified by the user organisation. Some of the methods can be linked back to quantified targets but some approaches are qualitative only;
5) more than one method may be used. One method may be used for screening purposes followed by another more rigorous approach if the screening method shows the need for high safety integrity levels;
6) the severity of the consequences. More rigorous methods may be selected for consequences that include multiple fatalities;
7) whether common cause occurs between the E/E/PE safety related systems or between the E/E/PE safety related system and demand causes.

Whatever method is used all assumptions should be recorded for future safety management. All decisions should be recorded so that the SIL assessment can be verified and be subject to independent functional safety assessment.

B.2 The ALARP method

The ALARP principles may be used on its own or with other methods to determine the SIL requirements for a safety function. It can be used in a qualitative or quantitative way. When used in a qualitative way the SIL requirements for a specified safety function are increased until the frequency of occurance is reduced such that the conditions associated with Class II or Class III risk class are satisfied. When used in a quantitative way frequencies and consequences are specified numerically and the SIL requirements increased until it can be shown that the additional capital and operating cost associated with implementing a higher SIL would meet the condition associated with Class II or Class III risk class (see Figure C.1).

In using the ALARP method the boundary between the intolerable region and the ALARP region will need to be considered.

B.3 Quantitative method of SIL determination

The quantitative method is described in Annex D. It may be used together with the ALARP method described in Annex C.

The quantitative method can be used for both simple and complex applications. With complex applications, fault trees can be constructed to represent the hazard model. The top event will generally be one or more fatalities and logic constructed to represent demand causes and failures of the E/E/PE safety related systems that lead to the top event. Software tools are available to allow modeling of common cause if the same type of equipment is used for control and protection functions. In some complex applications, a single failure event may occur in more than one place in the fault tree and this will require a boolean reduction to be carried out. The tools also facilitate sensitivity analysis that shows the dominant factors that influence the frequency of the top event. SIL can be established by determining the required risk reduction to achieve the tolerable risk criteria.

The method is suitable for safety functions operating in continuous/high demand mode and low demand mode. The method normally results in low SILs because the risk model is specifically designed for each application and numeric values are used to represent each risk factor rather than the numeric ranges used in calibrated risk graphs. Quantitative methods however require the construction of a specific model for each hazardous event. Modeling requires skill, tools and knowledge of the application and can take considerable time to develop and verify.

The method facilitates demonstration that risk has been reduced to as low as reasonably practicable. This can be done by considering options for further risk reduction, integrating the additional facilities in the fault tree model and then determining the reduction in risk and comparing this with the cost of the option.

B.4 The risk graph method

The risk graph qualitative method is described in Annex E. The method enables the safety integrity level to be determined from knowledge of the risk factors associated with the EUC and the EUC control system. A number of parameters are introduced which together describe the nature of the hazardous situation when safety related systems fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the safety integrity level allocated to the safety functions. The method has been used extensively within the machinery sector, see ISO 14121-2 and Annex A of ISO 13849-1.

The method can be qualitative in which case the selection of the parameters is subjective and requires considerable judgment. The residual risk cannot be calculated from knowledge of the parameter values. It will not be suitable if an organisation requires confidence that residual risk is reduced to a specified quantitative value.

The parameters descriptions can include numeric values that are derived by calibrating the risk graph against numeric tolerability risk criteria. The residual risk can be calculated from numeric values used for each of the parameters. It will be suitable if an organisation requires confidence that residual risk is reduced to a specified quantitative value. Experience has shown that use of the calibrated risk graph method can result in high safety integrity levels. This is because calibration is usually carried out using worst case values of each parameter. Each parameter has a decade range so that for applications where all the parameters are average for the range, the SIL will be one higher than necessary for tolerable risk. The method is extensively used in the process and offshore sector.

The risk graph method does not take into account common cause failures between causes of demand and cause of the E/E/PE safety related system failure or common cause issues with other layers of protection.

B.5 Layer of protection analysis (LOPA)

The basic method is described in a number of books and the technique can be used in a number of different forms. A technique that can be used for SIL determination is described in Annex F.

The method is quantitative and the user will need to decide the tolerable frequencies for each consequence severity level. Numeric credit is given for protection layers that reduce the frequency of individual demand causes. Not all protection layers are relevant to all demand causes, so the technique can be used for more complex applications. The numeric values assigned to protection layers can be rounded up to the next significant figure or the next significant decade range. If numeric values of protection layers are rounded to the next significant figure, then the method on average gives lower requirements for risk reduction and lower SIL values than calibrated risk graphs.

Since numeric targets are assigned to specified consequence severity levels, the user can have confidence that residual risk meets corporate criteria.

The method as described is not suitable for functions that operate in continuous mode and does not take account of common cause failure between causes of demand and the E/E/PE safety related systems. The method can however be adjusted so as to be suitable for such cases.

B.6 Hazardous event severity matrix

The hazard event severity method is described in Annex G. An inherent assumption is that when a protection layer is added that an order of magnitude risk reduction is achieved. A further assumption is that protection layers are independent of demand cause and independent of each other. The method as described is not suitable for functions that operate in continuous mode. The method can be qualitative in which case the selection of the risk factors is subjective and requires considerable judgment. The residual risk cannot be calculated from knowledge of the risk factors selected. It will not be suitable if an organization requires confidence that residual risk is reduced to a specified quantitative value.

Annex C
(informative)

ALARP and tolerable risk concepts

C.1 General

This annex considers one particular approach to the achievement of a tolerable risk. The intention is not to provide a definitive account of the method but rather an illustration of the general principles. The approach includes a process of continuous improvement where all options that would reduce risk further are considered in terms of benefits and costs. Those intending to apply the methods indicated in this annex should consult the source material referenced (see reference [7] in the Bibliography).

C.2 ALARP model

C.2.1 Introduction

Clause C.2 outlines the main tests that are applied in regulating industrial risks and indicates that the activities involve determining whether:

a) the risk is so great that it shall be refused altogether; or

b) the risk is, or has been made, so small as to be insignificant; or

c) the risk falls between the two states specified in a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.

With respect to c), the ALARP principle requires that any risk shall be reduced so far as is reasonably practicable, or to a level which is as low as reasonably practicable (these last 5 words form the abbreviation ALARP). If a risk falls between the two extremes (i.e. the unacceptable region and broadly acceptable region) and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application. This three zone approach is shown in Figure C.1.

Above a certain level, a risk is regarded as intolerable and cannot be justified in any ordinary circumstance.

Below that level, there is the tolerability region where an activity is allowed to take place provided the associated risks have been made as low as reasonably practicable. Tolerable here is different from acceptable: it indicates a willingness to live with a risk so as to secure certain benefits, at the same time expecting it to be kept under review and reduced as and when this can be done. Here a cost benefit assessment is required either explicitly or implicitly to weigh the cost and the need or otherwise for additional safety measures. The higher the risk, the more proportionately would be expected to be spent to reduce it. At the limit of tolerability, expenditure in gross disproportion to the benefit would be justified. Here the risk will by definition be substantial, and equity requires that a considerable effort is justified even to achieve a marginal reduction.

Where the risks are less significant, proportionately less needs to be spent in order to reduce them and at the lower end of the tolerability region, a balance between costs and benefits will suffice.

Below the tolerability region is the broadly acceptable region where the risks are small in comparison with the everyday risks we all experience. While in the broadly acceptable region, there is no need for a detailed working to demonstrate ALARP, it is, however, necessary to remain vigilant to ensure that the risk remains at this level.

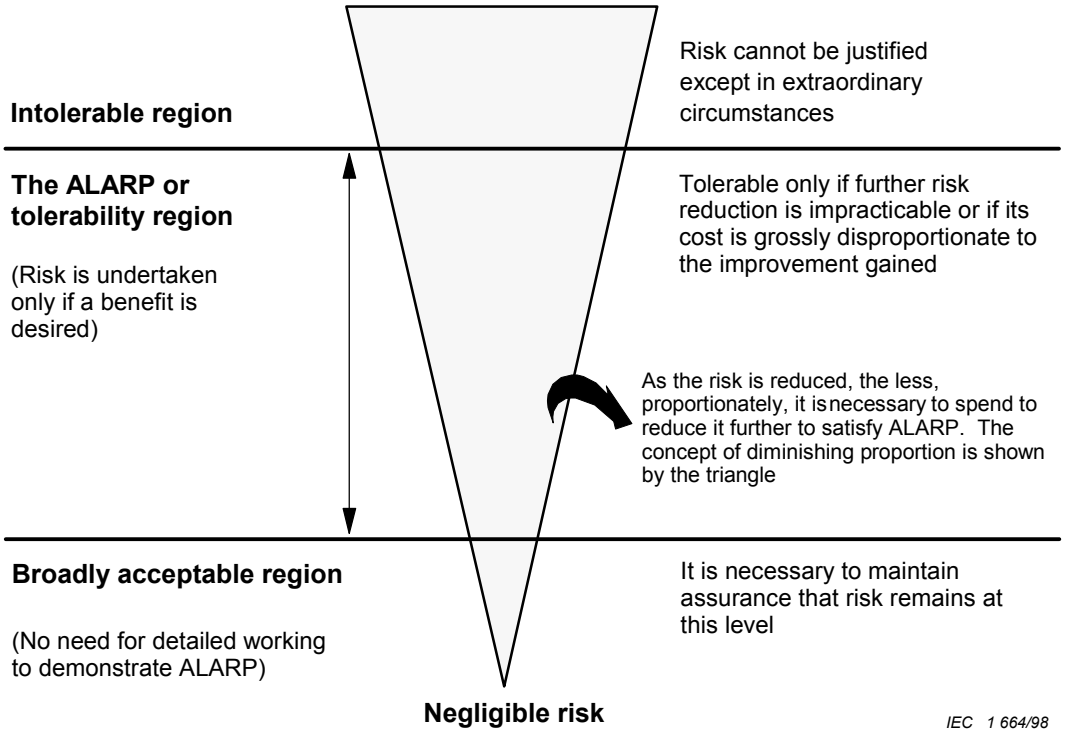


Figure C.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Subclause C.2.2 outlines a method for quantitative risk targets. (Annex D and F outline quantitative methods and Annexes E and G outline qualitative methods for the determination of the necessary risk reduction for a specific hazard. The methods indicated could incorporate the concept of ALARP in the decision making.)

NOTE Further information on ALARP is given in reference [7] in the Bibliography.

C.2.2 Tolerable risk target

One way in which a tolerable risk target can be obtained is for a number of consequences to be determined and tolerable frequencies allocated to them. This matching of the consequences to the tolerable frequencies would take place by discussion and agreement between the interested parties (for example safety regulatory authorities, those producing the risks and those exposed to the risks).

To take into account ALARP concepts, the matching of a consequence with a tolerable frequency can be done through risk classes. Table C.1 is an example showing four risk classes (I, II, III, IV) for a number of consequences and frequencies. Table C.2 interprets each of the risk classes using the concept of ALARP. That is, the descriptions for each of the four risk classes are based on Figure C.1. The risks within these risk class definitions are the risks that are present when risk reduction measures have been put in place. With respect to Figure C.1, the risk classes are as follows:

– risk class I is in the intolerable region;
– risk classes II and III are in the ALARP region, risk class II being just inside the ALARP region;
– risk class IV is in the broadly acceptable region.

For each specific situation, or sector comparable industries, a table similar to Table C.1 would be developed taking into account a wide range of social, political and economic factors. Each consequence would be matched against a frequency and the table populated by the risk classes. For example, frequent in Table C.1 could denote an event that is likely to be

continually experienced, which could be specified as a frequency greater than 10 per year. A critical consequence could be a single death and/or multiple severe injuries or severe occupational illness.

Table C.1 – Example of risk classification of accidents

Frequency	Consequence			
	Catastrophic	**Critical**	**Marginal**	**Negligible**
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV
NOTE 1 The actual population with risk classes I, II, III and IV will be sector dependent and will also depend upon what the actual frequencies are for frequent, probable, etc. Therefore, this table should be seen as an example of how such a table could be populated, rather than as a specification for future use. NOTE 2 Determination of the safety integrity level from the frequencies in this table is outlined in Annex D.				

Table C.2 – Interpretation of risk classes

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

Annex D
(informative)

Determination of safety integrity levels – A quantitative method

D.1 General

This annex outlines how the safety integrity levels can be determined if a quantitative approach is adopted and illustrates how the information contained in tables such as Table C.1 can be used. A quantitative approach is of particular value when:

– the tolerable risk is to be specified in a numerical manner (for example that a specified consequence should not occur with a greater frequency than one in 10^4 years);

– numerical targets have been specified for the safety integrity levels for the safety-related systems. Such targets have been specified in this standard (see Tables 2 and 3 of IEC 61508-1).

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is particularly applicable when the risk model is as indicated in Figures A.1 and A.2.

D.2 General method

The model used to illustrate the general principles is that shown in Figure A.1. The key steps in the method are as follows and will need to be done for each safety function to be implemented by the E/E/PE safety-related system:

– determine the tolerable risk from a table such as Table C.1;

– determine the EUC risk;

– determine the necessary risk reduction to meet the tolerable risk;

– allocate the necessary risk reduction to the E/E/PE safety-related systems, other technology safety-related systems and other risk reduction measures (see 7.6 of IEC 61508-1).

Table C.1 is populated with risk frequencies and allows a numerical tolerable risk target (F_t) to be specified.

The frequency associated with the risk that exists for the EUC, including the EUC control system and human factor issues (the EUC risk), without any protective features, can be estimated using quantitative risk assessment methods. This frequency with which a hazardous event could occur without protective features present (F_{np}) is one of two components of the EUC risk; the other component is the consequence of the hazardous event. F_{np} may be determined by:

– analysis of failure rates from comparable situations;

– data from relevant databases;

– calculation using appropriate predictive methods.

This standard places constraints on the minimum failure rates that can be claimed for the EUC control system (see 7.5.2.5 of IEC 61508-1). If it is to be claimed that the EUC control system has a failure rate less than these minimum failure rates, then the EUC control system shall be considered a safety-related system and shall be subject to all the requirements for safety-related systems in this standard.

D.3 Example calculation

Figure D.1 provides an example of how to calculate the target safety integrity for a single safety-related protection system. For such a situation

$$PFD_{avg} \leq F_t / F_{np}$$

where

PFD_{avg} is the average probability of failure on demand of the safety-related protection system, which is the target failure measure for safety-related protection systems operating in a low demand mode of operation (see Table 2 of IEC 61508-1 and 3.5.16 of IEC 61508-4);

F_t is the tolerable hazard frequency;

F_{np} is the demand rate on the safety-related protection system.

Also in Figure D.1:

– C is the consequence of the hazardous event;

– F_p is the risk frequency with the protective features in place.

It can be seen that determination of F_{np} for the EUC is important because of its relationship to PFD_{avg} and hence to the safety integrity level of the safety-related protection system.

The necessary steps in obtaining the safety integrity level (when the consequence C remains constant) are given below (as in Figure D.1), for the situation where the entire necessary risk reduction is achieved by a single safety-related protection system which must reduce the hazard rate, as a minimum, from F_{np} to F_t:

– determine the frequency element of the EUC risk without the addition of any protective features (F_{np});

– determine the consequence C without the addition of any protective features;

– determine, by use of Table C.1, whether for frequency F_{np} and consequence C a tolerable risk level is achieved. If, through the use of Table C.1, this leads to risk class I, then further risk reduction is required. Risk class IV or III would be tolerable risks. Risk class II would require further investigation;

NOTE Table C.1 is used to check whether or not further risk reduction measures are necessary, since it may be possible to achieve a tolerable risk without the addition of any protective features.

– determine the probability of failure on demand for the safety-related protection system (PFD_{avg}) to meet the necessary risk reduction (ΔR). For a constant consequence in the specific situation described, $PFD_{avg} = (F_p / F_{np}) = \Delta R$;

– for $PFD_{avg} = (F_p / F_{np})$, the safety integrity level can be obtained from Table 2 of IEC 61508-1 (for example, for $PFD_{avg} = 10^{-2} – 10^{-3}$, the safety integrity level = 2).

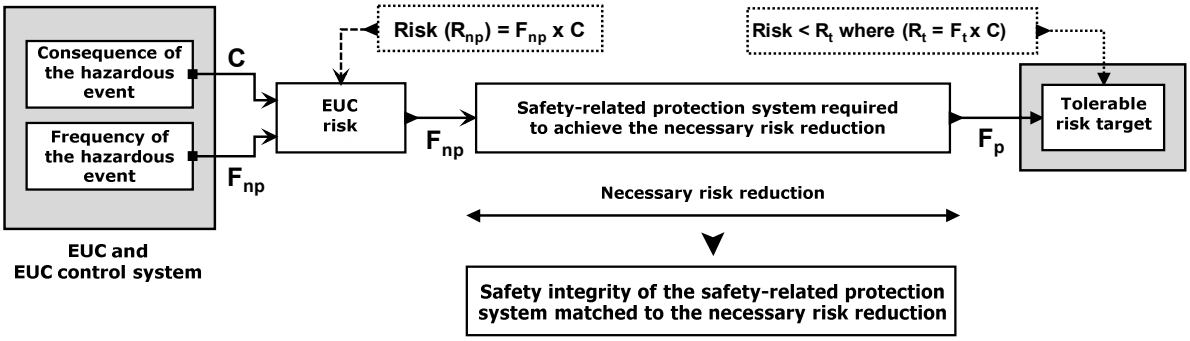


Figure D.1 – Safety integrity allocation – example for safety-related protection system

Annex E
(informative)

Determination of safety integrity levels – Risk graph methods

E.1 General

This annex describes the risk graph method, which is a method that enables the safety integrity level of a safety-related system to be determined from a knowledge of the risk factors associated with the EUC and the EUC control system. It is particularly applicable when the risk model is as indicated in Figures A.1 and A.2. The method can be used on a qualitative or quantitative basis.

Where this approach is adopted, in order to simplify matters a number of parameters are introduced which together describe the nature of the hazardous situation when safety-related systems fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the safety integrity level allocated to the safety functions. These parameters

– allow a meaningful graduation of the risks to be made; and
– contain the key risk assessment factors.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles.

E.2 Risk graph synthesis

The following simplified procedure is based on the following equation:

$$R = (f) \text{ of a specified } (C)$$

where

R is the risk with no safety-related systems in place;

f is the frequency of the hazardous event with no safety-related systems in place;

C is the consequence of the hazardous event (the consequences could be related to harm associated with health and safety or harm from environmental damage).

The frequency of the hazardous event f is, in this case, considered to be made up of three influencing factors:

– frequency of, and exposure time in, the hazardous zone;
– the possibility of avoiding the hazardous event;
– the probability of the hazardous event taking place without the addition of any safety-related systems (but having in place other risk reduction facilities) – this is termed the probability of the unwanted occurrence.

This produces the following four risk parameters:

– consequence of the hazardous event (C);
– frequency of, and exposure time in, the hazardous zone (F);
– possibility of failing to avoid the hazardous event (P);
– probability of the unwanted occurrence (W).

The risk parameters may be decided on a qualitative basis as described in Table E.1 or on a quantitative basis as described in Table E.2. In deciding the numeric values associated with each parameter in Table E.2 a calibration process will be required.

E.3 Calibration

The objectives of the calibration process are as follows:

- to describe all parameters in such a way as to enable the SIL assessment team to make objective judgments based on the characteristics of the application;
- to ensure the SIL selected for an application is in accordance with corporate risk criteria and takes account of risks from other sources;
- to enable the parameter selection process to be verified.

Calibration of the risk graph is the process of assigning numerical values to risk graph parameters. This forms the basis for the assessment of the existing process risk and allows determination of the required integrity of the safety instrumented function under consideration. Each of the parameters is assigned a range of values such that when applied in combination a graded assessment of the risk which exists in the absence of the particular safety function is produced. Thus, a measure of the degree of reliance to be placed on the safety function is determined. The risk graph relates particular combinations of the risk parameters to safety integrity levels. The relationship between the combinations of risk parameters and safety integrity levels is established by considering the tolerable risk associated with specific hazards.

When considering the calibration of risk graphs, it is important to consider requirements relating to risk arising from both the owners' expectations and regulatory authority requirements. Risks to life can be considered in a number of ways as described in A.2 and Annex C.

If it is necessary to reduce the frequency of an individual fatality to a specified maximum then it cannot be assumed that all this risk reduction can be assigned to a single E/E/PE safety-related system. The exposed persons are subject to a wide range of risks arising from other sources (e.g., falls, fire and explosion risks). During calibration, the number of hazards that individuals are exposed to, and the total time at risk, will need to be considered.

When considering the extent of risk reduction required, an organization may have criteria relating to the incremental cost of averting a fatality. This can be calculated by dividing the annualised cost of the additional hardware and engineering associated with a higher level of integrity by the incremental risk reduction. An additional level of integrity is justified if the incremental cost of averting a fatality is less than a predetermined amount.

The above issues need to be considered before each of the parameter values can be specified. Most of the parameters are assigned a range (e.g., If the expected demand rate of a particular process falls between a specified decade range of demands per year then W3 may be used). Similarly, for demands in the lower decade range, W2 would apply and for demands in the next lower decade range, W1 applies. Giving each parameter a specified range assists the team in making decisions on which parameter value to select for a specific application. To calibrate the risk graph, values or value ranges are assigned to each parameter. The risk associated with each of the parameter combinations is then assessed against the defined risk criteria. Parameter descriptions are then modified so that for all combinations of all parameter values, the defined risk criteria is achieved. In the example calibration as shown in Table E.2 a "D" factor is introduced to enable the range of demands associated with each W factor to be modified so that tolerable risk is achieved. In some cases, the ranges associated with other risk factors may need to be modified to reflect the parameter values encountered in the spread of applications being considered. Calibration is an iterative process and continues until the specified risk acceptability criteria are satisfied for all combinations of parameter values.

The calibration activity does not need to be carried out each time the SIL for a specific application is to be determined. It is normally only necessary for organisations to undertake the work once, for similar hazards. Adjustment may be necessary for specific projects if the original assumptions made during the calibration are found to be invalid for any specific project.

When parameter assignments are made, information should be available as to how the values were derived.

It is important that this process of calibration is agreed at a senior level within the organization taking responsibility for safety. The decisions taken determine the overall safety achieved.

In general, it will be difficult for a risk graph to consider the possibility of dependent failure between the sources of demand and the equipment used within the E/E/PE safety related system. It can therefore lead to an over-estimation of the effectiveness of the E/E/PE safety related system. If risk graphs are calibrated to include demand rates higher than once per year, then the SIL requirements that results from use of the risk graph may be higher than necessary and the use of other techniques is recommended.

E.4 Other possible risk parameters

The risk parameters specified above are considered to be sufficiently generic to deal with a wide range of applications. There may, however, be applications which have aspects which require the introduction of additional risk parameters e.g. the use of new technologies in the EUC and the EUC control system. The purpose of the additional parameters would be to estimate more accurately the necessary risk reduction (see Figure A.1).

E.5 Risk graph implementation – general scheme

The combination of the risk parameters described above enables a risk graph such as that shown in Figure E.1 to be developed. With respect to Figure E.1:

$$C_A < C_B < C_C < C_D;\ F_A < F_B;\ P_A < P_B;\ W_1 < W_2 < W_3.$$

An explanation of this risk graph is as follows.

– Use of risk parameters C, F and P leads to a number of outputs X_1, X_2, X_3... X_n (the exact number being dependent upon the specific application area to be covered by the risk graph). Figure E.1 indicates the situation when no additional weighting is applied for the more serious consequences. Each one of these outputs is mapped onto one of three scales (W_1, W_2 and W_3). Each point on these scales is an indication of the necessary safety integrity that has to be met by the E/E/PE safety-related system under consideration. In practice, there will be situations when for specific consequences, a single E/E/PE safety-related system is not sufficient to give the necessary risk reduction;

– The mapping onto W1, W2 or W3 allows the contribution of other risk reduction measures to be made. The offset feature of the scales for W1, W2 and W3 is to allow for three different levels of risk reduction from other measures. That is, scale W3 provides the minimum risk reduction contributed by other measures (i.e. the highest probability of the unwanted occurrence taking place), scale W2 a medium contribution and scale W1 the maximum contribution. For a specific intermediate output of the risk graph (i.e. X1, X2... or X6) and for a specific W scale (i.e. W1, W2 or W3) the final output of the risk graph gives the safety integrity level of the E/E/PE safety-related system (i.e. 1, 2, 3 or 4) and is a measure of the required risk reduction for this system. This risk reduction, together with the risk reductions achieved by other measures (for example by other technology safety-related systems and other risk reduction measures) which are taken into account by the W scale mechanism, gives the necessary risk reduction for the specific situation.

The parameters indicated in Figure E.1 (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3), and their weightings, would need to be accurately defined for each specific situation or sector comparable industries, and would also need to be defined in application sector international standards.

E.6 Risk graph example

An example of a risk graph implementation based on the example data in Table E.1 below is shown in Figure E.2. Use of the risk parameters C, F, and P lead to one of eight outputs. Each one of these outputs is mapped onto one of three scales (W1, W2 and W3). Each point on these scales (a, b, c, d, e, f, g and h) is an indication of the necessary risk reduction that has to be met by the safety-related system.

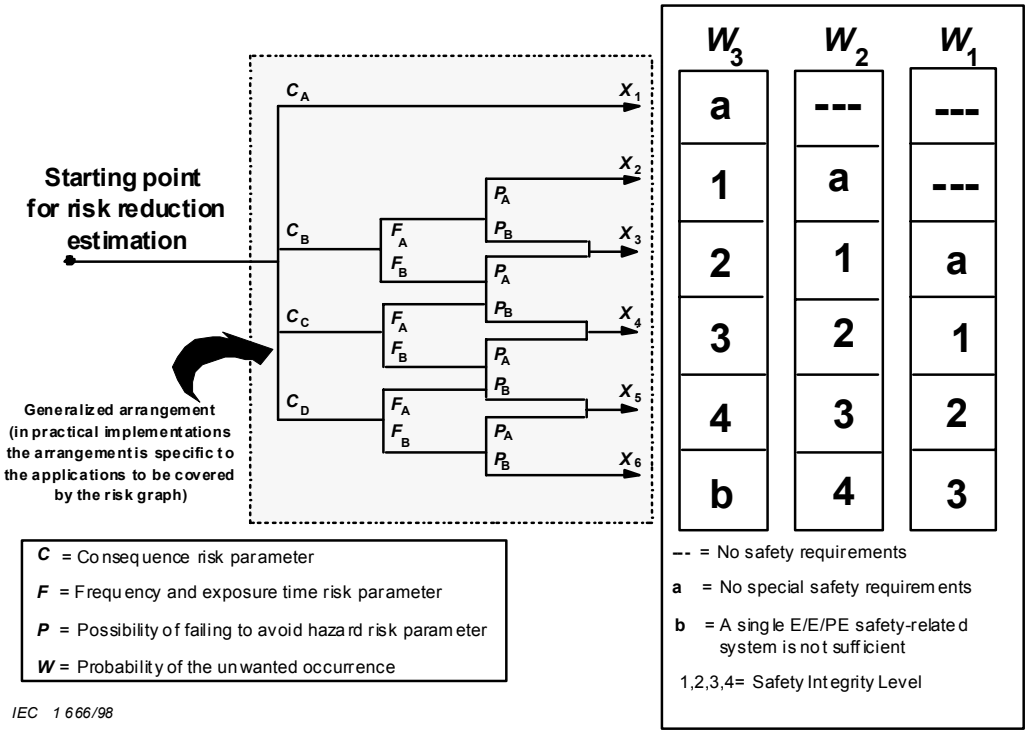
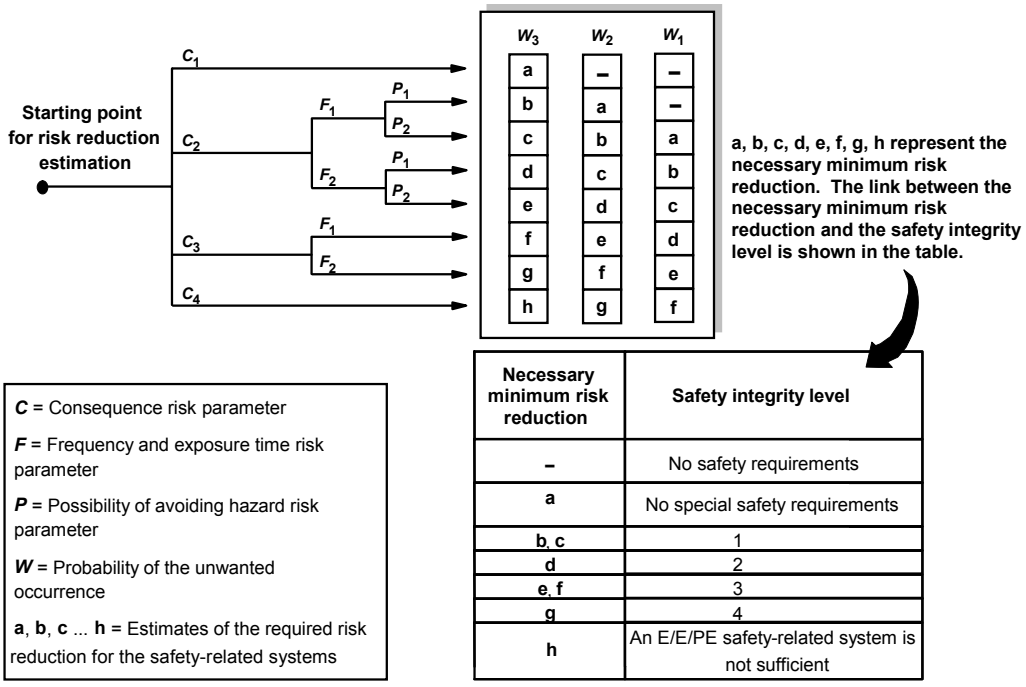


Figure E.1 – Risk Graph: general scheme



Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE safety-related system is not sufficient

Figure E.2 – Risk graph – example (illustrates general principles only)

Table E.1 – Example of data relating to risk graph (Figure E.2)

Risk parameter		Classification	Comments
Consequence (*C*)	C_1	Minor injury	1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage
	C_2	Serious permanent injury to one or more persons; death to one person	
	C_3	Death to several people	2 For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing shall be taken into account
	C_4	Very many people killed	
Frequency of, and exposure time in, the hazardous zone (*F*)	F_1	Rare to more often exposure in the hazardous zone	3 See comment 1 above.
	F_2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the hazardous event (*P*)	P_1	Possible under certain conditions	4 This parameter takes into account – operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised); – rate of development of the hazardous event (for example suddenly, quickly or slowly); – ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); – avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).
	P_2	Almost impossible	
Probability of the unwanted occurrence (*W*)	W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	5 The purpose of the *W* factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any other risk reduction measures
	W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	6 If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the *W* factor may be made by calculation. In such an event a worst case prediction shall be made
	W_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	

Table E.2 – Example of calibration of the general purpose risk graph

Risk parameter		Classification	Comments
Consequence (C) Number of fatalities This can be calculated by determining the numbers of people present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: V=0,01 Small release of flammable or toxic material V=0,1 Large release of flammable or toxic material V=0,5 As above but also a high probability of catching fire or highly toxic material V=1 Rupture or explosion	C_A C_B C_C C_D	Minor injury Range 0,01 to 0,1 Range >0,1 to 1,0 Range > 1,0	1 The classification system has been developed to deal with injury and death to people 2 For the interpretation of C_A, C_B, C_C and C_D, the consequences of the accident and normal healing shall be taken into account
Occupancy (F) This is calculated by determining the proportional length of time the area exposed to the hazard is occupied during a normal working period NOTE 1 If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected NOTE 2 It is only appropriate to use F_A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities	F_A F_B	Rare to more often exposure in the hazardous zone. Occupancy less than 0,1 Frequent to permanent exposure in the hazardous zone	3 See comment 1 above
Probability of avoiding the hazardous event (P) if the protection system fails to operate	P_A P_B	Adopted if all conditions in column 4 are satisfied Adopted if all the conditions are not satisfied	4 P_A should only be selected if all the following are true: – facilities are provided to alert the operator that the SIS has failed; – independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area; – the time between the operator being alerted and a hazardous event occurring exceeds 1 h or is definitely sufficient for the necessary actions.

Table E.2 (*continued*)

Risk parameter		Classification	Comments
Demand rate (W) The number of times per year that the hazardous event would occur in absence of a the E/E/PE safety related system To determine the demand rate it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61508, is limited to below the performance ranges associated with SIL 1	W_1 W_2 W_3	Demand rate less than 0,1 D per year Demand rate between 0,1 D and D per year Demand rate between D and 10 D per year For demand rates higher than 10 D per year higher integrity shall be needed	5 The purpose of the *W* factor is to estimate the frequency of the hazard taking place without the addition of the E/E/PE safety related systems If the demand rate is very high the SIL has to be determined by another method or the risk graph recalibrated. It should be noted that risk graph methods may not be the best approach in the case of applications operating in continuous mode (see 3.5.16 of IEC 61508-4). 6 The value of D should be determined from corporate criteria on tolerable risk taking into consideration other risks to exposed persons
NOTE This is an example to illustrate the application of the principles for the design of risk graphs. Risk graphs for particular applications and particular hazards will be agreed with those involved, taking into account tolerable risk, see Clauses E.1 to E.6.			

Annex F
(informative)

Semi-quantitative method using layer of protection analysis (LOPA)

F.1 General

F.1.1 Description

This annex describes a method called layer of protection analysis (LOPA). It is not intended to be a definitive account of the method, but is intended to illustrate the general principles.

F.1.2 Annex reference

This annex is based on a method described in more detail in an AIChE publication (see [8] in the Bibliography). This reference details many ways of using LOPA techniques.

In one approach, all relevant parameters are rounded to the higher decade range (for example, a probability of $5 \cdot 10^{-2}$ is rounded to 10^{-1}. This is a very conservative approach and can lead to significantly higher SIL levels. Data uncertainty should however be recognised by rounding all parameter values to the next highest significant figure (for example, $5{,}4 \cdot 10^{-2}$ should be rounded to $6 \cdot 10^{-2}$).

F.1.3 Method description

LOPA analyses hazards to determine if safety functions are required and if so, the required SIL of each safety function. The LOPA method needs to be adapted to meet the risk acceptance criteria to be applied. The method starts with data developed in the hazard identification and accounts for each identified hazard by documenting the initiating causes and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction can then be determined and the need for more risk reduction analysed. If additional risk reduction is required and if it is to be provided in the form of an E/E/PE safety-related system, the LOPA methodology allows the determination of the appropriate SIL. For each hazard an appropriate SIL is determined to reduce risks to tolerable levels. Table F.1 hereinafter shows a typical LOPA format

F.2 Impact event

Using Table F.1, each Impact event description (consequence) determined from the hazard identification is entered in column 1 of Table F.1.

F.3 Severity level

The severity level of the event is entered in column 2 of Table F.1. The severity level will be derived from a table that specifies general descriptions of consequence levels e.g. minor, severe, catastrophic, with specified consequence ranges and maximum frequency for each severity level. In effect this table sets down the user tolerability criteria. Information will be needed to allow severity levels and maximum frequencies to be determined for events leading to safety and environmental consequences.

F.4 Initiating cause

All the initiating causes of the impact event are listed in column 3 of Table F.1. Impact events may have many initiating causes, and all should be listed.

F.5 Initiation likelihood

Likelihood values of each of the initiating causes listed in column 3 of Table F.1, in events per year, are entered into column 4 of Table F.1.

Initiation likelihood can be calculated from generic data on equipment failure rates and knowing proof test intervals, or from facility records. Low initiation likelihood should only be used where there is sufficient statistical basis for the data.

Table F.1 – LOPA report

[a]	1	2	3	4	5			6	7	8	9	10	11
					Protection layers (PLs)								
	Impact event description F.2	Severity level F.3	Initiating cause F.4	Initiation likelihood F.5	General design F.6.1	Control system F.6.2	Alarms, etc. F.6.3	Additional mitigation, restricted access F.7	Additional mitigation F.8	Intermediate event likelihood F.9	PFD_{avg} required for E/E/PES (and SIL) F.10	Tolerable Mitigated event likelihood F.11	Notes
1	Overspeed of rotor leading to fracture of casing	Loss of life of persons located adjacent to casing, fatalities will not exceed 2	Speed control system fails	0,1	1	1	1	0,1	0,1	10^{-3}	$5 \cdot 10^{-3}$ (SIL 2 with a minimum PFD_{avg} of $5 \cdot 10^{-3}$)	10^{-5}	
			Loss of load	1	1	0,1	1	0,1	0,1	10^{-3}			
			Clutch failure	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						0,1 credit given to control system		Occupancy limited, persons not present 90 % of the time	Fatality will only occur if fragments contact persons	Total $2{,}1 \cdot 10^{-3}$		Tolerable frequency if fatalities do not exceed 5	
2	Repeat above case for environmental risk analysis												
3				Continued as required.									
.													
.													
N													

NOTE 1 Severity levels may be classified as C (catastrophic), E (extensive), S (serious) or M (minor). Tolerable mitigated event likelihood will depend on severity level.

NOTE 2 Units in columns 4, 8 and 10 are events per year.

NOTE 3 Units in columns 5 to 7 and 9 are dimensionless. The numbers between 0 and 1 are the factors by which event likelihood may be multiplied to represent the mitigating effect of the associated protection layer. Thus 1 means no mitigating effect and 0,1 means a factor of 10 risk reduction.

[a] Column and row numbers are given, as further descriptions of these are included in Annex F.

F.6 Protection layers (PLs)

F.6.1 General

Each PL consists of a grouping of equipment and/or administrative controls that function independently from other layers.

Design features that reduce the likelihood of an impact event from occurring when an initiating cause occurs are listed first in column 5 of Table F.1.

PLs should have the following important characteristics:

– Specificity: A PL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event and therefore multiple event scenarios may initiate action of one PL.

– Effective: A PL must on its own be capable of preventing the outcome of concern when all other measures have completely failed

– Independence: A PL is independent of the other PLs associated with the identified hazardous event.

– Dependability: A PL can be counted on to do what it was designed to do. Both random and systematic failure modes are addressed in the design.

– Auditability: A PL is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system are necessary.

F.6.2 Basic control system

The next item in column 5 of Table F.1 is the EUC control system. If a control function prevents the impact event from occurring when the initiating cause occurs, credit based on its PFD_{avg} is claimed. No credit should be claimed for a control function if failure of that function would cause a demand on the E/E/PE safety-related system. It should also be noted that the PFD_{avg} claimed from a control function should be limited to a minimum of 0,1 if the control function is not designed and operated as a safety system.

F.6.3 Alarms

The last item in column 5 of Table F.1 takes credit for alarms that alert the operator and utilize operator intervention. Credit for alarms should only be claimed under the following circumstances:

– Hardware and software used are separate and independent of that used for the control system (for example, input cards and processors should not be shared).

– The alarm is displayed with a high priority in a permanently manned location. Credit claimed for alarms should take into account the following:

  - the effectiveness of an alarm will depend on the complexity of the task that needs to be performed in the event of the alarm and the other tasks that need to be performed at the same time;.
  - the credit should be limited to a minimum PFD_{avg} of 0,1;
  - the operator needs to have sufficient time and independent facilities to be able to terminate the hazard. Normally, credit should not be claimed unless the time available between the alarm and the hazard exceeds 20 min.

F.7 and F.8 Additional mitigation

Mitigation layers are normally mechanical, structural, or procedural. Examples include:

– restricted access;
– reduction of ignition probability;
– any other factors that reduce the vulnerability of persons exposed to the hazard.

Mitigation layers may reduce the severity of the impact event, but not prevent the event from occurring. Examples include:

– deluge systems in the case of a fire;
– gas alarms;
– evacuation procedures that would reduce the probability of persons being exposed to an escalating event.

Under mitigation, the percentage occupancy of the most exposed person in the hazard zone can be taken account of. This percentage should be determined by establishing the number of hours in the hazardous zone per year and dividing by 8,760 h per year.

The appropriate PFD_{avg} or equivalent for all mitigation layers should be determined and listed in column 6 and 7 of Table F.1.

F.9 Intermediate event likelihood

The intermediate event likelihood for each cause is calculated by multiplying the following factors and the result in frequency per year entered in column 8 of Table F.1:

– vulnerability of the most exposed person;
– initiation likelihood (column 4);
– PFD_{avg} of the Protection Layers and mitigation layers (columns 5, 6 and 7).

The total intermediate event frequency should be calculated by adding intermediate event frequencies for each cause.

The total intermediate event frequency should be compared with the tolerable risk frequency for the associated severity level. If the total intermediate frequency exceeds the tolerable frequency, then risk reduction will be required. Inherently safer methods and solutions should be considered before additional PLs in the form of E/E/PE safety-related system are applied.

If the intermediate event likelihood figures cannot be reduced below the maximum frequency criteria then an E/E/PE safety-related system will be required.

F.10 Safety integrity levels (SILs)

If a safety function is needed, the required SIL can be determined as follows:

– Divide the maximum frequency for the associated severity level by the total intermediate event likelihood for to determine the PFD_{avg} required;
– The numeric target value of the PFD_{avg} can then be used in the safety requirement specification together with the associated SIL. The associated SIL can be obtained from Table 2 of IEC 61508-1;
– If the numeric value of PFD_{avg} is not to be in the process requirements specification and only the required SIL is to be stated, the SIL should be one level higher so that adequate risk reduction will be achieved with all values of PFD_{avg} associated with the specified SIL;

If the PFD_{avg} required for the tolerable risk is greater than or equal to 0,1 the function is allocated the classification “No special safety integrity requirements”.

F.11 Tolerable mitigated event likelihood

The tolerable mitigated event likelihood will depend on the severity level of the consequences. This will depend on the tolerable risk criteria adopted (see A.2 for tolerable risk criteria).

Annex G
(informative)

Determination of safety integrity levels – A qualitative method – hazardous event severity matrix

G.1 General

The numeric method described in Annex D is not applicable where the risk (or the frequency portion of it) cannot be quantified. This annex describes the hazardous event severity matrix method, which is a qualitative method that enables the safety integrity level of an E/E/PE safety-related system to be determined from knowledge of the risk factors associated with the EUC and the EUC control system. It is particularly applicable when the risk model is as indicated in Figures A.1 and A.2.

The scheme outlined in this annex assumes that each safety-related system and other risk reduction measure is independent.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles of how such a matrix could be developed by those having a detailed knowledge of the specific parameters that are relevant to its construction. Those intending to apply the methods indicated in this annex should consult the source material referenced.

NOTE Further information on the hazardous event matrix is given in reference [4] in the Bibliography.

G.2 Hazardous event severity matrix

The following requirements underpin the matrix and each one is necessary for the method to be valid:

a) the E/E/PE safety-related systems and other risk reduction measures are independent;

b) each safety-related system (E/E/PE and other technology) and other risk reduction measures are considered as protection layers which provide, in their own right, partial risk reductions as indicated in Figure A.1;

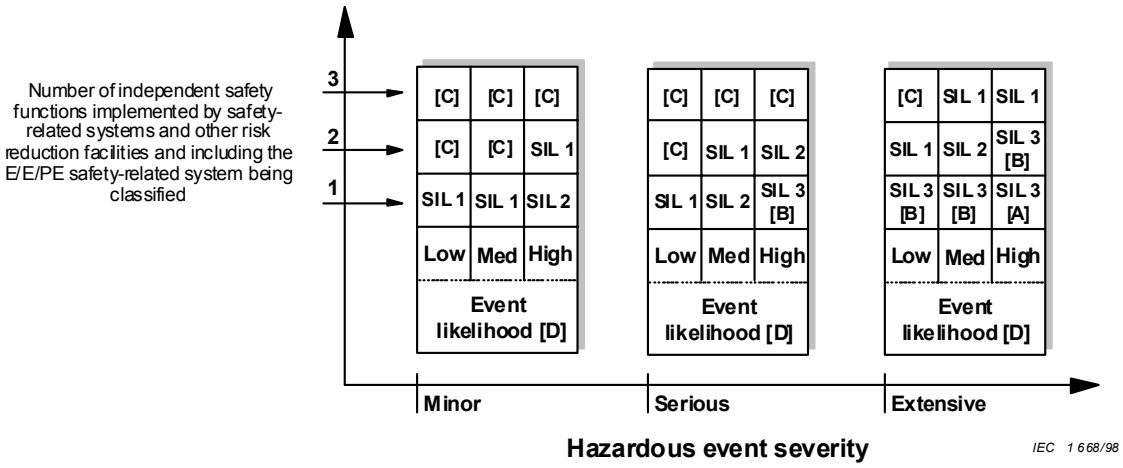
NOTE 1 This assumption is valid only if regular proof tests of the protection layers are carried out.

c) when one protection layer (see b) above) is added, then one order of magnitude improvement in safety integrity is achieved;

NOTE 2 This assumption is valid only if the safety-related systems and other risk reduction measures achieve an adequate level of independence.

d) only one E/E/PE safety-related system is used (but this may be in combination with an other technology safety-related system and/or other risk reduction measures), for which this method establishes the necessary safety integrity level;

e) The above considerations lead to the hazardous event severity matrix shown in Figure G.1. It should be noted that the matrix has been populated with example data to illustrate the general principles. For each specific situation, or sector comparable industries, a matrix similar to Figure G.1 would be developed and calibrated to the tolerable risk criteria applicable to the situation.



[A] One SIL 3 E/E/PE safety function does not provide sufficient risk reduction at this risk level. Additional risk reduction measures are required.

[B] One SIL 3 E/E/PE safety function may not provide sufficient risk reduction at this risk level. Hazard and risk analysis is required to determine whether additional risk reduction measures are necessary.

[C] An independent E/E/PE safety function is probably not required.

[D] Event likelihood is the likelihood that the hazardous event occurs without any safety function or other risk reduction measure.

[E] Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

Figure G.1 – Hazardous event severity matrix – example (illustrates general principles only)

Bibliography

[1] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[2] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[3] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

[4] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries*

[5] Health and Safety Executive (UK) *publication, ISBN 011 886368 1, Tolerability of risk from nuclear power stations,* <www.hse.gov.uk/nuclear/tolerability.pdf>

[6] The Motor Industry Research Association, 1994, ISBN 09524156 0 7, *Development guidelines for vehicle based software*

[7] Health and Safety Executive (UK) publication, ISBN 0 7176 2151 0, *Reducing Risks, Protecting People*, <www.hse.gov.uk/risk/theory/r2p2.pdf>

[8] CCPS ISBN 0-8169-0811-7, *Layer of Protection Analysis – Simplified Process Risk Assessment*

[9] ISO/IEC 31010, *Risk management – Risk assessment techniques*[3]

[10] ISO 10418:2003, *Petroleum and natural gas industries – Offshore production installations – Basic surface process safety systems*

[11] ISO/TR 14121-2*, Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods*

[12] ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

[13] IEC 60601 (all parts), *Medical electrical equipment*

[14] IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[15] IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

[16] IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[17] IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

[18] IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

_____

3 To be published.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch