IEC 61508-5

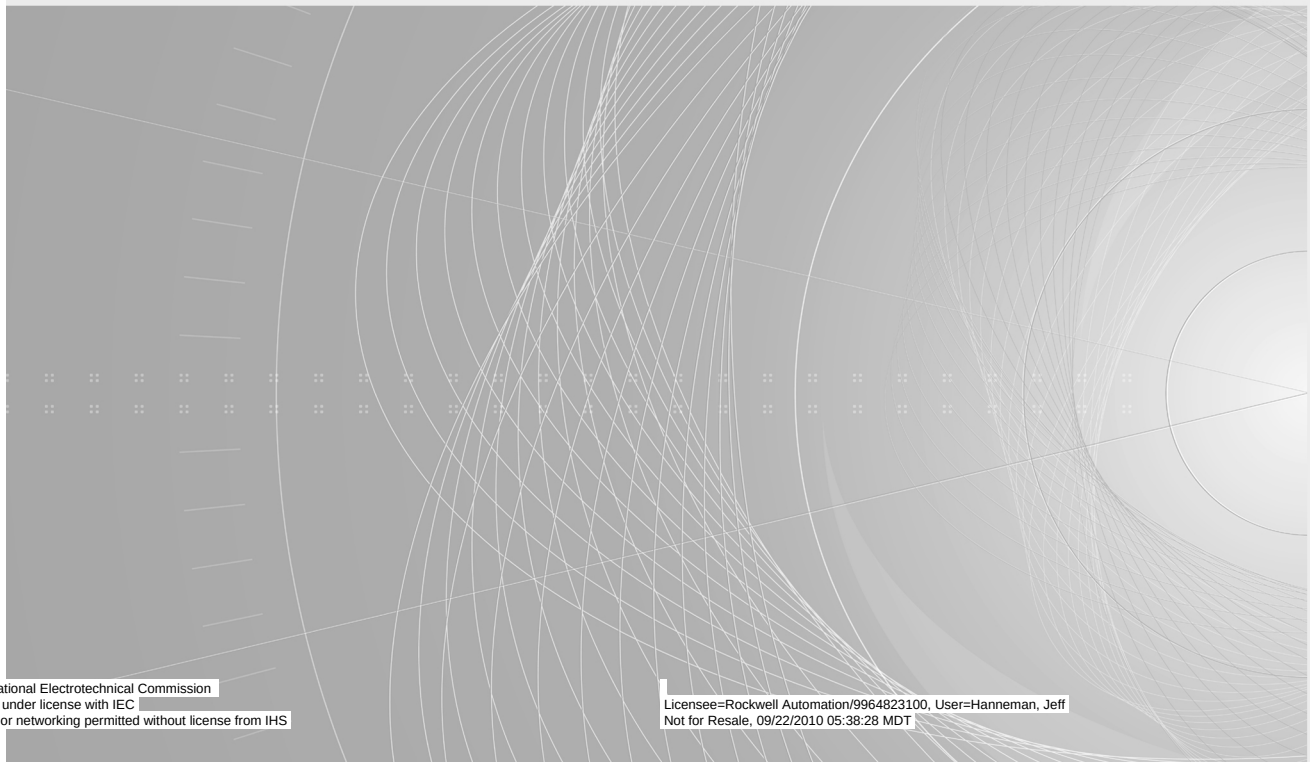
Edition 2.0 2010-04

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 It also gives information on projects, withdrawn and replaced publications.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.

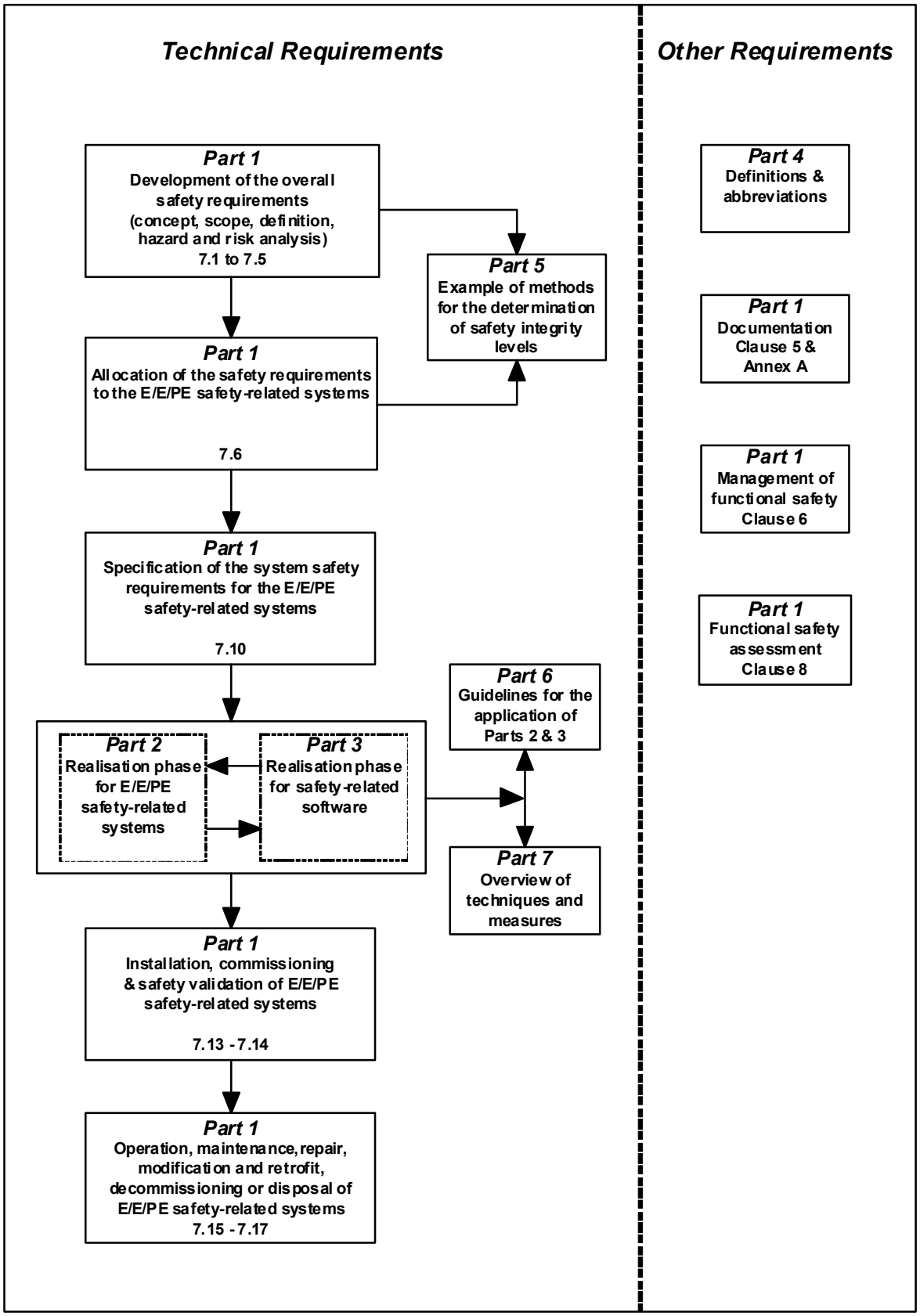


Figure 1 – Overall framework of the IEC 61508 series

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).

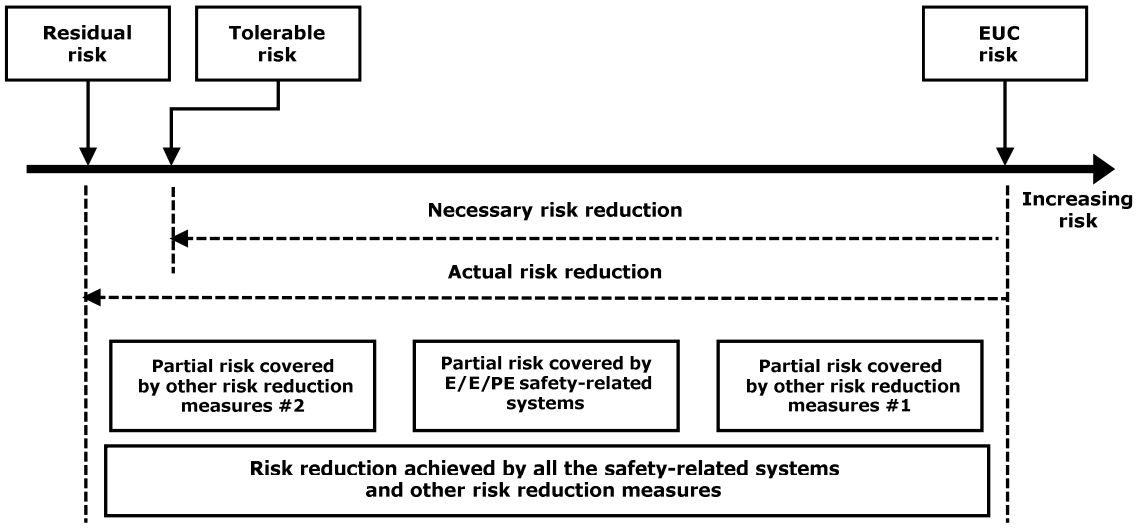


Figure A.1 – Risk reduction – general concepts (low demand mode of operation)

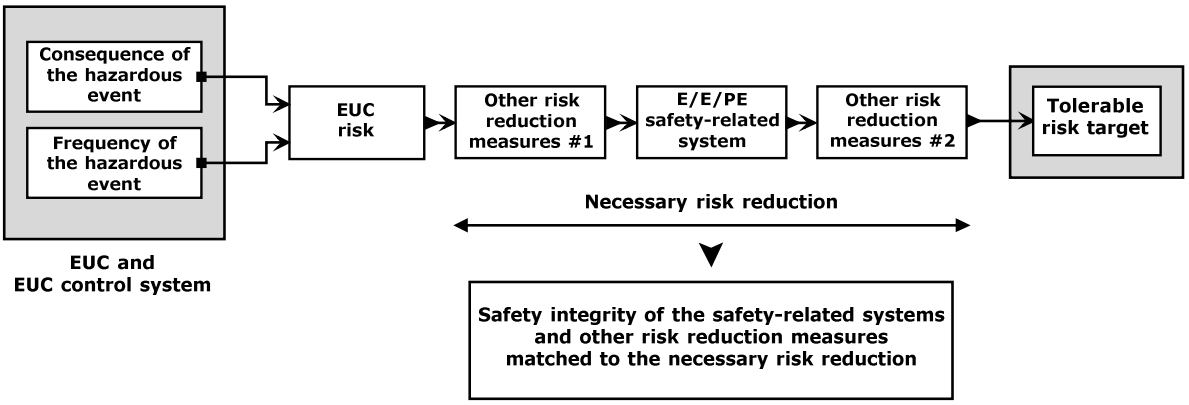


Figure A.2 – Risk and safety integrity concept

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.

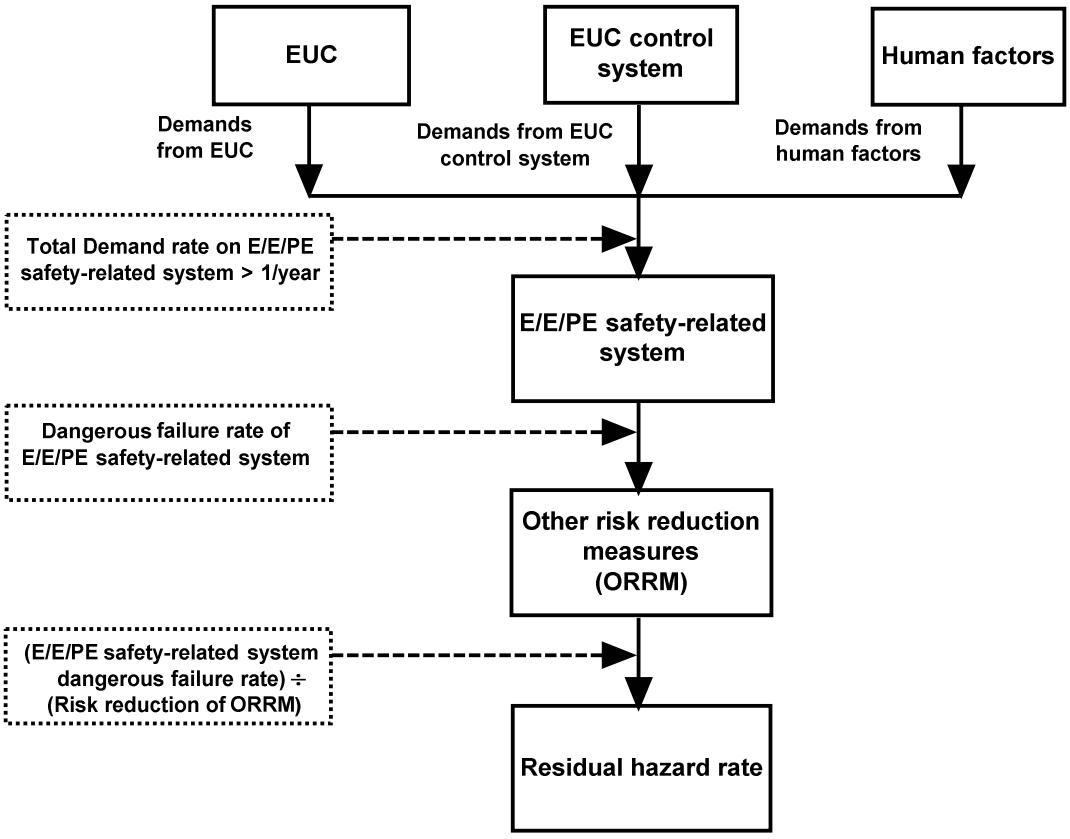


Figure A.3 – Risk diagram for high demand applications

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.

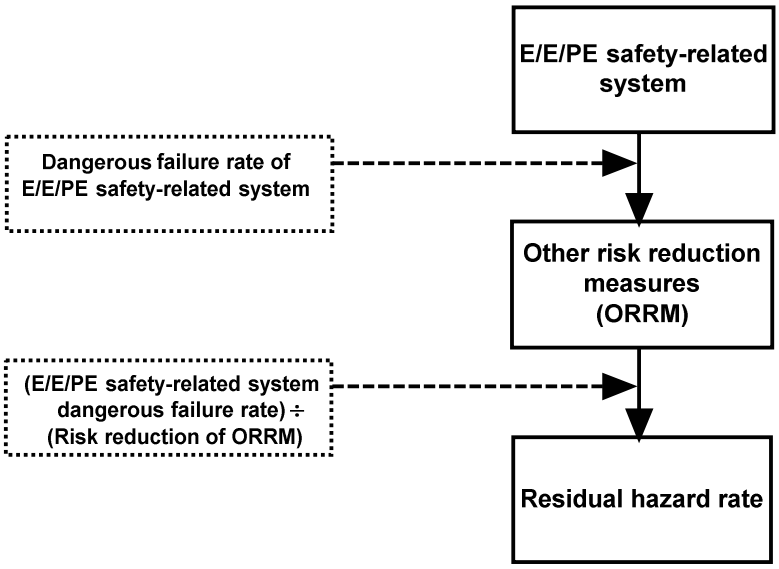


Figure A.4 – Risk diagram for continuous mode operation

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.

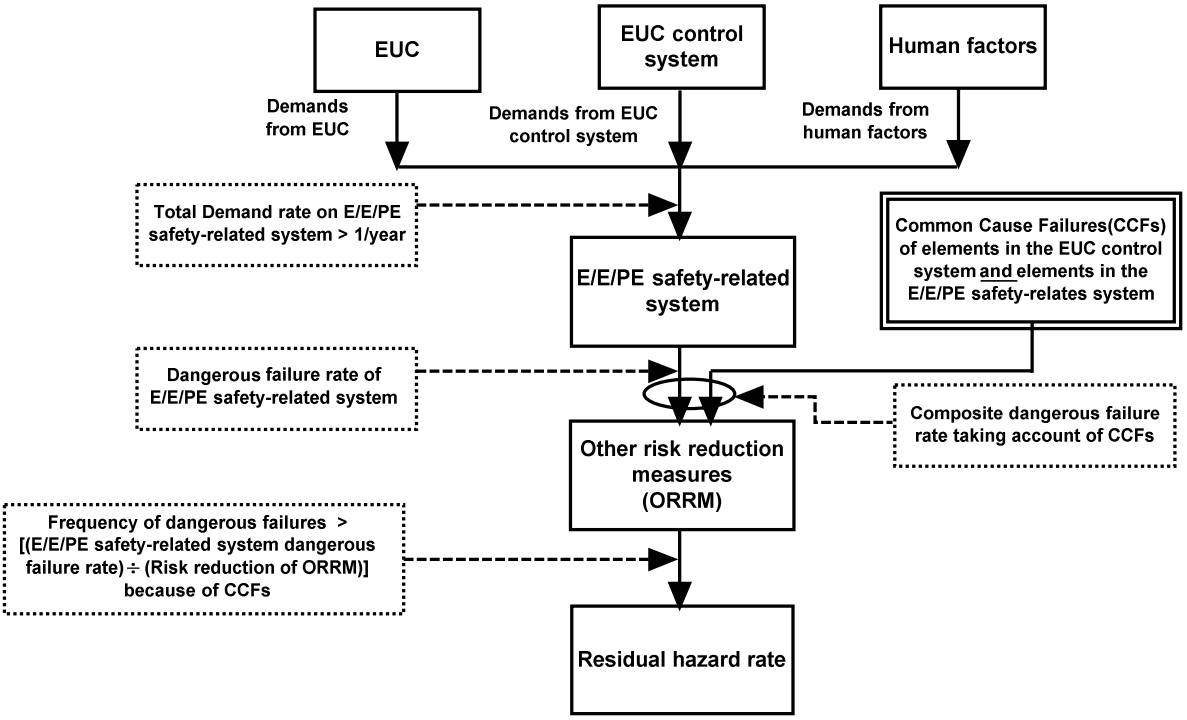


Figure A.5 – Illustration of common cause failures (CCFs) of elements in the EUC control system and elements in the E/E/PE safety-related system

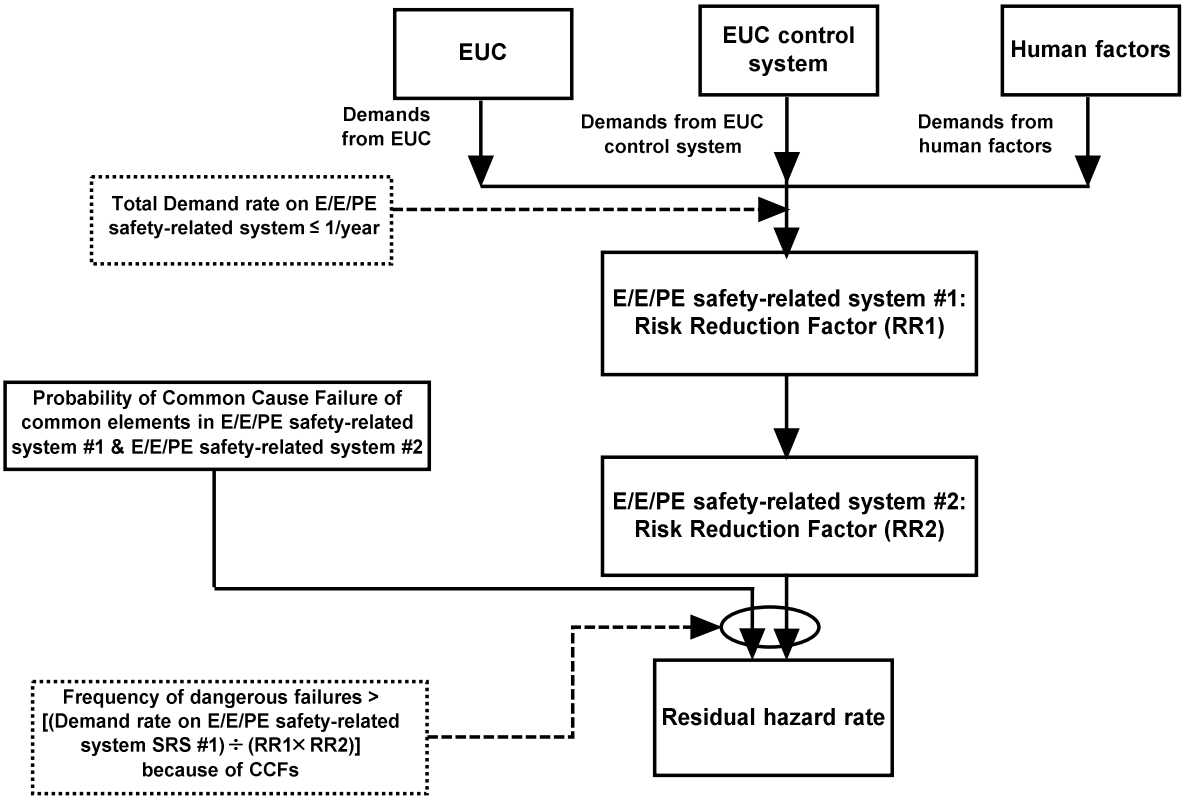


Figure A.6 – Common cause between two E/E/PE safety-related systems

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.

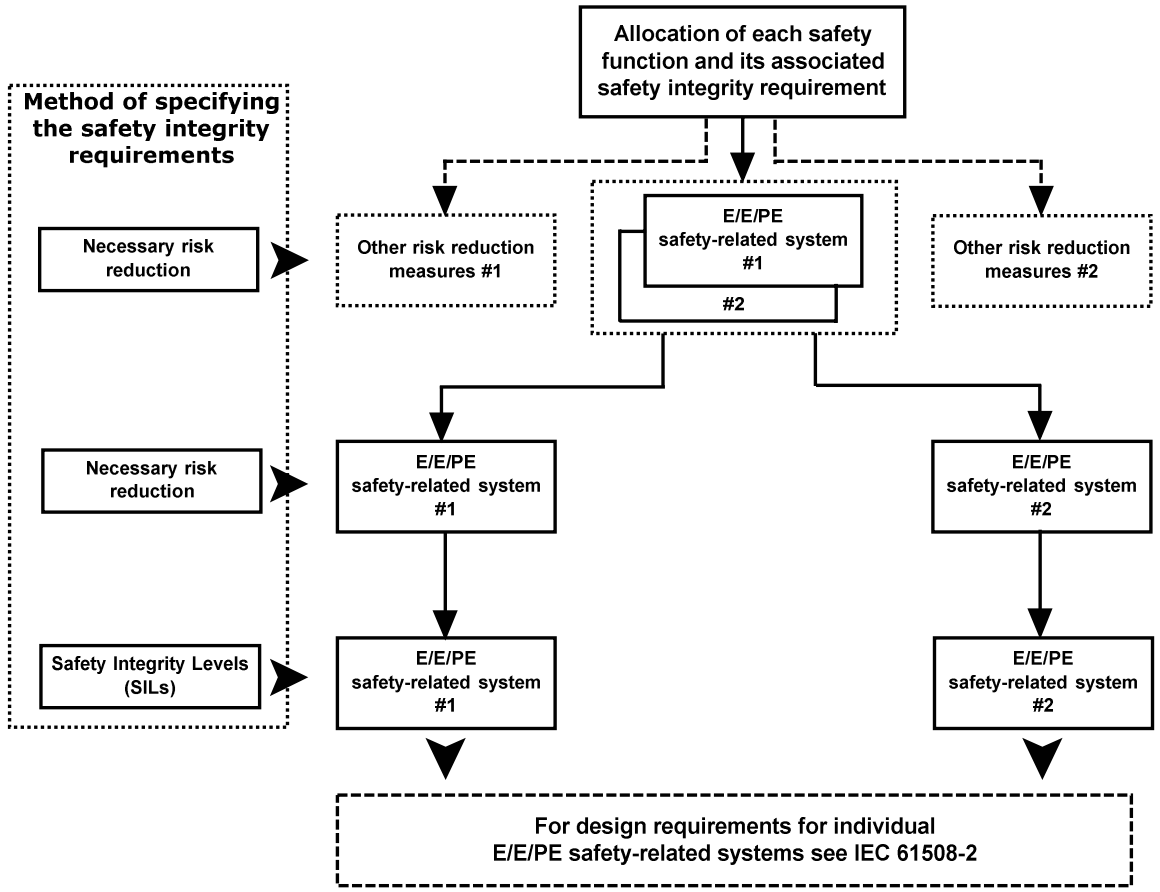
The safety integrity level target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1. Two parameters are specified, one for safety-related systems operating in a low demand mode of operation and one for safety-related systems operating in a high demand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

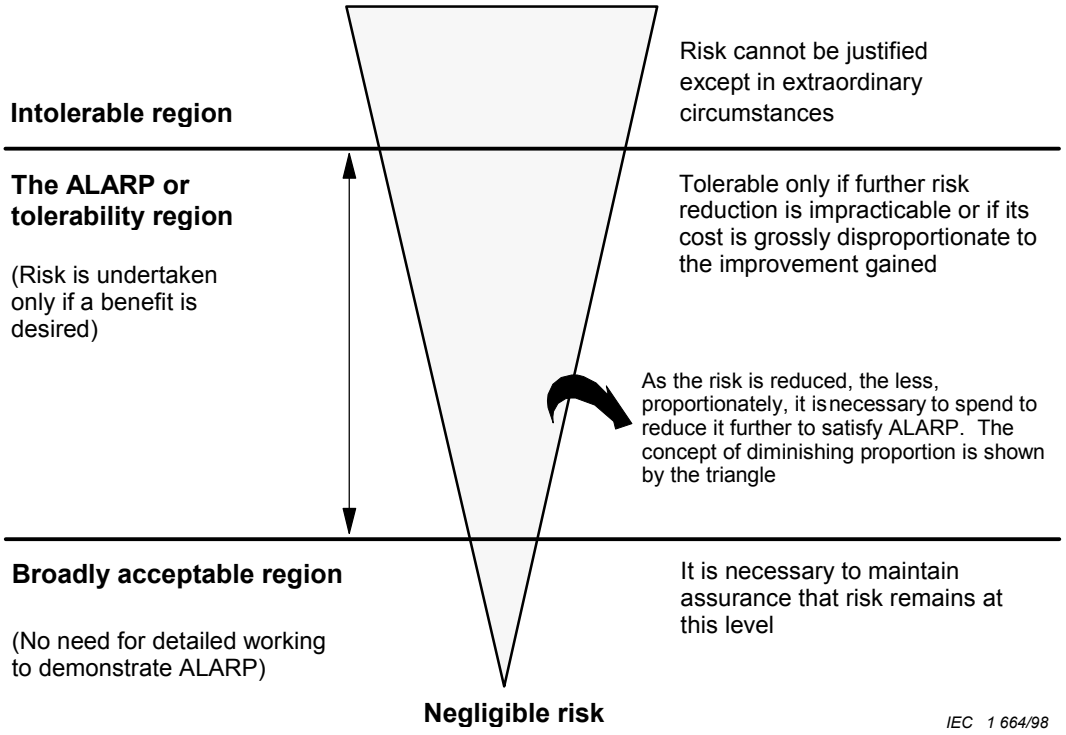


Figure C.1 – Tolerable risk and ALARP

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).

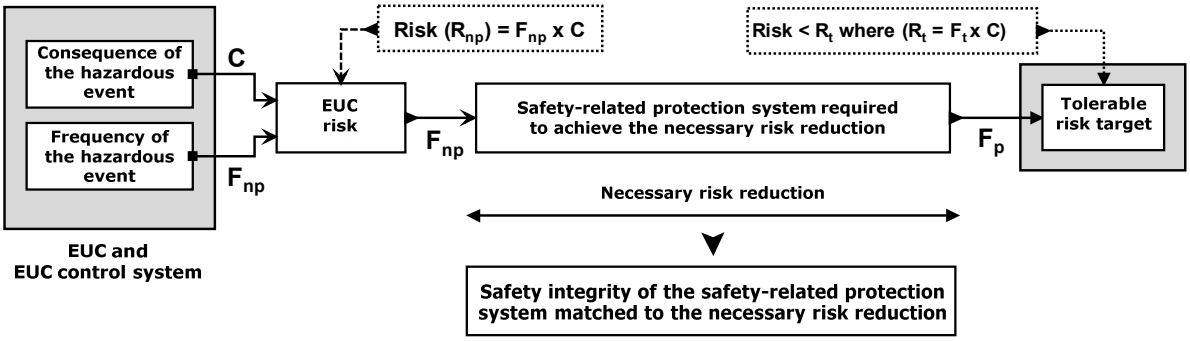


Figure D.1 – Safety integrity allocation – example for safety-related protection system

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.

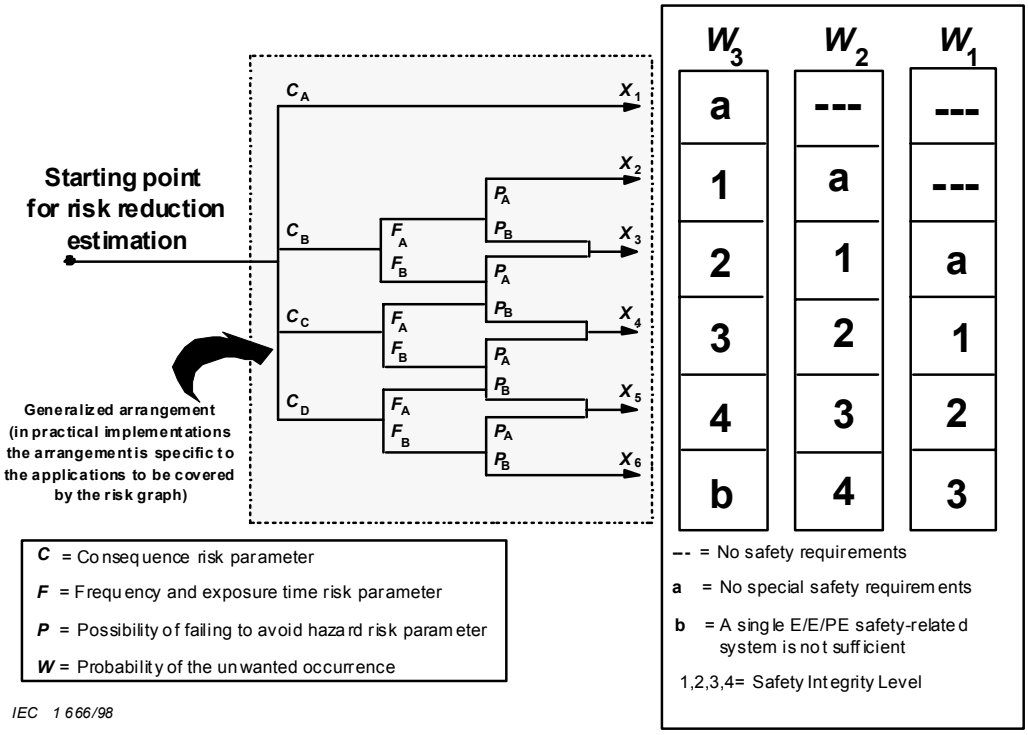
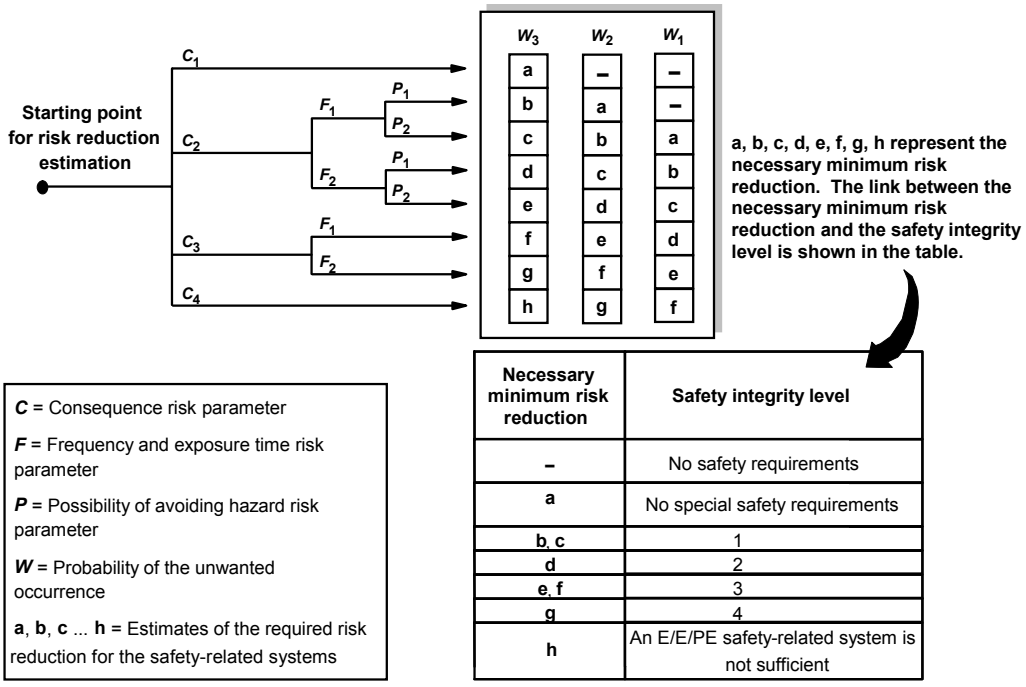


Figure E.1 – Risk Graph: general scheme



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;

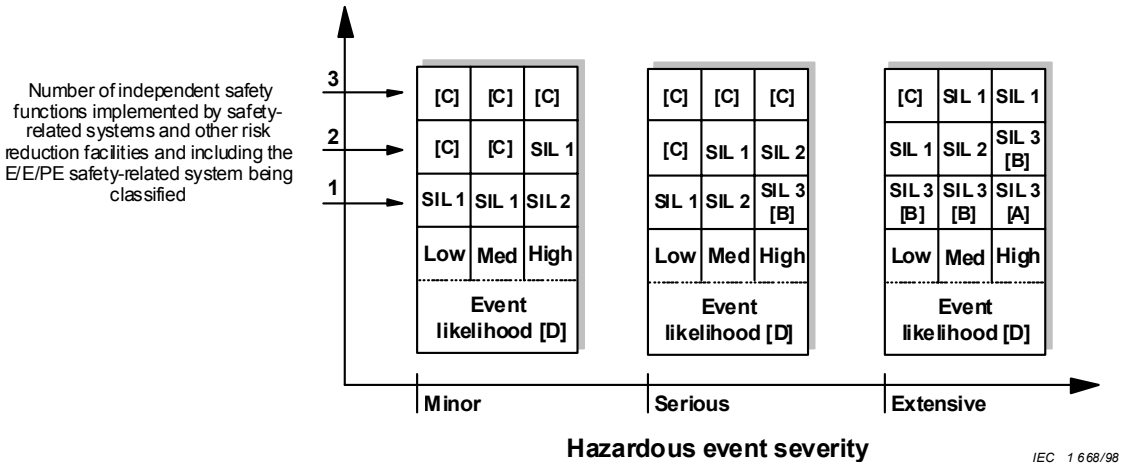
NOTE 1 This assumption is valid only if regular proof tests of the protection layers are carried out.

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.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61508-5 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition publiée en 1998 dont elle constitue une révision technique.

La présente édition a fait l'objet d'une révision approfondie et intègre de nombreux commentaires reçus lors des différentes phases de révision.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/552/FDIS	65A/576/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

Les systèmes comprenant des composants électriques et/ou électroniques sont utilisés depuis de nombreuses années pour exécuter des fonctions relatives à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (dénommés de manière générique systèmes électroniques programmables) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non relatives à la sécurité, mais aussi de plus en plus souvent relatives à la sécurité. Si l'on veut exploiter efficacement et en toute sécurité la technologie des systèmes informatiques, il est indispensable de fournir à tous les responsables suffisamment d'éléments relatifs à la sécurité pour les guider dans leurs prises de décisions.

La présente Norme internationale présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PE) qui sont utilisés pour réaliser des fonctions de sécurité. Cette approche unifiée a été adoptée afin de développer une politique technique rationnelle et cohérente concernant tous les systèmes électriques relatifs à la sécurité. Un objectif principal de cette approche est de faciliter le développement de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508.

NOTE 1 Des exemples de normes internationales de produit et d'application sectorielle basées sur la série CEI 61508 sont donnés dans la Bibliographie (voir références [1], [2] et [3]).

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, toute stratégie de sécurité doit non seulement prendre en compte tous les éléments d'un système individuel (par exemple, les capteurs, les appareils de commande et les actionneurs), mais également prendre en considération tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. Par conséquent, la présente Norme internationale, bien que traitant des systèmes E/E/PE relatifs à la sécurité, peut aussi fournir un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

Il est admis qu'il existe une grande variété d'applications utilisant des systèmes E/E/PE relatifs à la sécurité dans un grand nombre de secteurs, et couvrant un large éventail de complexité et de potentiel de dangers et de risques. Pour chaque application particulière, les mesures de sécurité requises dépendent de nombreux facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rend désormais possible la prescription de ces mesures dans les futures normes internationales de produit et d'application sectorielle, ainsi que dans les révisions des normes déjà existantes.

La présente Norme internationale

– concerne toutes les phases appropriées du cycle de vie de sécurité global des systèmes E/E/PE et du logiciel (par exemple, depuis le concept initial, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les systèmes E/E/PE permettent d'exécuter des fonctions de sécurité,
– a été élaborée dans le souci de la prise en compte de l'évolution rapide des technologies; le cadre fourni par la présente Norme internationale est suffisamment solide et étendu pour pourvoir aux évolutions futures,
– permet l'élaboration de normes internationales de produit et d'application sectorielle concernant les systèmes E/E/PE relatifs à la sécurité; il convient que l'élaboration de normes internationales de produit et d'application sectorielle dans le cadre de la présente norme, permette d'atteindre un haut niveau de cohérence (par exemple, pour ce qui est des principes sous-jacents, de la terminologie, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en sera une amélioration en termes de sécurité et de gains économiques,
– fournit une méthode de définition d'une spécification des exigences de sécurité nécessaire pour obtenir la sécurité fonctionnelle requise des systèmes E/E/PE relatifs à la sécurité,

– adopte une approche basée sur les risques qui permet de déterminer les exigences en matière d'intégrité de sécurité,

– introduit les niveaux d'intégrité de sécurité pour la spécification du niveau cible d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE relatifs à la sécurité,

NOTE 2 La norme ne spécifie aucune exigence de niveau d'intégrité de sécurité pour aucune fonction de sécurité, ni comment le niveau d'intégrité de sécurité est déterminé. Elle fournit en revanche un cadre conceptuel basé sur les risques, ainsi que des exemples de méthodes.

– fixe des objectifs chiffrés de défaillance pour les fonctions de sécurité exécutées par les systèmes E/E/PE relatifs à la sécurité, qui sont en rapport avec les niveaux d'intégrité de sécurité,

– fixe une limite inférieure pour les objectifs chiffrés de défaillance pour une fonction de sécurité exécutée par un système E/E/PE relatif à la sécurité unique. Pour des systèmes E/E/PE relatifs à la sécurité fonctionnant

  – en mode de fonctionnement à faible sollicitation, la limite inférieure est fixée pour une probabilité moyenne de défaillance dangereuse de 10^{-5} en cas de sollicitation,

  – en mode de fonctionnement continu ou à sollicitation élevée, la limite inférieure est fixée à une fréquence moyenne de défaillance dangereuse de 10^{-9} [h^{-1}],

NOTE 3 Un système E/E/PE relatif à la sécurité unique n'implique pas nécessairement une architecture à un seul canal.

NOTE 4 Dans le cas de systèmes non complexes, il peut être possible de concevoir des systèmes relatifs à la sécurité ayant des valeurs plus basses pour l'intégrité de sécurité cible. Il est toutefois considéré que ces limites représentent ce qui peut être réalisé à l'heure actuelle pour des systèmes relativement complexes (par exemple, des systèmes électroniques programmables relatifs à la sécurité).

– établit des exigences fondées sur l'expérience et le jugement acquis dans le domaine des applications industrielles afin d'éviter des anomalies systématiques ou pour les maintenir sous contrôle. Même si, en général, la probabilité d'occurrence des défaillances systématiques ne peut être quantifiée, la norme permet cependant pour une fonction de sécurité spécifique, de déclarer que l'objectif chiffré de défaillance associé à cette fonction de sécurité peut être réputé atteint si toutes les exigences de la norme sont remplies,

– introduit une capabilité systématique s'appliquant à un élément du fait qu'il permet d'assurer que l'intégrité de sécurité systématique satisfait aux exigences du niveau d'intégrité de sécurité spécifié,

– adopte une large gamme de principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais n'utilise pas de manière explicite le concept de sécurité intrinsèque. Les principes de « sécurité intrinsèque » peuvent toutefois être applicables, l'adoption de ces concepts étant par ailleurs acceptable sous réserve de la satisfaction aux exigences des articles concernés de la norme.

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

1 Domaine d'application

1.1 La présente partie de la CEI 61508 fournit des informations sur

– les concepts sous-jacents à la notion de risque et les liens entre le risque et l'intégrité de sécurité (voir Annexe A),

– un certain nombre de méthodes qui permettent de déterminer les niveaux d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité (voir Annexes B, C, D et E).

La méthode retenue dépend du secteur d'application et des conditions spécifiques à prendre en considération. Les Annexes C, D, E, F et G illustrent les approches quantitatives et qualitatives et ont été simplifiées dans le but d'illustrer les principes sous-jacents. Ces annexes ont été incluses pour illustrer les principes généraux d'un certain nombre de méthodes mais ne fournissent pas une interprétation figée. Il convient que les personnes souhaitant appliquer les méthodes indiquées dans ces annexes consultent les sources documentaires référencées.

NOTE Pour plus d'informations concernant les approches illustrées par les Annexes B et E, voir les références [5] et [8] dans la Bibliographie. Voir aussi la référence [6] dans la Bibliographie qui décrit une autre approche.

1.2 Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont des publications fondamentales de sécurité, bien que ce statut ne soit pas applicable dans le contexte des systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.3 de la CEI 61508-4). En tant que publications fondamentales de sécurité, ces normes sont destinées à être utilisées par les comités d'études pour la préparation des normes conformément aux principes contenus dans le Guide CEI 104 et le Guide ISO/CEI 51. Les CEI 61508-1, CEI 61508-2, CEI 61508-3 et CEI 61508-4 sont également destinées à être utilisées comme publications autonomes. La fonction de sécurité horizontale de la présente norme internationale ne s'applique pas aux appareils médicaux conformes à la série CEI 60601.

1.3 Une des responsabilités incombant à un comité d'études consiste, dans toute la mesure du possible, à utiliser les publications fondamentales de sécurité pour la préparation de ses publications. Dans ce contexte, les exigences, les méthodes ou les conditions d'essai de cette publication fondamentale de sécurité ne s'appliquent que si elles sont indiquées spécifiquement ou incluses dans les publications préparées par ces comités d'études.

1.4 La Figure 1 illustre la structure générale de la série CEI 61508 et montre le rôle que la CEI 61508-5 joue dans la réalisation de la sécurité fonctionnelle pour les systèmes E/E/PE relatifs à la sécurité.

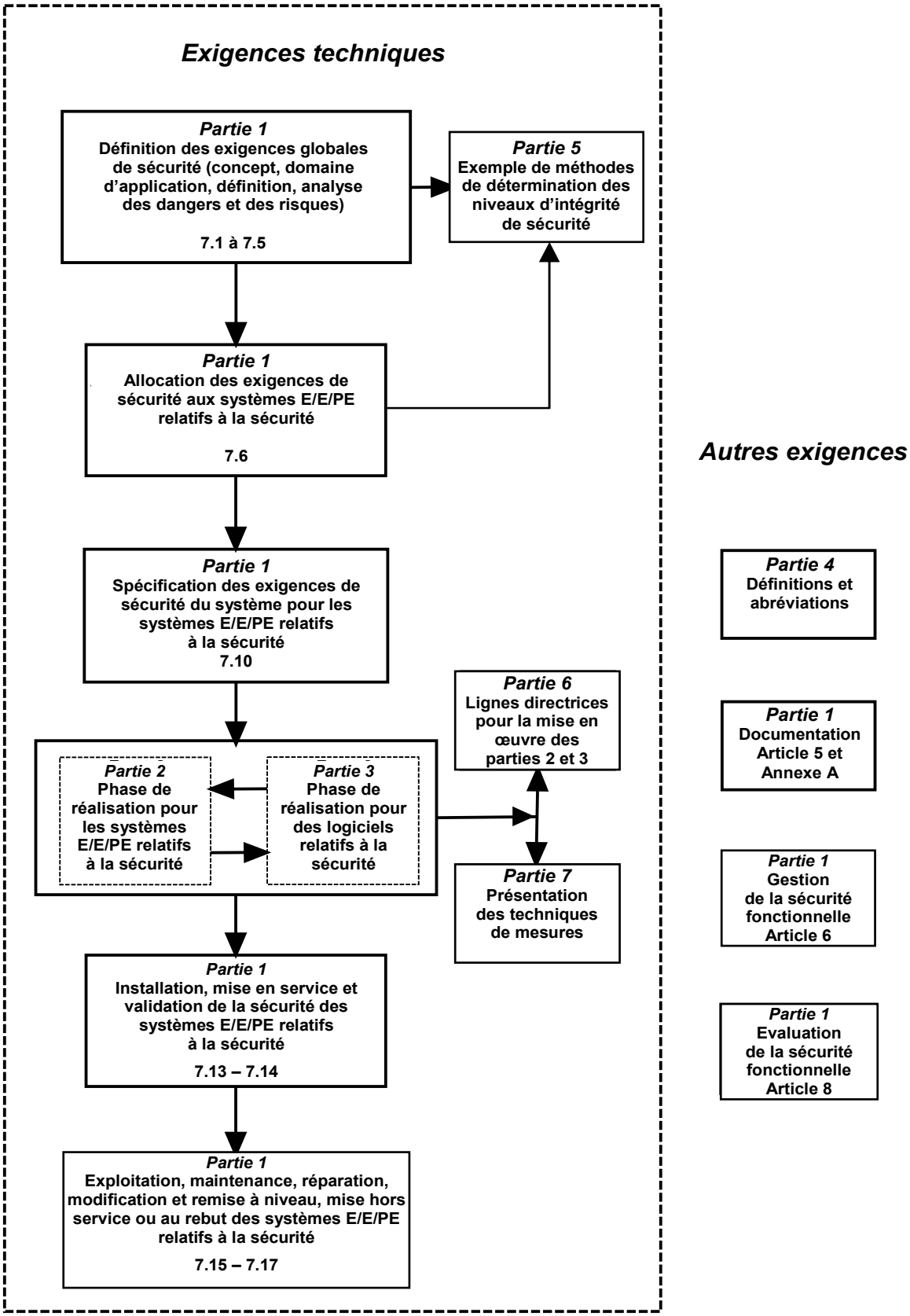


Figure 1 – Structure générale de la série CEI 61508

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

3 Définitions et abréviations

Pour les besoins du présent document, les définitions et les abréviations données dans la CEI 61508-4 s'appliquent.

Annexe A
(informative)

Risques et intégrité de sécurité – Concepts généraux

A.1 Généralités

La présente annexe donne des informations sur les concepts sous-jacents à la notion de risque et les liens entre le risque et l'intégrité de sécurité.

A.2 Réduction de risque nécessaire

La réduction de risque nécessaire (voir 3.5.18 de la CEI 61508-4) est la réduction du risque qui doit être réalisée pour atteindre l'objectif de risque tolérable dans une situation spécifique (qui peut être définie soit qualitativement[1] soit quantitativement[2]). Le concept de réduction de risque nécessaire est d'une importance fondamentale dans la réalisation de la spécification des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité (en particulier, les exigences d'intégrité de sécurité qui font partie de la spécification des exigences de sécurité). La détermination du risque tolérable pour un événement dangereux spécifique a pour but d'établir ce qui est jugé raisonnable compte tenu de la fréquence (ou probabilité) de l'événement dangereux et de ses conséquences spécifiques. Les systèmes relatifs à la sécurité sont conçus pour réduire la fréquence (ou probabilité) de l'événement dangereux et/ou les conséquences de l'événement dangereux.

Le risque tolérable dépend de nombreux facteurs (par exemple, la gravité des blessures, le nombre de personnes exposées au danger, la fréquence à laquelle une personne ou des personnes sont exposées au danger et la durée de cette exposition). La perception et le point de vue des personnes exposées à l'événement dangereux sont des facteurs importants. La définition du risque tolérable d'une application spécifique tient compte d'un grand nombre de points. Ces derniers incluent:

– les exigences légales, générales et celles relevant directement de l'application spécifique,
– les lignes directrices émises par l'autorité réglementaire appropriée en matière de sécurité,
– les discussions et accords avec les différentes parties impliquées dans l'application,
– les normes et lignes directrices de l'industrie,
– les discussions et accords internationaux; le rôle des normes nationales et internationales devient de plus en plus important dans la définition de critères de risque tolérable appropriés pour les applications spécifiques,
– les avis indépendants les plus pertinents émis par des organismes consultatifs représentant l'industrie, les experts et les scientifiques.

La détermination des exigences d'intégrité de sécurité du ou des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque, permettant d'atteindre l'objectif da fréquence tolérable d'un événement dangereux, doit tenir compte des caractéristiques du risque pertinentes pour l'application. La fréquence tolérable dépend des exigences légales en vigueur dans le pays d'application et des critères spécifiés par l'organisme utilisateur. Les

---

1 Lors de la détermination du risque tolérable, la réduction de risque nécessaire doit être établie. Les Annexes E et G du présent document décrivent les grandes lignes des méthodes qualitatives, bien que dans les exemples donnés, la réduction de risque nécessaire soit incluse implicitement par la spécification de l'exigence de niveau d'intégrité de sécurité plutôt que clairement explicitée par une valeur numérique de réduction de risque requise.

2 Par exemple, l'évènement dangereux, qui amène une conséquence spécifique, ne doit pas se produire à une fréquence supérieure à plus d'une fois en 10^8 h.

problèmes susceptibles de devoir être pris en compte ainsi que leur mode possible d'application aux systèmes E/E/PE relatifs à la sécurité sont abordés ci-après.

A.2.1 Risque individuel

Généralement, des objectifs différents sont définis pour les travailleurs et le public. L'objectif relatif au risque individuel des travailleurs concerne la personne la plus exposée et peut être exprimé comme le risque total par an engendré par toutes les activités professionnelles. L'objectif s'applique à une personne fictive et doit par conséquent tenir compte du pourcentage de temps que la personne passe au travail. L'objectif s'applique à tous les risques encourus par la personne exposée et le risque tolérable pour une fonction de sécurité individuelle nécessite de tenir compte d'autres risques.

La réduction du risque total au-dessous d'une cible spécifiée peut être garantie de plusieurs façons. Une méthode consiste à considérer tous les risques encourus par la personne la plus exposée et d'en faire la somme. Ceci peut se révéler difficile lorsqu'une personne est exposée à de nombreux risques et lorsque des décisions rapides doivent être prises pour l'élaboration du système. Une autre approche consiste à allouer un pourcentage de l'objectif de risque individuel global à chaque fonction de sécurité considérée. Le pourcentage alloué peut généralement être déterminé sur la base de l'expérience acquise pour le type d'installation considéré.

Il convient que l'objectif appliqué à une fonction de sécurité individuelle tienne également compte du principe prudentiel de la méthode d'analyse de risque utilisée. Toutes les méthodes qualitatives telles que les graphes de risque impliquent une évaluation des paramètres critiques qui contribuent au risque. Les facteurs liés au risque sont la conséquence de l'événement dangereux et sa fréquence. La détermination de ces facteurs peut nécessiter de prendre en compte un certain nombre de paramètres de risque tels que la vulnérabilité à l'événement dangereux, le nombre de personnes susceptibles d'être affectées par l'événement dangereux, la probabilité de la présence d'une personne en cas d'occurrence de l'événement dangereux (c'est-à-dire l'occupation) et la possibilité d'éviter l'événement dangereux.

Les méthodes qualitatives impliquent généralement de déterminer si un paramètre s'inscrit dans une étendue donnée. Lorsqu'on utilise ces méthodes, les descriptions des critères nécessitent de pouvoir établir un degré élevé de confiance dans le fait que la cible spécifiée pour les risques n'est pas dépassée. Ceci peut impliquer d'établir des limites d'étendue pour tous les paramètres permettant ainsi aux applications utilisant tous les paramètres aux conditions limites de satisfaire aux critères de risque spécifiés relatifs à la sécurité. Cette approche consistant à établir les limites d'étendue est très prudente dans la mesure où il n'existe que quelques rares applications pour lesquelles tous les paramètres se situent dans le cas le plus défavorable de l'étendue. Un objectif plus faible s'applique généralement lorsque les personnes du public doivent être exposées au risque résultant de la défaillance d'un système E/E/PE relatif à la sécurité.

A.2.2 Risque sociétal

Ce type de risque survient lorsque plusieurs accidents mortels sont susceptibles de se produire du fait d'événements uniques. Ces événements sont appelés sociétaux car ils risquent de provoquer une réaction au niveau social et politique. Le public et les groupes sociaux peuvent de manière significative ne pas tolérer des événements à conséquences élevées et dans certains cas ceci doit être pris en compte. Le critère applicable au risque sociétal est souvent exprimé comme une fréquence cumulée maximale de blessures mortelles affectant un nombre spécifié de personnes. Le critère est généralement spécifié sous la forme d'une ou plusieurs droites tracées sur une courbe F/N où F est la fréquence cumulée des dangers et N est le nombre d'accidents mortels résultant de ces dangers. La relation est généralement représentée par une droite tracée sur des échelles logarithmiques. La pente de la droite dépend de l'étendue dans laquelle l'entité considère le risque comme intolérable à des niveaux supérieurs de conséquence. L'exigence garantit que la fréquence cumulée pour

un nombre spécifié d'accidents mortels est inférieure à la fréquence cumulée exprimée par la courbe F/N. (voir la référence [7] de la Bibliographie.)

A.2.3 Amélioration continue

L'Annexe C traite des principes de réduction de risque jusqu'à un niveau qui soit aussi faible que raisonnablement possible.

A.2.4 Profil de risque

La détermination des critères de risque à appliquer à un danger spécifique peut nécessiter de tenir compte du profil de risque sur la durée de vie du produit. Le risque résiduel varie d'un niveau minimal, juste après un essai périodique ou une réparation, à un niveau maximal, juste avant un essai périodique. Ceci peut nécessiter d'être pris en compte par les entités qui spécifient les critères de risque à appliquer. Si les intervalles entre essais périodiques sont importants, il peut alors se révéler approprié de spécifier la probabilité de danger maximale acceptable juste avant un essai périodique ou de spécifier que la $PFD_{(t)}$ ou $PFH_{(t)}$ est inférieure à la limite SIL supérieure de plus d'un pourcentage spécifié de temps (par exemple, 90 %).

A.3 Rôle des systèmes E/E/PE relatifs à la sécurité

Les systèmes E/E/PE relatifs à la sécurité contribuent à obtenir la réduction de risque nécessaire dans le but d'atteindre l'objectif de risque tolérable.

Un système relatif à la sécurité

– met en oeuvre les fonctions de sécurité requises et nécessaires pour atteindre un état de sécurité de l'équipement commandé, ou maintenir l'équipement commandé dans un état de sécurité, et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité ou dispositifs externes de réduction de risque, l'intégrité de sécurité nécessaire des fonctions de sécurité requises (voir 3.5.1 de la CEI 61508-4).

NOTE 1 La première partie de la définition spécifie que le système relatif à la sécurité doit accomplir les fonctions de sécurité qui seraient spécifiées dans la spécification des exigences des fonctions de sécurité. Par exemple, la spécification des exigences des fonctions de sécurité peut spécifier que lorsque la température atteint x, la vanne y doit s'ouvrir pour permettre à l'eau d'entrer dans le récipient.

NOTE 2 La seconde partie de la définition spécifie que les fonctions de sécurité doivent être accomplies par les systèmes relatifs à la sécurité avec un degré de confiance convenant à l'application afin de permettre d'atteindre l'objectif de risque tolérable.

Une personne peut faire partie intégrante d'un système E/E/PE relatif à la sécurité. Par exemple, une personne peut recevoir des informations sur l'état de l'EUC depuis un écran et exécuter une activité de sécurité à partir de cette information.

Les systèmes E/E/PE relatifs à la sécurité peuvent fonctionner en mode faible sollicitation ou en mode sollicitation élevée ou mode continu (voir 3.5.16 de la CEI 61508-4).

A.4 Intégrité de sécurité

L'intégrité de sécurité est définie comme la probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises, dans toutes les conditions spécifiées et dans une période de temps spécifiée (3.5.4 de la CEI 61508-4). L'intégrité de sécurité renvoie aux performances des systèmes relatifs à la sécurité lors de l'exécution de fonctions de sécurité (les fonctions de sécurité à mettre en oeuvre sont présentées dans la spécification des exigences concernant les fonctions de sécurité).

On considère que l'intégrité de sécurité se compose des deux éléments suivants:

– Intégrité de sécurité du matériel; cette partie de l'intégrité de sécurité est relative aux défaillances aléatoires du matériel en mode de défaillance dangereux (voir 3.5.7 de la CEI 61508-4). L'obtention du niveau d'intégrité de sécurité spécifié pour un matériel relatif à la sécurité peut être estimée avec une précision suffisante et les exigences peuvent par conséquent être réparties entre les sous-systèmes en utilisant les règles usuelles de combinaison de probabilités. Des architectures redondantes peuvent être nécessaires pour réaliser l'intégrité de sécurité adéquate du matériel.

– Intégrité de sécurité systématique; cette partie de l'intégrité de sécurité est relative aux défaillances systématiques en mode de défaillance dangereux (voir 3.5.6 de la CEI 61508-4). Bien que le taux moyen de défaillance dû à des défaillances systématiques puisse être estimé, les données de défaillances résultant d'anomalies de conception et de défaillances de cause commune font qu'il peut être difficile de prévoir la distribution des défaillances. L'incertitude des calculs de probabilité des défaillances pour une situation spécifique (par exemple la probabilité d'une défaillance d'un système de protection relatif à la sécurité) s'en trouve augmentée. Il est donc nécessaire d'opter pour les techniques les plus à même de réduire cette incertitude. Toutefois, les mesures prises pour réduire la probabilité d'une défaillance aléatoire du matériel n'ont pas nécessairement un effet correspondant sur la probabilité d'une défaillance systématique. Les techniques telles que les redondances de matériel réalisées par deux canaux identiques, qui sont certes très efficaces pour maîtriser les défaillances aléatoires du matériel, n'ont qu'un effet très limité dans la réduction des défaillances systématiques telles que des erreurs de logiciel.

A.5 Modes de fonctionnement et détermination du niveau d'intégrité de sécurité (SIL)

Le mode de fonctionnement concerne la façon dont une fonction de sécurité est prévue d'être utilisée par rapport à la fréquence des sollicitations dont elle fait l'objet et qui peut être:

– **mode faible sollicitation:** pour lequel la fréquence des sollicitations sur la fonction de sécurité n'est pas supérieure à une par an, ou

– **mode sollicitation élevée:** pour lequel la fréquence des sollicitations sur la fonction de sécurité est supérieure à une par an, ou

– **mode continu:** pour lequel la sollicitation sur la fonction de sécurité est continue.

Les Tableaux 2 et 3 de la CEI 61508-1 détaillent les objectifs chiffrés de défaillance associés aux quatre niveaux d'intégrité de sécurité pour chacun des modes de fonctionnement. Les modes de fonctionnement sont expliqués plus en détail dans les alinéas suivants.

A.5.1 Intégrité de sécurité et réduction de risque pour les applications en mode faible sollicitation

L'intégrité de sécurité requise des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque doit être à un niveau tel que:

– la probabilité moyenne de non fonctionnement en cas de sollicitation des systèmes relatifs à la sécurité soit suffisamment faible pour éviter que la fréquence des événements dangereux n'excède la valeur requise pour atteindre l'objectif de risque tolérable, et/ou

– les systèmes relatifs à la sécurité aient une action suffisante sur les conséquences des défaillances pour atteindre le niveau de risque tolérable.

La Figure A.1 illustre les concepts généraux de réduction de risque. Le modèle général suppose que:

– il existe un EUC et un système de commande,

– il existe des problèmes liés au facteur humain,

– les dispositifs de protection comprennent:

  – des systèmes E/E/PE relatifs à la sécurité,

  – des dispositifs externes de réduction de risque.

NOTE La Figure A.1 est un modèle de risque généralisé pour illustrer les principes généraux. Le modèle de risque pour une application spécifique doit être développé en tenant compte de la manière spécifique selon laquelle la réduction de risque nécessaire est accomplie par les systèmes E/E/PE relatifs à la sécurité et/ou les dispositifs externes de réduction de risque. Le modèle de risque résultant peut cependant différer de celui présenté à la Figure A.1.

Les divers risques indiqués aux Figures A.1 et A.2 sont les suivants:

– risque EUC: pour les événements dangereux spécifiés, risque encouru par l'EUC, son système de commande et les facteurs humains associés: aucun dispositif de protection n'est pris en compte dans la détermination de ce risque (voir 3.1.9 de la CEI 61508-4),
– risque tolérable: risque accepté dans un certain contexte et fondé sur les valeurs admises de la société (voir 3.1.7 de la CEI 61508-4),
– risque résiduel: dans le contexte de la présente norme, pour les événements dangereux spécifiés, risque encouru par l'EUC, son système de commande et les problèmes liés aux facteurs humain, mais avec ajout de systèmes E/E/PE relatifs à la sécurité et de dispositifs externes de réduction de risque (voir aussi 3.1.7 de la CEI 61508-4).

Le risque EUC est fonction du risque associé à l'EUC lui-même, compte tenu toutefois de la réduction de risque résultant du système de commande de l'EUC. La présente norme définit des contraintes régissant les déclarations qui peuvent être formulées de manière à prévenir des déclarations déraisonnables pour l'intégrité de sécurité du système de commande de l'EUC (voir 7.5.2.5 de la CEI 61508-1).

La réduction de risque nécessaire est atteinte par une combinaison de tous les dispositifs de protection relatifs à la sécurité. La réduction de risque nécessaire pour atteindre l'objectif de risque tolérable spécifié, à partir d'un point initial du risque EUC, est représentée à la Figure A.1 (applicable à une fonction de sécurité fonctionnant en mode faible sollicitation).

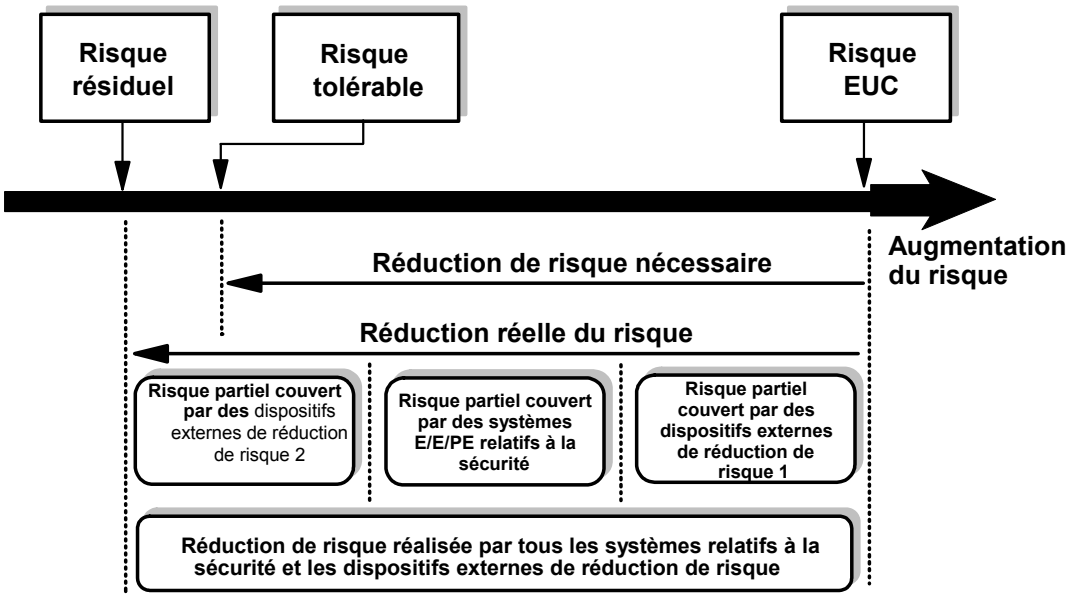


Figure A.1 – Réduction de risque – concepts généraux (mode de fonctionnement faible sollicitation)

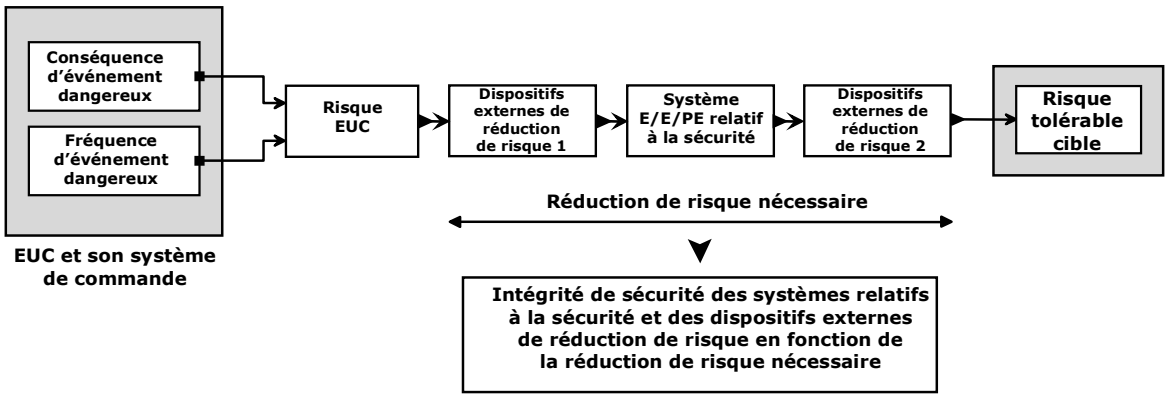


Figure A.2 – Concepts de risque et d'intégrité de sécurité

A.5.2 Intégrité de sécurité pour des applications en mode sollicitation élevée

L'intégrité de sécurité requise des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque doit être à un niveau tel que:

– la probabilité moyenne de défaillance en cas de sollicitation des systèmes relatifs à la sécurité soit suffisamment faible pour éviter que la fréquence des événements dangereux n'excède la valeur requise pour atteindre l'objectif de risque tolérable, et/ou

– la probabilité moyenne de défaillance par heure du système relatif à la sécurité soit suffisamment faible pour éviter que la fréquence des événements dangereux n'excède la valeur requise pour atteindre l'objectif de risque tolérable.

La Figure A.3 illustre les concepts généraux des applications en mode sollicitation élevée. Le modèle général suppose:

– qu'il existe un EUC et un système de commande,

– qu'il existe des problèmes liés au facteur humain,

– que les dispositifs de protection comprennent:

  – des systèmes E/E/PE relatifs à la sécurité fonctionnant en mode sollicitation élevée,

  – des dispositifs externes de réduction de risque.

Les différentes sollicitations sur les systèmes E/E/PE relatifs à la sécurité sont les suivantes:

– sollicitations générales de l'EUC,

– sollicitations résultant de défaillances dans le système de commande de l'EUC,

– sollicitations résultant d'erreurs humaines.

Si le taux de sollicitation total résultant de toutes les sollicitations sur le système dépasse 1 par an, le facteur critique est le taux de défaillance dangereuse du système E/E/PE relatif à la sécurité. La fréquence de risque résiduel ne peut jamais dépasser le taux de défaillance dangereuse du système E/E/PE relatif à la sécurité. Elle peut être inférieure si des dispositifs externes de réduction de risque réduisent la probabilité de dommage.

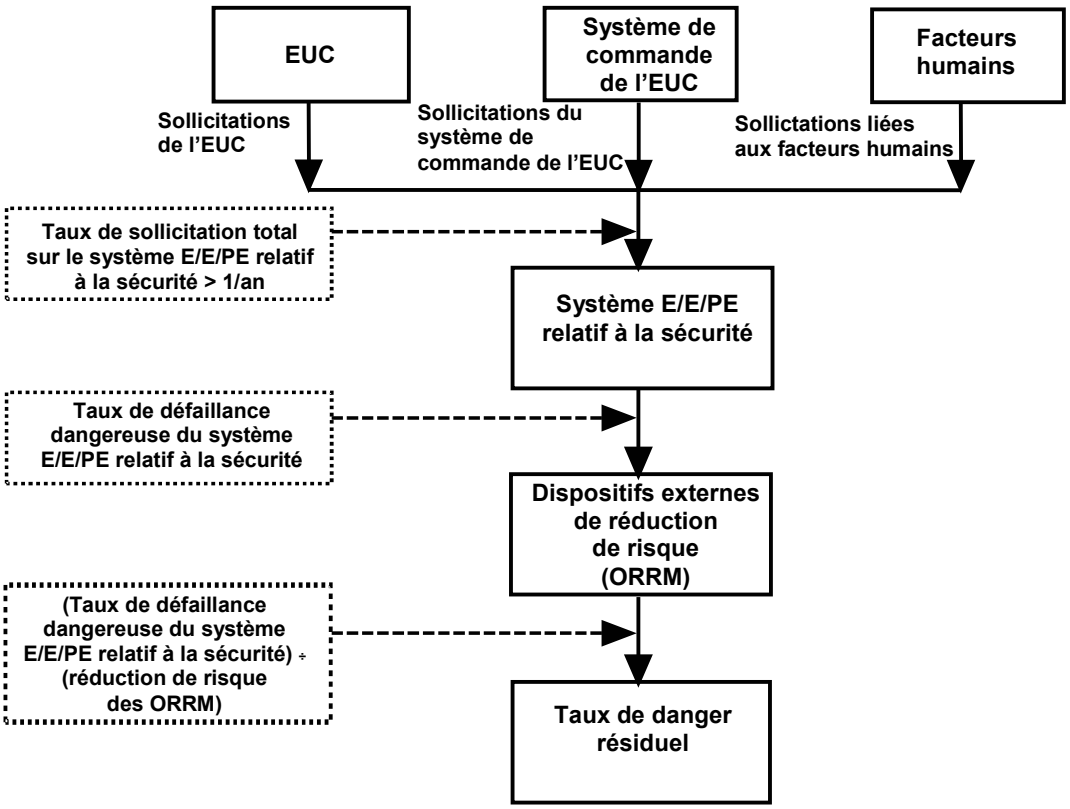


Figure A.3 – Diagramme de risque pour des applications en mode sollicitation élevée

A.5.3 Intégrité de sécurité pour des applications en mode continu

L'intégrité de sécurité requise des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque doit être à un niveau tel que la probabilité moyenne de défaillance dangereuse par heure du système relatif à la sécurité soit suffisamment faible pour éviter que la fréquence des événements dangereux n'excède la valeur requise pour atteindre l'objectif de risque tolérable.

Lorsqu'un système E/E/PE relatif à la sécurité fonctionne en mode continu, des dispositifs externes de réduction de risque peuvent réduire la fréquence de risque résiduel selon la réduction de risque fournie. Le modèle est illustré à la Figure A.4.

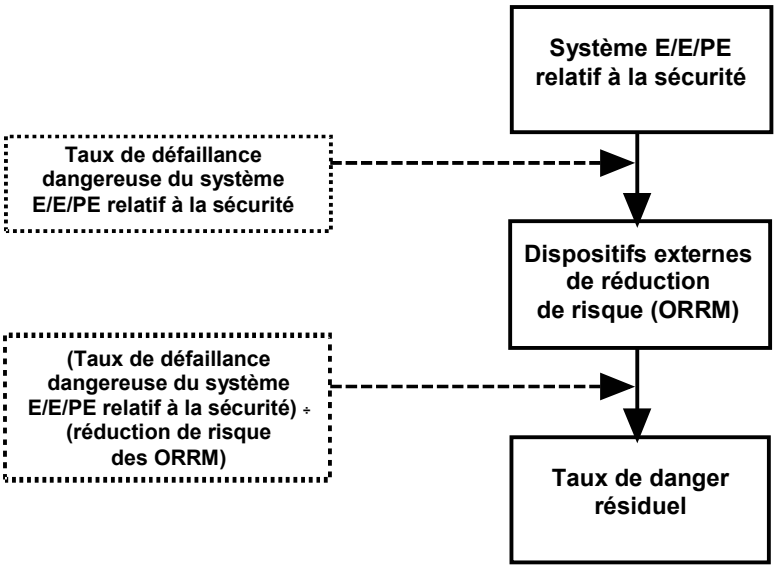


Figure A.4 – Diagramme de risque en mode de fonctionnement continu

A.5.4 Défaillances de cause commune et défaillances dépendantes

Lors de la détermination des niveaux d'intégrité de sécurité, il est important de tenir compte des défaillances de cause commune et des défaillances dépendantes. Les modèles illustrés aux Figures A.1, A.2, A.3 et A.4 ci-dessus sont fondés sur le principe selon lequel chaque système de sécurité concernant le même danger est totalement indépendant. Ce principe ne s'applique cependant pas pour de nombreuses applications. Des exemples de cas sont donnés ci-dessous:

1) Lorsqu'une défaillance dangereuse d'un élément au sein du système de commande de l'EUC peut provoquer une sollicitation sur un système relatif à la sécurité et que ce dernier utilise un élément faisant l'objet d'une défaillance de cause commune. Il peut s'agir par exemple du cas de capteurs d'un système de commande et de protection qui sont séparés mais dont la cause commune peut provoquer la défaillance des deux (voir Figure A.5).
2) En cas d'utilisation de plusieurs systèmes relatifs à la sécurité, et lorsque certains équipements de même type sont utilisés au sein de chaque système relatif à la sécurité faisant l'objet d'une défaillance de cause commune. Il peut s'agir par exemple du cas où le même type de capteur est utilisé dans deux systèmes de protection séparés assurant chacun la réduction de risque pour le même danger (voir Figure A.6).
3) En cas d'utilisation de plusieurs systèmes de protection, lorsque ces derniers sont diversifiés mais que l'essai périodique est réalisé sur tous les systèmes de manière synchrone. Dans ce cas, la valeur réelle de PFD_{avg} obtenue par la combinaison de plusieurs systèmes est sensiblement supérieure à celle de la PFD_{avg} obtenue par la multiplication de la PFD_{avg} des systèmes individuels.
4) Lorsque le même élément individuel est utilisé comme partie intégrante du système de commande et du système relatif à la sécurité.
5) En cas d'utilisation de plusieurs systèmes de protection, lorsque le même élément individuel est utilisé comme partie intégrante de plusieurs systèmes.

Dans ces cas, l'effet de cause commune/dépendance doit être pris en compte. Il convient de considérer la possibilité que la configuration finale soit capable de satisfaire à la capabilité systématique nécessaire et la probabilité nécessaire de taux de défaillance dangereuse aléatoire du matériel concernant la réduction de risque global requise. Il est difficile de déterminer l'effet des défaillances de cause commune, ce qui nécessite souvent de construire des modèles spécial (par exemple, arbre de panne ou modèles de Markov).

L'effet de cause commune est susceptible d'être plus significatif dans des applications impliquant des niveaux d'intégrité de sécurité élevés. Pour certaines applications, il peut se révéler nécessaire d'intégrer la notion de diversité afin de réduire au minimum les effets de cause commune. Il convient cependant de noter que l'intégration de la diversité peut poser des problèmes au cours des opérations de conception, de maintenance et de modification. L'introduction de la diversité peut donner lieu à des erreurs dues à une méconnaissance et au manque d'expérience d'exploitation des différents dispositifs.

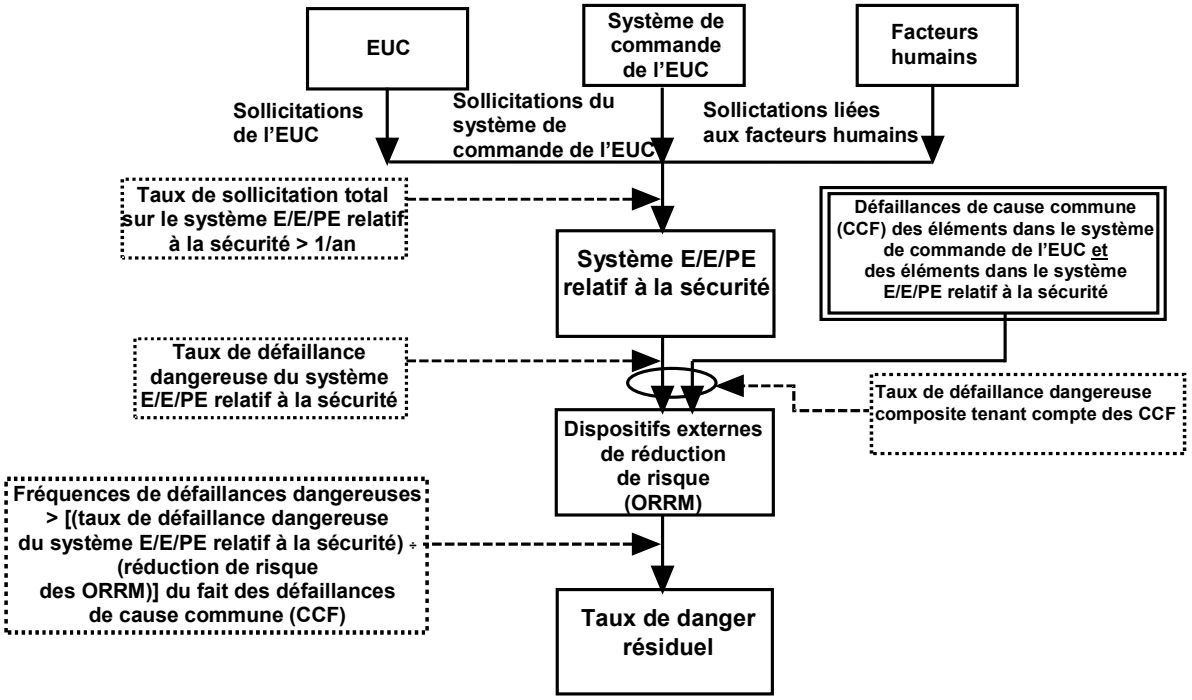


Figure A.5 – Illustration des défaillances de cause commune (CCF) des éléments dans le système de commande de l'EUC et des éléments dans le système E/E/PE relatif à la sécurité

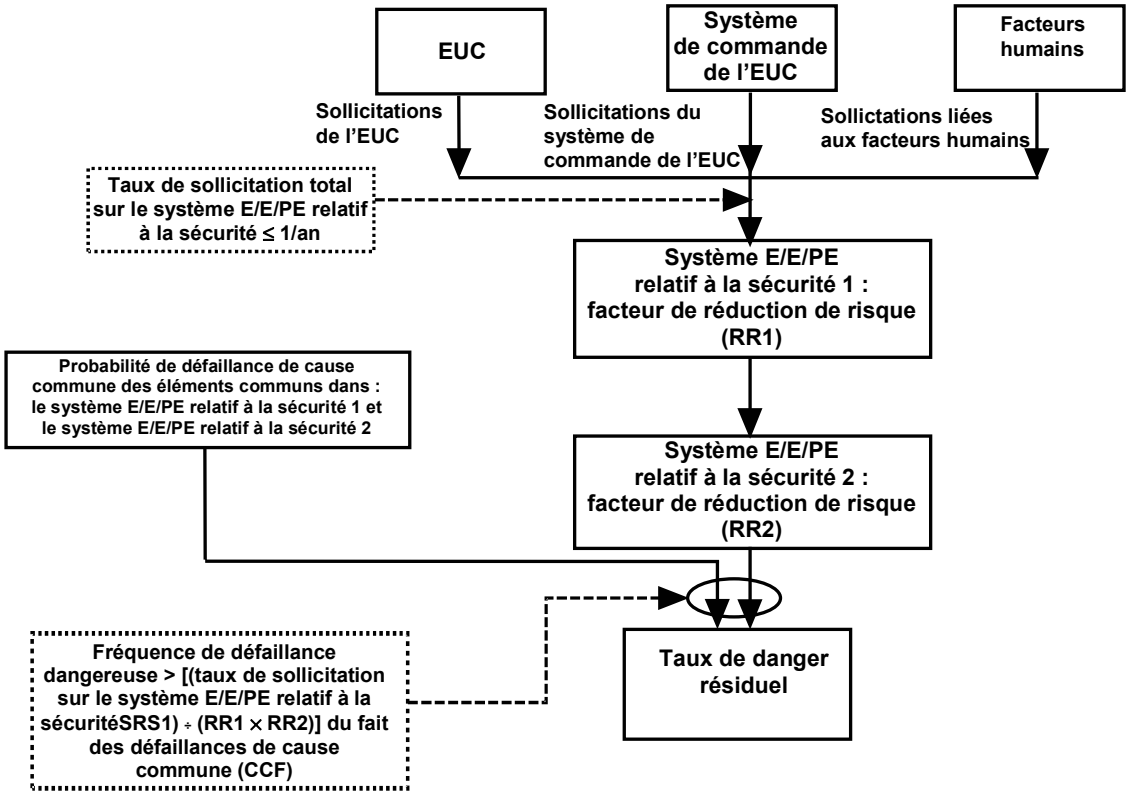


Figure A.6 – Cause commune entre deux systèmes E/E/PE relatifs à la sécurité

A.5.5 Niveaux d'intégrité de sécurité en cas d'utilisation de plusieurs couches de protection

Lorsque plusieurs couches de protection sont utilisées pour obtenir un risque tolérable, des interactions peuvent se produire entre les systèmes eux-mêmes ainsi qu'entre les systèmes et les causes de sollicitation. Comme spécifié en A.5.4 ci-dessus, la (dé)synchronisation d'essai et les défaillances de cause commune représentent toujours un sujet de préoccupation car elles peuvent constituer des facteurs significatifs, lorsque les exigences de réduction de risque global sont élevées ou lorsque la fréquence de sollicitation est faible. L'évaluation des interactions entre les couches de sécurité ainsi qu'entre les couches de sécurité et les causes de sollicitation peut être complexe et nécessiter l'élaboration d'un modèle holistique (par exemple, comme décrit dans l'ISO/CEI 31010) basé, par exemple, sur une approche « du haut vers le bas », l'événement de tête étant spécifié comme la fréquence de danger tolérable. Le modèle peut comprendre toutes les couches de sécurité utilisées pour le calcul de la réduction de risque réel ainsi que toutes les causes de sollicitation utilisées pour le calcul de la fréquence réelle d'accident. Ceci permet d'identifier des coupes d'ordre minimal (c'est-à-dire des scénarios de défaillance), de détecter les points faibles (c'est-à-dire les coupes d'ordre minimal les plus courtes: défaillances simples, doubles, etc.) dans la configuration des systèmes et de faciliter l'amélioration du système grâce à l'analyse de sensibilité.

A.6 Risque et intégrité de sécurité

Il est important de bien distinguer le risque et l'intégrité de sécurité. Le risque est une mesure de la probabilité pour qu'un événement dangereux spécifié se produise et de ses conséquences. Il peut être évalué pour différentes situations (le risque EUC, la réduction de risque requise pour atteindre l'objectif de risque tolérable, le risque réel (voir Figure A.1). Le risque tolérable est déterminé en tenant compte des problèmes décrits en A.2. L'intégrité de sécurité s'applique exclusivement aux systèmes E/E/PE relatifs à la sécurité et aux dispositifs externes de réduction de risque et elle correspond à la probabilité pour que ces systèmes/dispositifs réalisent de manière satisfaisante la réduction de risque nécessaire dans le cadre des fonctions de sécurité spécifiées. Une fois le risque tolérable défini et la réduction de risque nécessaire estimée, les exigences d'intégrité de sécurité pour les systèmes relatifs à la sécurité peuvent être allouées (voir 7.4, 7.5 et 7.6 de la CEI 61508-1).

NOTE Cette allocation est nécessairement itérative pour optimiser la conception afin de répondre aux diverses exigences.

A.7 Niveaux d'intégrité de sécurité et capabilité systématique du logiciel

Pour répondre au grand nombre de réductions de risque nécessaires que les systèmes relatifs à la sécurité doivent réaliser, il est utile de disposer d'un certain nombre de niveaux d'intégrité de sécurité pour satisfaire aux exigences d'intégrité de sécurité des fonctions de sécurité allouées aux systèmes relatifs à la sécurité. La capabilité systématique du logiciel constitue la base des spécifications des exigences d'intégrité de sécurité des fonctions de sécurité remplies partiellement par les logiciels relatifs à la sécurité. Il convient que la spécification des exigences d'intégrité de sécurité spécifie les niveaux d'intégrité de sécurité pour les systèmes E/E/PE relatifs à la sécurité.

La présente norme spécifie quatre niveaux d'intégrité de sécurité, le niveau 4 étant le plus élevé et le niveau 1 le plus faible.

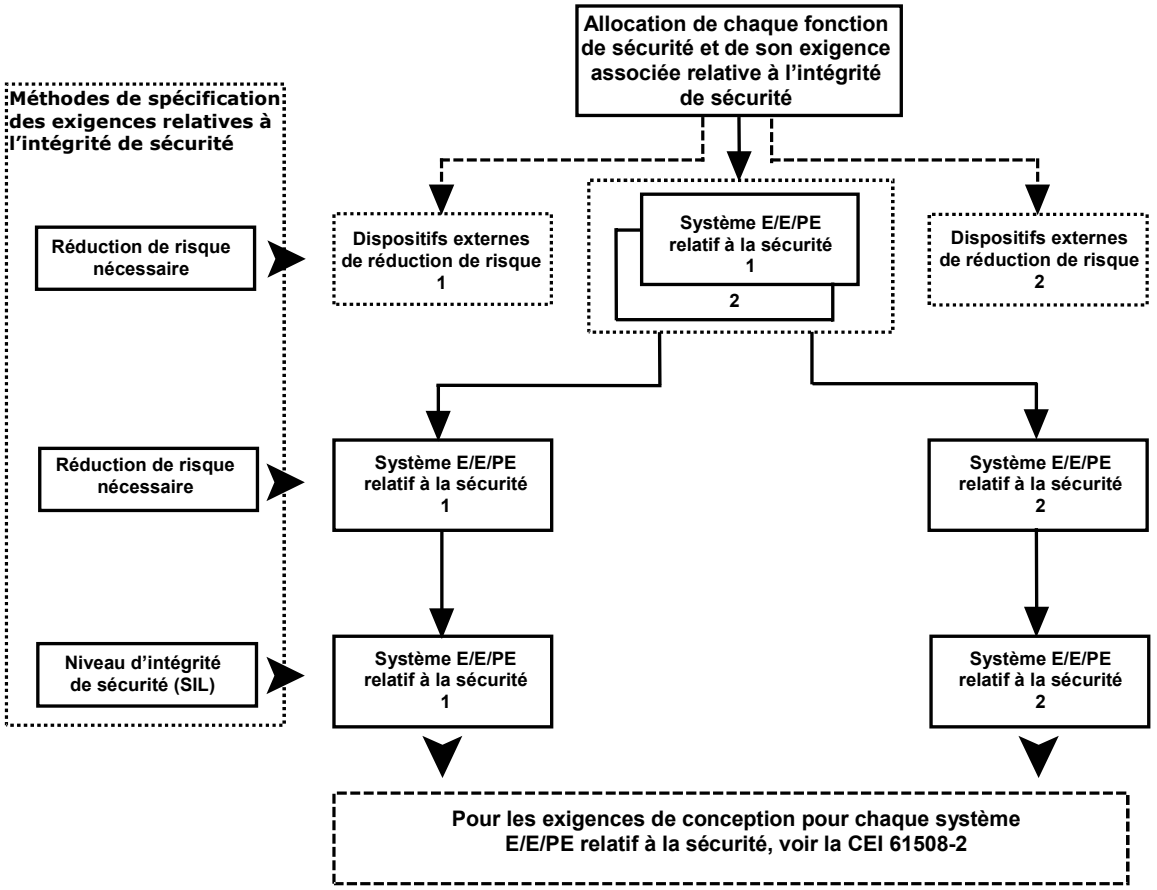
Les objectifs chiffrés de défaillance, en matière de niveau d'intégrité de sécurité, pour les quatre niveaux d'intégrité de sécurité sont spécifiées dans les Tableaux 2 et 3 de la CEI 61508-1. Deux paramètres sont spécifiés, un pour les systèmes relatifs à la sécurité fonctionnant en mode faible sollicitation et un pour les systèmes relatifs à la sécurité fonctionnant en mode sollicitation élevée ou en mode continu.

NOTE Pour les systèmes relatifs à la sécurité fonctionnant en mode faible sollicitation, la mesure de l'intégrité de sécurité concernée est la probabilité de défaillance dans l'accomplissement de sa fonction sur sollicitation. Pour les systèmes relatifs à la sécurité fonctionnant en mode sollicitation élevée ou en mode continu, la mesure de l'intégrité de sécurité concernée est la probabilité moyenne de défaillance dangereuse par heure (voir 3.5.16 et 3.5.17 de la CEI 61508-4).

A.8 Allocation des exigences de sécurité

L'allocation des exigences de sécurité (les exigences relatives à la fonction de sécurité et à l'intégrité de sécurité) aux systèmes E/E/PE relatifs à la sécurité, aux systèmes relatifs à la sécurité basés sur d'autres technologies et aux dispositifs externes de réduction de risque est présentée à la Figure A.7 (identique à la Figure 6 de la CEI 61508-1). Les exigences pour la phase d'allocation des exigences de sécurité sont données en 7.6 de la CEI 61508-1.

Les méthodes utilisées pour allouer les exigences d'intégrité de sécurité aux systèmes E/E/PE relatifs à la sécurité, aux systèmes relatifs à la sécurité basés sur d'autres technologies et aux dispositifs externes de réduction de risque dépendent principalement du fait que la réduction de risque nécessaire est spécifiée explicitement d'une manière numérique ou qualitative. Ces approches sont appelées méthodes quantitatives ou qualitatives, respectivement (voir Annexes B, C, D et E).



NOTE 1 Les exigences relative à l'intégrité de sécurité sont associées à chaque fonction de sécurité avant allocation (voir 7.5.2.3 et 7.5.2.4 de la CEI 61508-2)

NOTE 2 Une fonction de sécurité peut-être allouée sur plusieurs systèmes relatifs à la sécurité

Figure A.7 – Allocation des exigences de sécurité aux systèmes E/E/PE relatifs à la sécurité et dispositifs externes de réduction de risque

A.9 Systèmes de limitation

Les systèmes de limitation s'appliquent dans le cas de défaillance totale ou partielle d'autres systèmes relatifs à la sécurité tels que les systèmes E/E/PE relatifs à la sécurité. L'objectif est de réduire les conséquences associées à un événement dangereux plutôt que sa fréquence. Les exemples de systèmes de limitation comprennent les réseaux d'incendie et de gaz (détection d'incendie/gaz et action ultérieure d'extinction de l'incendie (par exemple, par inondation à l'eau), et les systèmes « airbag » dans une automobile.

Lors de la détermination des exigences d'intégrité de sécurité, il convient d'admettre que pour la formulation de jugements sur la gravité de la conséquence, il convient de ne tenir compte que des conséquences incrémentielles. En d'autres termes, il s'agit de déterminer l'augmentation de la gravité de la conséquence si la fonction ne remplit pas son rôle par rapport à la conséquence lorsque la fonction remplit son rôle comme prévu. Ceci peut être réalisé en tenant en premier lieu compte des conséquences lorsque le système est défaillant, puis en considérant la situation correspondante lorsque la fonction de limitation fonctionne correctement. La prise en compte des conséquences en cas de défaillance de fonctionnement du système donne généralement lieu à un certain nombre de résultats présentant toutes sortes de probabilités différentes. L'analyse par arbre d'événements (AAE) peut se révéler un outil utile dans ce cas.

NOTE Des lignes directrices relatives à la détermination des niveaux d'intégrité de sécurité des réseaux d'incendie et de gaz et des systèmes d'arrêt d'urgence sont données dans l'Annexe B de l'ISO 10418.

Annexe B
(informative)

Sélection des méthodes de détermination des exigences relatives aux niveaux d'intégrité de sécurité

B.1 Généralités

La présente annexe répertorie un certain nombre de techniques qu'il est possible d'utiliser pour la détermination des niveaux d'intégrité de sécurité. Aucune des méthodes n'étant appropriée à toutes les applications, les utilisateurs doivent sélectionner celle qui convient le mieux. Dans le cadre de la sélection de la méthode la plus appropriée, il convient de tenir compte des facteurs suivants:

1) les critères d'acceptation de risque qui doivent être satisfaits. Certaines techniques ne sont pas appropriées lorsqu'il s'agit de démontrer que le risque a été ramené à un niveau aussi faible que raisonnablement possible,
2) le mode de fonctionnement de la fonction de sécurité. Certaines méthodes ne s'appliquent qu'en mode faible sollicitation,
3) la connaissance et l'expérience des personnes chargées de déterminer les niveaux SIL ainsi que l'approche conventionnelle appliquée dans le secteur,
4) la confiance nécessaire dans le fait que le risque résiduel résultant satisfait aux critères spécifiés par l'organisme utilisateur. Certaines méthodes peuvent être liées à des cibles quantifiées mais d'autres ne sont que qualitatives,
5) plusieurs méthodes peuvent être utilisées. Une méthode peut être utilisée à des fins de dépistage, suivie d'une autre approche plus rigoureuse si la méthode de dépistage montre la nécessité de niveaux d'intégrité de sécurité élevés,
6) la gravité des conséquences. Des méthodes plus rigoureuses peuvent être sélectionnées pour ce qui concerne les conséquences, comprenant plusieurs accidents mortels,
7) l'éventuelle occurrence de cause commune entre les systèmes E/E/PE relatifs à la sécurité ou entre le système E/E/PE relatif à la sécurité et les causes de sollicitation.

Quelle que soit la méthode utilisée, il convient d'enregistrer toutes les hypothèses pour la gestion future de la sécurité. Il convient d'enregistrer toutes les décisions prises afin de pouvoir vérifier l'évaluation des niveaux d'intégrité de sécurité et réaliser une évaluation de la sécurité fonctionnelle indépendante.

B.2 Méthode ALARP

Les principes ALARP peuvent être appliqués en tant que tels ou associés à d'autres méthodes pour déterminer les exigences SIL relatives à une fonction de sécurité. Ils peuvent être utilisés de manière qualitative ou quantitative. Lorsqu'elles sont utilisées de manière qualitative, les exigences SIL pour une fonction de sécurité spécifiée sont augmentées jusqu'à ce que la fréquence d'occurrence soit réduite de sorte que les conditions associées à la classe de risque II ou III soient satisfaites. Lorsqu'elles sont utilisées de manière quantitative, les fréquences et les conséquences sont spécifiées numériquement et les exigences SIL sont augmentées jusqu'à ce qu'il puisse être démontré que les coûts supplémentaires en capital et les coûts d'exploitation associés à la mise en oeuvre d'un SIL plus élevé satisferaient à la condition associée à la classe de risque Classe II ou III.

L'utilisation de la méthode ALARP doit tenir compte de la limite entre la zone intolérable et la zone ALARP.

B.3 Méthode quantitative de détermination des niveaux d'intégrité de sécurité (SIL)

L'Annexe D décrit la méthode quantitative. Elle peut être utilisée conjointement à la méthode ALARP décrite à l'Annexe C.

La méthode quantitative peut être utilisée tant pour les applications simples que complexes. Pour les applications complexes, les arbres de panne peuvent être construits pour représenter le modèle de danger. L'événement de tête est généralement constitué d'un ou de plusieurs accidents mortels et construit de manière logique pour représenter les causes de sollicitation et les défaillances des systèmes E/E/PE relatifs à la sécurité donnant lieu à l'événement de tête. Des outils logiciels permettent de modéliser la cause commune en cas d'utilisation du même type d'équipement pour les fonctions de commande et de protection. Dans le cas de certaines applications complexes, un événement de défaillance simple peut se produire à plusieurs endroits dans l'arbre de panne, ce qui nécessite de réaliser une réduction booléenne. Les outils facilitent également la réalisation de l'analyse de sensibilité permettant d'indiquer les facteurs dominants qui ont une influence sur la fréquence de l'événement de tête. Il est possible d'établir les niveaux SIL en déterminant la réduction de risque requise pour satisfaire aux critères de risque tolérable.

La méthode s'applique aux fonctions de sécurité fonctionnant en mode continu/mode sollicitation élevée et en mode faible sollicitation. La méthode conduit généralement à des niveaux SIL faibles dans la mesure où le modèle de risque est spécifiquement conçu pour chaque application et où les valeurs numériques sont utilisées pour représenter chaque facteur de risque plutôt que les étendues numériques utilisées dans les graphes de risque étalonnés. Les méthodes quantitatives nécessitent cependant de construire un modèle spécifique à chaque événement dangereux. La modélisation nécessite de disposer des compétences, des outils et des connaissances concernant l'application et peut être lente à développer et vérifier.

La méthode facilite la démonstration que le risque a été ramené à un niveau aussi faible que raisonnablement possible. Ceci peut être réalisé en envisageant les options de réduction de risque ultérieure, en intégrant les dispositifs supplémentaires au modèle de l'arbre de panne, puis en déterminant la réduction de risque pour finalement comparer les résultats obtenus au coût de l'option.

B.4 Méthode du graphe de risque

La méthode qualitative du graphe de risque est décrite à l'Annexe E. La méthode permet de déterminer le niveau d'intégrité de sécurité à partir des facteurs de risque connus associés à l'EUC et à son système de commande. Un certain nombre de paramètres sont introduits qui permettent de décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi chacun des quatre groupes, et les paramètres sélectionnés sont alors associés pour décider du niveau d'intégrité de sécurité alloué aux fonctions de sécurité. La méthode a été largement utilisée dans le domaine des machines, voir l'ISO 14121-2 et l'Annexe A de l'ISO 13849-1.

La méthode peut être qualitative, auquel cas la sélection des paramètres est subjective et se fonde pour une part importante sur le jugement. Le risque résiduel ne peut être calculé à partir des valeurs de paramètre connues. La méthode ne s'applique pas dans le cas où un organisme pose le principe de la confiance dans le fait que le risque résiduel est réduit à une valeur quantitative spécifiée.

Les descriptions de paramètre peuvent comprendre des valeurs numériques calculées par étalonnage du graphe de risque en fonction de critères de risque tolérable spécifiés sous forme numérique. Le risque résiduel peut être calculé à partir des valeurs numériques utilisées pour chacun des paramètres. La méthode s'applique dans le cas où un organisme pose le principe de la confiance dans le fait que le risque résiduel est réduit à une valeur

quantitative spécifiée. L'expérience a montré que l'utilisation de la méthode du graphe de risque étalonné peut conduire à des niveaux d'intégrité de sécurité élevés. Ceci est dû au fait que l'étalonnage est généralement réalisé sur la base des valeurs du cas le plus défavorable de chaque paramètre. Chaque paramètre est positionné sur une étendue limitée à une décade de sorte que pour les applications pour lesquelles tous les paramètres constituent une moyenne de l'étendue, le niveau SIL est supérieur de un au niveau nécessaire pour le risque tolérable. La méthode est largement utilisée dans le domaine des processus et des activités offshore.

La méthode du graphe de risque ne prend pas en compte les défaillances de cause commune entre les causes de sollicitation et la cause de défaillance du système E/E/PE relatif à la sécurité ou les problèmes de cause commune avec d'autres couches de protection.

B.5 Analyse des couches de protection (LOPA)

La méthode de base est décrite dans un certain nombre d'ouvrages et la technique peut être utilisée sous différentes formes. L'Annexe F décrit une technique qu'il est possible d'utiliser pour la détermination des niveaux d'intégrité de sécurité.

La méthode est quantitative et l'utilisateur doit déterminer les fréquences tolérables pour chaque niveau de gravité des conséquences. Un crédit chiffré est attribué pour les couches de protection qui réduisent la fréquence des causes individuelles de sollicitation. Toutes les couches de protection ne s'appliquent pas à toutes les causes de sollicitation, ce qui permet d'utiliser la technique pour des applications plus complexes. Les valeurs numériques allouées aux couches de protection peuvent être arrondies au chiffre significatif suivant ou à l'étendue d'une décade suivante. Si les valeurs numériques des couches de protection sont arrondies au chiffre significatif suivant, la méthode sur la moyenne donne alors des exigences inférieures pour la réduction de risque et des valeurs de niveau SIL inférieures à celles obtenues avec des graphes de risque étalonnés.

Dans la mesure où les objectifs numériques sont alloués à des niveaux de gravité des conséquences spécifiés, l'utilisateur peut avoir confiance dans le fait que le risque résiduel satisfait aux critères admis.

La méthode décrite ne s'applique pas aux fonctions en mode continu et ne tient pas compte des défaillances de cause commune entre les causes de sollicitation et les systèmes E/E/PE relatifs à la sécurité. La méthode peut cependant être adaptée pour s'appliquer aux cas de cette nature.

B.6 Matrice de gravité des événements dangereux

La méthode de gravité des événements dangereux est décrite à l'Annexe G. Une hypothèse intrinsèque veut que l'ajout d'une couche de protection permet d'atteindre un ordre de grandeur de réduction du risque. Une autre hypothèse veut que les couches de protection soient indépendantes de la cause de sollicitation et indépendantes les unes des autres. La méthode décrite n'est pas appropriée aux fonctions en mode continu. La méthode peut être qualitative, auquel cas la sélection des facteurs de risque est subjective et se fonde en partie sur le jugement. Le risque résiduel ne peut être calculé à partir des valeurs de facteurs de risque connues. La méthode ne s'applique pas dans le cas où un organisme pose le principe de la confiance dans le fait que le risque résiduel est réduit à une valeur quantitative spécifiée.

Annexe C
(informative)

Concepts d'ALARP et de risque tolérable

C.1 Généralités

La présente annexe propose une approche particulière permettant de parvenir à un risque tolérable. Le but n'est pas de donner une interprétation figée de la méthode mais plutôt une illustration des principes généraux. L'approche comprend un processus d'amélioration continue par lequel toutes les options permettant d'assurer une réduction de risque supplémentaire sont prises en compte en termes de bénéfices et de coûts. Il convient que les personnes souhaitant appliquer les méthodes indiquées dans la présente annexe consultent les sources documentaires référencées (voir la référence [7] de la Bibliographie).

C.2 Modèle ALARP

C.2.1 Introduction

L'Article C.2 présente les principaux essais appliqués à la régulation des risques industriels et indique que les activités impliquent de déterminer si:

a) le risque est si important qu'il doive être complètement refusé, ou

b) le risque est si faible ou a été tellement réduit qu'il en devient non significatif, ou

c) le risque se situe entre les deux niveaux a) et b) définis ci-dessus et a été ramené au plus bas niveau possible, en tenant compte des bénéfices résultant de son acceptation et des coûts qu'engendrerait toute réduction supplémentaire.

Si l'on considère le point c), le principe ALARP stipule que tout risque doit être ramené au plus bas niveau possible ou jusqu'à un niveau qui soit aussi faible que raisonnablement possible (les 5 mots anglais « as low as reasonably praticable » forment l'abréviation ALARP). Si un risque se situe entre les deux extrêmes (c'est-à-dire la zone inacceptable et la zone globalement acceptable) et si le principe ALARP a été appliqué, le risque résultant est alors le risque tolérable pour l'application concernée. Cette approche des trois zones est illustrée à la Figure C.1.

Au-dessus d'un certain niveau, un risque est considéré comme intolérable et ne peut être justifié dans aucune circonstance ordinaire.

Au-dessous de ce niveau, il existe une zone tolérable où une activité peut avoir lieu sous réserve que les risques associés soient aussi faibles que raisonnablement possible. Tolérable a ici une signification différente d'acceptable: cela indique un souhait d'admettre de vivre avec un risque en contrepartie de certains bénéfices, tout en supposant que ce risque soit examiné et réduit quand il peut l'être. L'évaluation du bénéfice est demandée soit explicitement, soit implicitement pour mesurer le coût et la nécessité ou encore pour envisager d'autres mesures de sécurité. Il faut s'attendre à une dépense d'autant plus importante pour réduire un risque qu'il est lui-même plus important. A la limite du tolérable, des dépenses disproportionnées au bénéfice peuvent être justifiées. Le risque est considéré dans ce cas comme substantiel, et un effort considérable est justifié, même pour atteindre une réduction marginale.

Lorsque les risques sont moins significatifs, la dépense est d'autant moins importante pour les réduire et, à la limite la plus basse de la zone tolérable, il suffit d'équilibrer les coûts et les bénéfices.

Au-dessous de la zone tolérable se situe la zone généralement acceptée, où les risques sont faibles en comparaison avec les risques de tous les jours. Alors que la zone généralement

acceptée ne nécessite pas de travail détaillé pour démontrer ALARP, il est toutefois nécessaire de rester vigilant pour s'assurer que le risque reste à ce niveau.

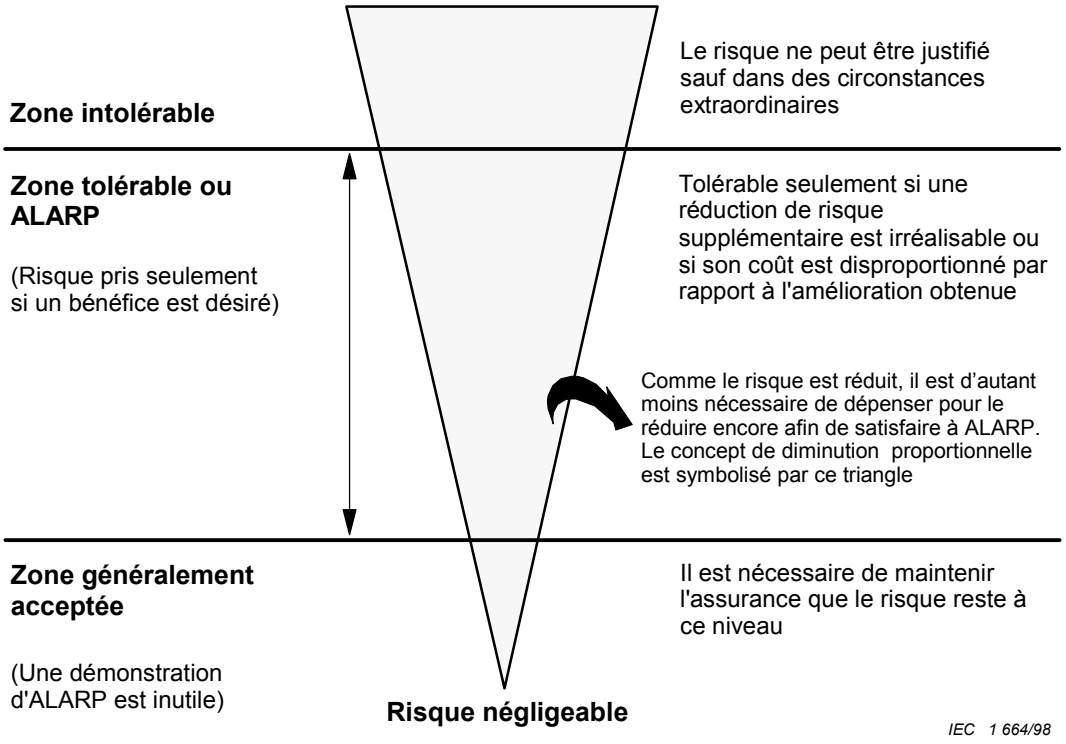


Figure C.1 – Risque tolérable et ALARP

Le concept d'ALARP peut être employé lorsque des objectifs de risque qualitatifs ou quantitatifs sont adoptés. Le paragraphe C.2.2 présente une méthode adaptée aux objectifs de risque quantitatifs. (Les Annexes D et F présentent des méthodes quantitatives et les Annexes E et G présentent des méthodes qualitatives pour la détermination de la réduction de risque nécessaire pour un danger spécifique. Les méthodes indiquées peuvent incorporer le concept d'ALARP dans la prise de décision.)

NOTE Des informations supplémentaires sur ALARP sont données dans la référence [7] dans la Bibliographie.

C.2.2 Objectif de risque tolérable

Une façon de parvenir à un objectif de risque tolérable consiste à déterminer un certain nombre de conséquences et à leur allouer les fréquences tolérables. Pour parvenir à un équilibre entre les conséquences et les fréquences tolérables, une discussion aboutissant à un accord devrait avoir lieu entre les parties concernées (par exemple, les organismes réglementaires en matière de sécurité, les personnes à l'origine des risques et celles exposées aux risques).

Pour prendre en compte les concepts ALARP, la mise à niveau entre une conséquence et une fréquence tolérable peut être effectuée par l'intermédiaire de classes de risque. Le Tableau C.1 présente quatre classes de risque (I, II, III, IV) pour un certain nombre de conséquences et de fréquences. Le Tableau C.2 interprète chacune des classes de risque qui utilisent le concept d'ALARP. La description de chacune des quatre classes de risque est basée sur la Figure C.1. Les risques de chacune de ces classes de risque sont ceux qui subsistent une fois appliquées les mesures de réduction de risque. Si l'on considère la Figure C.1, les classes de risque sont les suivantes:

– la classe de risque I se situe dans la zone intolérable,

– les classes de risque II et III se situent dans la zone ALARP, la classe de risque II se situant juste à l'intérieur de la zone ALARP,

– la classe de risque IV se situe dans la zone généralement acceptée.

Pour chaque situation spécifique, ou industrie sectorielle comparable, un tableau comparable au Tableau C.1 pourrait être développé en tenant compte d'un grand nombre de facteurs sociaux, politiques et économiques. Chaque conséquence pourrait correspondre à une fréquence et au tableau comprenant les classes de risque. Par exemple, «fréquent» dans le Tableau C.1 peut désigner un événement susceptible de se produire de façon permanente, ce qui peut être spécifié par une fréquence supérieure à 10 fois par an. Une conséquence critique peut correspondre à un décès et/ou de multiples blessures graves ou une maladie professionnelle grave.

Tableau C.1 – Exemple de classement des accidents en fonction des risques

Fréquence	Conséquence			
	Catastrophique	Critique	Marginale	Négligeable
Fréquent	I	I	I	II
Probable	I	I	II	III
Occasionnel	I	II	III	III
Peu fréquent	II	III	III	IV
Improbable	III	III	IV	IV
Non crédible	IV	IV	IV	IV

NOTE 1 L'attribution réelle des classes de risque I, II, III et IV dépend du secteur d'application et également des fréquences réelles (fréquent, probable, etc.). En conséquence, il convient que ce tableau soit perçu comme un exemple de la manière suivant laquelle un tel tableau pourrait être enrichi, plutôt que comme une spécification pour une utilisation future.

NOTE 2 Un aperçu de la détermination des niveaux d'intégrité de sécurité, à partir des fréquences présentées dans ce tableau, est donné à l'Annexe D.

Tableau C.2 – Interprétation des classes de risque

Classe de risque	Interprétation
Classe I	Risque intolérable
Classe II	Risque indésirable, et tolérable uniquement s'il est impossible de le réduire ou si le coût de la réduction est disproportionné par rapport à l'amélioration apportée
Classe III	Risque tolérable si le coût de la réduction de risque est supérieur à l'amélioration apportée
Classe IV	Risque négligeable

Annexe D
(informative)

Détermination des niveaux d'intégrité de sécurité – Une méthode quantitative

D.1 Généralités

La présente annexe donne un aperçu sur la manière suivant laquelle les niveaux d'intégrité de sécurité peuvent être déterminés si une approche quantitative est adoptée. Elle illustre aussi la manière suivant laquelle l'information contenue dans les tableaux tels que le Tableau C.1 peut être utilisée. Une approche quantitative présente une valeur ajoutée, particulièrement dans les cas suivants:

– le risque tolérable doit être spécifié numériquement (par exemple, il convient qu'une conséquence spécifiée ne se produise pas plus d'une fois sur 10^4 années),

– des objectifs numériques ont été spécifiés pour les niveaux d'intégrité de sécurité des systèmes relatifs à la sécurité. Les objectifs de ce type ont été spécifiés dans la présente norme (voir Tableaux 2 et 3 de la CEI 61508-1).

La présente annexe n'a pas pour objectif de donner une interprétation figée de la méthode mais est destinée à illustrer les principes généraux. Elle est particulièrement applicable lorsque le modèle de risque est comme indiqué aux Figures A.1 et A.2.

D.2 Méthode générale

Le modèle utilisé pour illustrer les principes généraux est décrit à la Figure A.1. Les étapes clés de cette méthode sont décrites ci-dessous et doivent être accomplies pour chaque fonction de sécurité devant être mise en œuvre par le système E/E/PE relatif à la sécurité:

– déterminer le risque tolérable à partir d'un tableau, comme le Tableau C.1 par exemple,

– déterminer le risque EUC,

– déterminer la réduction de risque nécessaire pour atteindre l'objectif de risque tolérable,

– allouer la réduction de risque nécessaire aux systèmes E/E/PE relatifs à la sécurité, aux systèmes relatifs à la sécurité basés sur d'autres technologies et aux dispositifs externes de réduction de risque (voir 7.6 de la CEI 61508-1).

Le Tableau C.1 est enrichi avec les fréquences des risques et permet de spécifier une valeur numérique cible (F_t) de risque tolérable.

La fréquence associée au risque qui existe pour l'EUC, incluant le système de commande de l'EUC et les problèmes liés aux facteurs humains (le risque EUC), sans aucune protection, peut être estimée en utilisant les méthodes quantitatives d'appréciation du risque. Cette fréquence, suivant laquelle un événement dangereux peut se produire sans aucune protection (F_{np}), est une des deux composantes du risque EUC; l'autre composante est la conséquence de l'événement dangereux. F_{np} peut être déterminée:

– par l'analyse des taux de défaillance dans des situations comparables,

– à partir des informations provenant de bases de données appropriées,

– par calcul à l'aide de méthodes de prédiction appropriées.

La présente norme impose des contraintes aux taux minimaux de défaillance exigibles pour le système de commande de l'EUC (voir 7.5.2.5 de la CEI 61508-1). Si l'on impose que le système de commande de l'EUC ait un taux de défaillance inférieur aux taux minimaux de défaillance, alors le système de commande de l'EUC doit être considéré comme un système

relatif à la sécurité et il doit être soumis à toutes les exigences de la présente norme applicables aux systèmes relatifs à la sécurité.

D.3 Exemple de calcul

La Figure D.1 donne un exemple de calcul d'objectif d'intégrité de sécurité pour un seul système de protection relatif à la sécurité. Dans une telle situation

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

où

PFD_{avg} est la probabilité moyenne de défaillance en cas de sollicitation du système de protection relatif à la sécurité, qui est l'objectif chiffré de défaillance pour des systèmes de protection relatifs à la sécurité fonctionnant en mode faible sollicitation (voir Tableau 2 de la CEI 61508-1 et 3.5.16 de la CEI 61508-4),

F_t est la fréquence de danger tolérable,

F_{np} est le taux de sollicitation auquel est soumis le système de protection relatif à la sécurité.

De même dans la Figure D.1:

– C est la conséquence de l'événement dangereux,

– F_p est la fréquence du risque en présence de dispositifs de protection.

La détermination de F_{np} pour l'EUC peut être considérée comme importante à cause de sa relation avec PFD_{avg} et ainsi avec le niveau d'intégrité de sécurité du système de protection relatif à la sécurité.

Les étapes nécessaires pour parvenir au niveau d'intégrité de sécurité (lorsque la conséquence C reste constante) sont illustrées ci-dessous (ainsi qu'à la Figure D.1), pour le cas où la réduction globale de risque nécessaire est obtenue par le biais d'un seul système de protection relatif à la sécurité qui doit, au minimum, ramener le taux de danger de F_{np} à F_t:

– déterminer la fréquence du risque EUC sans aucun dispositif de protection supplémentaire (F_{np}),

– déterminer la conséquence C sans aucun dispositif de protection supplémentaire,

– déterminer, à l'aide du Tableau C.1, si pour la fréquence F_{np} et la conséquence C un niveau de risque tolérable est atteint. Si, par l'utilisation du Tableau C.1, cette méthode conduit à une classe de risque I, une réduction supplémentaire de risque est alors nécessaire. Les risques de classe IV ou III peuvent être des risques tolérables. Un risque de classe II peut nécessiter une étude plus approfondie,

NOTE Le Tableau C.1 est utilisé pour vérifier si des dispositifs supplémentaires de réduction de risque sont ou non nécessaires, dans la mesure où il peut être possible d'atteindre un risque tolérable sans l'aide d'aucun dispositif de protection.

– déterminer la probabilité de défaillance en cas de sollicitation pour le système de protection relatif à la sécurité (PFD_{avg}) qui permet d'atteindre la réduction de risque nécessaire (ΔR). Pour une conséquence constante dans une situation spécifique décrite, $PFD_{avg} = (F_p / F_{np}) = \Delta R$,

– pour $PFD_{avg} = (F_p / F_{np})$, le niveau d'intégrité de sécurité peut être obtenu à partir du Tableau 2 de la CEI 61508-1 (par exemple, pour $PFD_{avg} = 10^{-2} – 10^{-3}$, le niveau d'intégrité de sécurité est égal à 2).

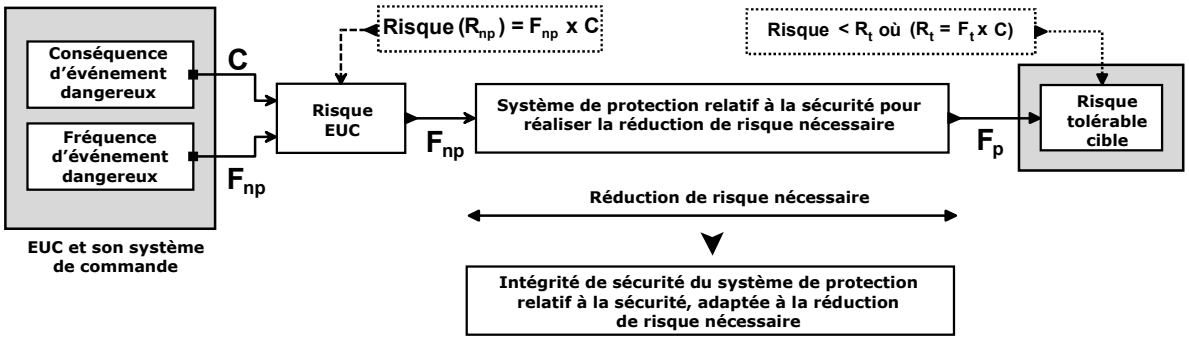


Figure D.1 – Allocation de l'intégrité de sécurité – exemple pour un système de protection relatif à la sécurité

Annexe E
(informative)

Détermination des niveaux d'intégrité de sécurité – Méthodes du graphe de risque

E.1 Généralités

La présente annexe décrit la méthode dite du «graphe de risque», méthode permettant de déterminer le niveau d'intégrité de sécurité d'un système relatif à la sécurité à partir des facteurs de risque connus associés à l'EUC et à son système de commande. Cette méthode est particulièrement applicable lorsque le modèle de risque est comparable à celui décrit aux Figures A.1 et A.2. La méthode peut être utilisée sur une base qualitative ou quantitative.

Lorsque cette méthode est adoptée, un certain nombre de paramètres de simplification sont introduits qui permettent de décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi chacun des quatre groupes et les paramètres sélectionnés sont alors associés pour décider du niveau d'intégrité de sécurité alloué aux fonctions de sécurité. Ces paramètres

– permettent de faire une gradation significative des risques, et
– contiennent les facteurs clés d'appréciation du risque.

La présente annexe n'a pas pour objectif de donner une interprétation figée de la méthode mais elle en illustre les principes généraux.

E.2 Synthèse du graphe de risque

La procédure simplifiée suivante s'appuie sur l'équation suivante:

R = *(f)* d'une conséquence *(C)* spécifiée

où

R est le risque en l'absence de systèmes relatifs à la sécurité,

f est la fréquence de l'événement dangereux en l'absence de systèmes relatifs à la sécurité,

C est la conséquence de l'événement dangereux (les conséquences peuvent être liées aux dommages associés à la santé et à la sécurité ou aux dommages provenant de dégâts environnementaux).

Dans le cas présent, la fréquence de l'événement dangereux *f* est supposée être le résultat de trois facteurs exerçant une influence:

– les fréquences et durée d'exposition dans la zone dangereuse,
– la possibilité d'éviter l'événement dangereux,
– la probabilité que l'événement dangereux se produise en l'absence de systèmes relatifs à la sécurité (mais en présence de dispositifs externes de réduction de risque). C'est ce que l'on appelle la probabilité d'occurrence non souhaitée.

On obtient les quatre paramètres de risque suivants:

– conséquence de l'événement dangereux (*C*),
– la fréquence et durée d'exposition au danger (*F*),

– la possibilité d'éviter l'événement dangereux (*P*),

– la probabilité de l'occurrence non souhaitée (*W*).

Les paramètres de risque peuvent être déterminés de manière qualitative comme décrit dans le Tableau E.1 ou de manière quantitative comme décrit dans le Tableau E.2. La détermination des valeurs numériques associées à chaque paramètre du Tableau E.2 nécessite d'appliquer un processus d'étalonnage.

E.3 Etalonnage

Les objectifs du processus d'étalonnage sont les suivants:

- décrire tous les paramètres afin de permettre à l'équipe d'évaluation des SIL de formuler des jugements objectifs sur la base des caractéristiques de l'application,
- garantir que le SIL sélectionné pour une application est conforme aux critères de risque d'exploitation et tient compte des risques issus d'autres sources,
- permettre la vérification du processus de sélection des paramètres.

Le processus d'étalonnage du graphe de risque consiste à allouer des valeurs numériques aux paramètres du graphe de risque. Ceci constitue la base pour l'évaluation du risque réel relatif au processus et permet de déterminer l'intégrité requise de la fonction de sécurité instrumentée considérée. Une étendue de valeurs est allouée à chacun des paramètres qui, lorsqu'ils sont associés, permet d'obtenir une évaluation graduée du risque qui existe en l'absence de fonction de sécurité particulière. Ceci permet ainsi d'obtenir une mesure du degré de confiance à accorder à la fonction de sécurité. Le graphe de risque associe des combinaisons particulières de paramètres de risque aux niveaux d'intégrité de sécurité. La relation entre les combinaisons de paramètres de risque et les niveaux d'intégrité de sécurité est établie en considérant le risque tolérable associé aux dangers spécifiques.

Pour ce qui concerne l'étalonnage des graphes de risque, il est important de tenir compte des exigences relatives au risque issues des attentes du propriétaire et des exigences de l'autorité réglementaire. Les risques pour la vie peuvent être considérés de nombreuses façons comme décrit en A.2 et dans l'Annexe C.

S'il est nécessaire de ramener la fréquence d'un accident mortel individuel à un niveau maximal spécifié, il ne peut alors être supposé que la réduction de risque dans son ensemble puisse être allouée à un seul système E/E/PE relatif à la sécurité. Les personnes sont exposées à une large étendue de risques générés par d'autres sources (par exemple, risques de chute, d'incendie et d'explosion). Pendant l'étalonnage, le nombre de dangers auxquels sont exposées les personnes et la durée totale d'exposition au risque doivent être pris en compte.

Pour évaluer l'étendue de la réduction de risque requise, un organisme peut disposer de critères relatifs au coût différentiel de prévention et de mise en garde d'un accident mortel. Ce coût peut être calculé en divisant le coût annualisé du matériel et de l'ingénierie supplémentaires associés à un niveau supérieur d'intégrité par la réduction de risque supplémentaire. Un niveau supplémentaire d'intégrité est justifié si le coût différentiel de prévention et de mise en garde d'un accident mortel est inférieur à un montant prédéterminé.

Les questions soulevées ci-dessus doivent être prises en compte avant de pouvoir spécifier chacune des valeurs de paramètre. Une étendue est allouée à la plupart des paramètres (par exemple, si le taux de sollicitation escompté d'un processus particulier s'inscrit dans une étendue de base dix spécifiée de sollicitations par an, alors W3 peut être utilisé). De même, pour les sollicitations comprises dans l'étendue de base dix inférieure, W2 peut s'appliquer et pour les sollicitations dans l'étendue de base dix inférieure suivante, W1 s'applique. L'allocation d'une étendue spécifiée à chaque paramètre permet à l'équipe de prendre des décisions concernant la valeur de paramètre à sélectionner pour une application spécifique. Pour étalonner le graphe de risque, des valeurs ou des étendues de valeurs sont allouées à

chaque paramètre. Le risque associé à chacune des combinaisons de paramètres est ensuite évalué en fonction des critères de risque définis. Les descriptions de paramètre sont alors modifiées pour pouvoir satisfaire aux critères de risque définis pour toutes les combinaisons de toutes les valeurs de paramètre. L'exemple d'étalonnage illustré au Tableau E.2 introduit un facteur « D » permettant de modifier l'étendue de sollicitations associées à chaque facteur W afin d'atteindre l'objectif de risque tolérable. Dans certains cas, il peut se révéler nécessaire de modifier les étendues associées à d'autres facteurs de risque pour refléter les valeurs de paramètre constatées dans l'étendue des applications considérées. L'étalonnage est un processus itératif qui se poursuit jusqu'à satisfaction des critères d'acceptation de risque spécifiés pour toutes les combinaisons de valeurs de paramètre.

Il n'est pas nécessaire de réaliser un étalonnage à chaque détermination du niveau d'intégrité de sécurité d'une application spécifique. Il suffit généralement que les organismes réalisent l'étalonnage une seule fois pour des dangers similaires. Des adaptations peuvent se révéler nécessaires pour des projets spécifiques si les hypothèses initiales formulées pendant l'étalonnage se révèlent non valables pour un projet spécifique.

Pour ce qui concerne les allocations de paramètres, il convient de fournir des informations sur le mode de calcul des valeurs.

Il est important que ce processus d'étalonnage soit convenu au niveau supérieur de l'entité responsable de la sécurité. Les décisions prises déterminent la sécurité globale obtenue.

En règle générale, un graphe de risque ne permet pas de prendre en compte la possibilité de défaillance dépendante entre les sources de sollicitation et l'équipement utilisé avec le système E/E/PE relatif à la sécurité. Il peut par conséquent donner lieu à une surestimation de l'efficacité du système E/E/PE relatif à la sécurité. Si les graphes de risque sont étalonnés pour comprendre des taux de sollicitations supérieurs à un par an, alors les exigences relatives au SIL résultant de l'utilisation du graphe de risque peuvent être plus sévères que nécessaire, et il est donc recommandé d'utiliser d'autres techniques.

E.4 Autres paramètres de risque possibles

Les paramètres de risque définis ci-dessus sont considérés comme suffisamment génériques pour concerner la plupart des applications. Toutefois, certaines de ces applications peuvent nécessiter le recours à des paramètres de risque supplémentaires. Il peut s'agir, par exemple, de l'utilisation de nouvelles technologies dans l'EUC et son système de commande. L'ajout de paramètres supplémentaires a pour objectif de resserrer l'évaluation de la réduction de risque nécessaire (voir la Figure A.1).

E.5 Mise en oeuvre du graphe de risque – schéma général

La combinaison des paramètres de risque décrits ci-dessus permet de développer un graphe de risque comparable à celui qui est présenté à la Figure E.1. En ce qui concerne la Figure E.1:

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

Le graphe de risque s'explique de la manière suivante:

– L'utilisation des paramètres de risque *C, F* et *P* aboutit à un certain nombre de sorties X_1, X_2, X_3... X_n (leur nombre exact étant fonction du domaine d'application spécifique que doit couvrir le graphe de risque). La Figure E.1 prend pour exemple une situation dans laquelle aucune pondération supplémentaire n'est appliquée aux pires conséquences. Chaque sortie est consignée dans une des trois échelles (W_1, W_2 et W_3). Chaque échelon indique l'intégrité de sécurité nécessaire à laquelle doit satisfaire le système E/E/PE relatif à la sécurité considéré. Dans la pratique, il arrive que, pour des conséquences spécifiques, un

seul système E/E/PE relatif à la sécurité ne suffise pas pour atteindre la réduction de risque nécessaire:

– La mise en correspondance avec W1, W2 ou W3 permet de réaliser la contribution des dispositifs externes de réduction de risque. Le décalage dans les échelles W1, W2 et W3 est nécessaire pour avoir trois niveaux différents de réduction de risque à partir d'autres mesures. Cette échelle est composée de l'échelle W3, qui fournit la réduction minimale de risque grâce à d'autres mesures (c'est-à-dire la plus forte probabilité de l'occurrence d'un événement non souhaité), l'échelle W2 une contribution moyenne et l'échelle W1 une contribution maximale. Pour une sortie intermédiaire spécifique du graphe de risque (c'est-à-dire X1, X2... ou X6) et pour une échelle W spécifique (c'est-à-dire W1, W2 ou W3), la sortie finale du graphe de risque donne le niveau d'intégrité de sécurité du système E/E/PE relatif à la sécurité (c'est-à-dire 1, 2, 3 ou 4) et correspond à une mesure de la réduction de risque nécessaire pour ce système. Cette réduction de risque, jointe aux réductions de risque réalisées par d'autres mesures (par exemple, grâce à des systèmes relatifs à la sécurité basés sur d'autres technologies et des dispositifs externes de réduction de risque) sont prises en compte par le mécanisme de l'échelle W et donnent la réduction de risque nécessaire pour une situation spécifique.

Les paramètres indiqués à la 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), et leurs pondérations doivent être précisément définis pour chaque situation spécifique ou des industries de secteurs comparables, et nécessiteraient aussi d'être définis par les normes internationales d'application sectorielle.

E.6 Exemple de graphe de risque

La Figure E.2 illustre un exemple de la mise en oeuvre du graphe de risque à partir des données de l'exemple du Tableau E.1 ci-après. En utilisant les paramètres de risque C, F et P, on parvient à l'une des huit sorties. Chacune de ces sorties est mise en correspondance avec l'une des trois échelles (W1, W2 et W3). Chaque échelon (a, b, c, d, e, f, g et h) indique la réduction de risque nécessaire à laquelle doit satisfaire le système relatif à la sécurité.

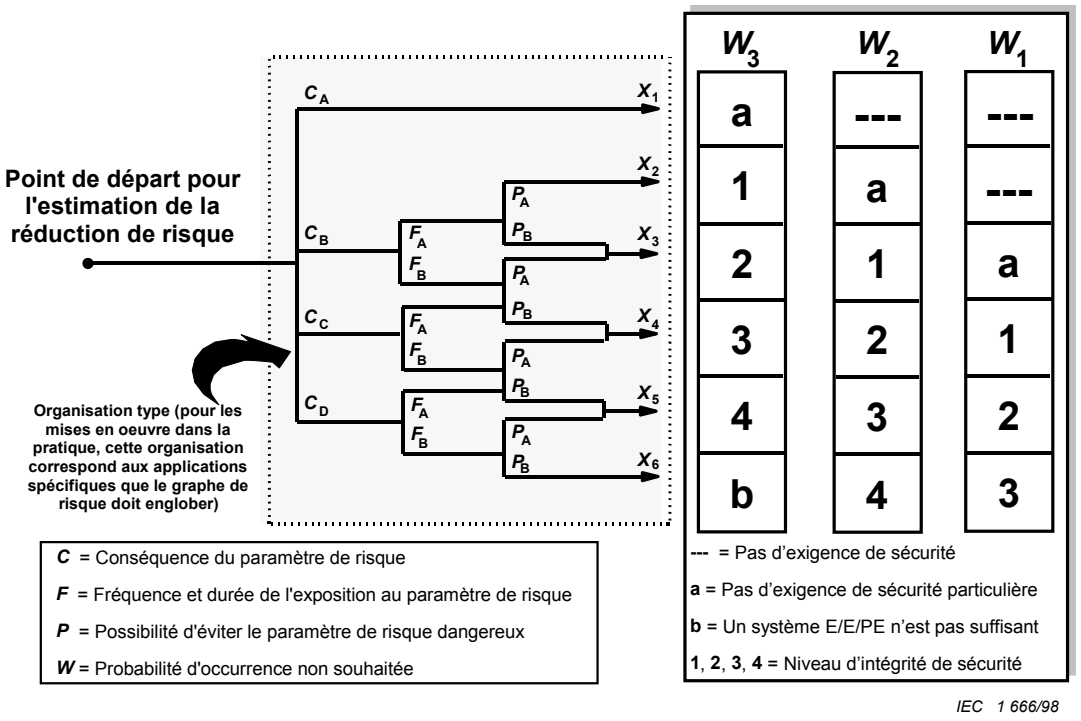
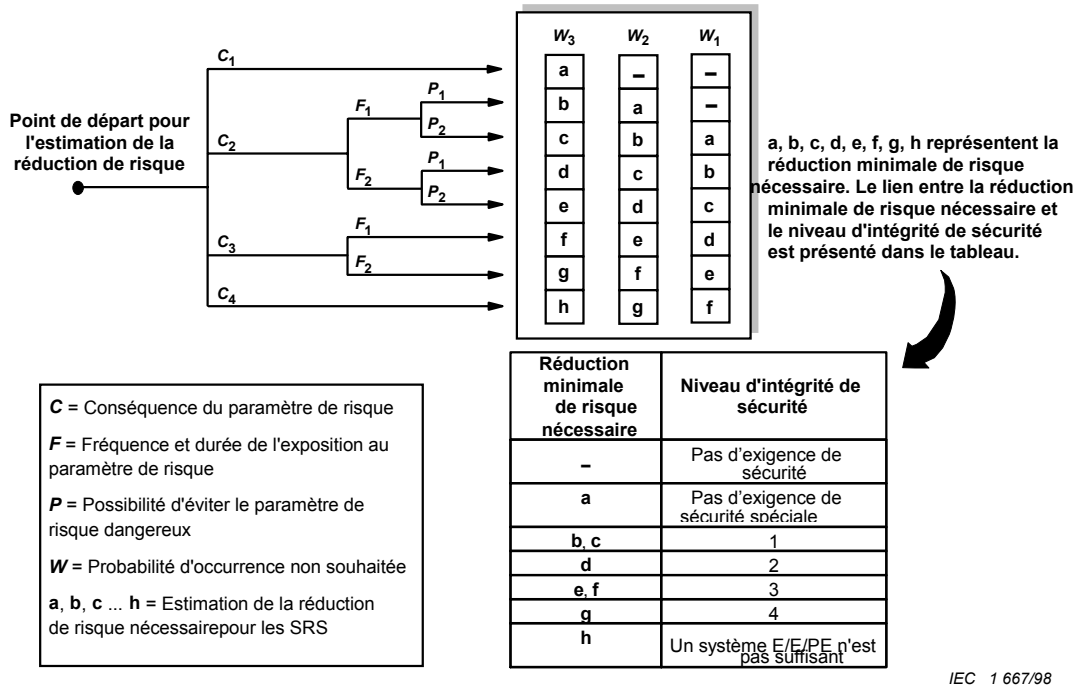


Figure E.1 – Graphe de risque – schéma général



Réduction minimale de risque nécessaire	Niveau d'intégrité de sécurité
–	Pas d'exigence de sécurité
a	Pas d'exigence de sécurité spéciale
b, c	1
d	2
e, f	3
g	4
h	Un système E/E/PE n'est pas suffisant

Figure E.2 – Graphe de risque – exemple (illustre seulement les principes généraux)

Tableau E.1 – Exemple de données relatives à un graphe de risque (Figure E.2)

Paramètre de risque		Classement	Commentaires
Conséquence (C)	C_1	Préjudice mineur	1 Le système de classement a été développé pour faire face aux préjudices et au décès des personnes. D'autres systèmes de classement devraient être développés pour les dommages causés à l'environnement ou au matériel
	C_2	Préjudice sérieux permanent pour une ou plusieurs personnes, mortel pour une personne	2 Pour interpréter C_1, C_2, C_3 et C_4, les conséquences de l'accident et la guérison normale doivent être prises en compte
	C_3	Mort de plusieurs personnes	
	C_4	Un très grand nombre de personnes tuées	
Fréquence et durée d'exposition dans la zone dangereuse (F)	F_1	Exposition rare à fréquente dans la zone dangereuse	3 Voir le commentaire 1 ci-dessus.
	F_2	Exposition fréquente à permanente dans la zone dangereuse	
Possibilité d'éviter l'événement dangereux (P)	P_1	Possible dans certaines conditions	4 Ce paramètre tient compte de – l'exploitation d'un processus (surveillé (c'est-à-dire utilisé par des personnes qualifiées ou non qualifiées) ou non surveillé), – la rapidité de développement de l'événement dangereux (par exemple, soudain, rapide ou lent), – la facilité de reconnaissance du danger (par exemple, vu immédiatement, détecté par des mesures techniques ou sans mesures techniques) , – l'évitement des événements dangereux (par exemple, présence déviation possible, impossible ou possible dans certaines conditions), – l'expérience de sécurité réelle (une telle expérience peut exister ou non avec un EUC identique ou similaire)
	P_2	Presque impossible	
Probabilité d'occurrence non souhaitée (W)	W_1	Une probabilité très faible que des occurrences non souhaitées surviennent ou seulement quelques occurrences non souhaitées sont probables	5 Le but du facteur W est d'estimer la fréquence des occurrences non souhaitées qui surviennent sans ajouter de systèmes relatifs à la sécurité (E/E/PE ou basés sur d'autres technologies) mais englobant tout autre dispositif externe de réduction de risque 6 S'il n'existe que peu ou pas d'expérience de l'EUC ou du système de commande de l'EUC ou d'un système similaire de commande de l'EUC et d'un EUC similaire, l'estimation du facteur W peut être faite par calcul. Dans ce cas, l'estimation d'un cas extrême doit être faite
	W_2	Une probabilité faible que des occurrences non souhaitées surviennent ou seulement quelques occurrences non souhaitées sont probables	
	W_3	Une probabilité forte que des occurrences non souhaitées surviennent et il est probable que des occurrences non souhaitées surviennent fréquemment	

Tableau E.2 – Exemple d'étalonnage du graphe de risque d'usage général

Paramètre de risque		Classement	Commentaires
Conséquence (C) Nombre d'accidents mortels Ceci peut être calculé en déterminant le nombre de personnes présentes lorsque la zone exposée au danger est occupée, puis en le multipliant par la vulnérabilité au danger identifié La vulnérabilité est déterminée par la nature du danger contre lequel une protection est assurée. Les facteurs suivants peuvent être utilisés: V=0,01 Faible dégagement de substance inflammable ou toxique V=0,1 Important dégagement de substance inflammable ou toxique V=0,5 Comme ci-dessus avec également une probabilité élevée de déclenchement d'incendie ou de dégagement de substance fortement toxique V=1 Rupture ou explosion	C_A C_B C_C C_D	Préjudice mineur Étendue de 0,01 à 0,1 Étendue de >0,1 à 1,0 Étendue > 1,0	1 Le système de classement a été développé pour faire face aux préjudices et au décès des personnes 2 Pour interpréter C_A, C_B, C_C et C_D, les conséquences de l'accident et la guérison normale doivent être prises en compte
Occupation (F) Elle est calculée en déterminant la durée proportionnelle d'occupation de la zone exposée au danger pendant une période de travail normale NOTE 1 Si la durée d'occupation dans la zone dangereuse varie en fonction des rotations effectuées, il convient alors de sélectionner la durée maximale NOTE 2 Il convient de n'utiliser F_A que s'il peut être démontré que le taux de sollicitation est aléatoire et sans relation avec un taux d'occupation susceptible d'être supérieur à la normale. Ce dernier cas se produit généralement avec des sollicitations au démarrage de l''équipement ou pendant l'étude d'anomalies	F_A F_B	Exposition rare à fréquente dans la zone dangereuse. Occupation inférieure à 0,1 Exposition fréquente à permanente dans la zone dangereuse	3 Voir le commentaire 1 ci-dessus
Possibilité d'éviter l'événement dangereux (P) si le fonctionnement du système de protection est défaillant	P_A P_B	Adopté si toutes les conditions de la colonne 4 sont satisfaites Adopté si toutes conditions ne sont pas satisfaites	4 Il convient de ne sélectionner P_A que si toutes les conditions suivantes sont vraies: – existence d'installations qui avertissent l'opérateur de la défaillance du SIS, – existence d'installations d'arrêt indépendantes permettant d'éviter le danger ou assurant l'évacuation de toutes les personnes vers une zone sûre, – le temps écoulé entre l'avertissement de l'opérateur et l'occurrence d'un événement dangereux dépasse 1 h ou est suffisamment long pour entreprendre les actions nécessaires.

Tableau E.2 *(suite)*

Paramètre de risque		Classement	Commentaires
Taux de sollicitation (W) Les durées cumulées annuelles d'éventuelles occurrences de l'événement dangereux en l'absence du système E/E/PE relatif à la sécurité Pour déterminer le taux de sollicitation, il est nécessaire de tenir compte de toutes les sources de défaillance susceptibles de donner lieu à un événement dangereux. La détermination du taux de sollicitation peut nécessiter d'allouer un crédit limité aux performances du système de commande et aux interventions. Les performances qu'il est possible de déclarer si le système de commande ne doit pas être conçu et maintenu conformément à la CEI 61508, se limitent aux étendues de performances inférieures associées au SIL 1	W_1 W_2 W_3	Taux de sollicitation inférieur à 0,1 D par an Taux de sollicitation compris entre 0,1 D et D par an Taux de sollicitation compris entre D et 10 D par an Pour des taux de sollicitation supérieurs à 10 D par an, une intégrité supérieure doit être requise	5 Le facteur *W* a pour objet d'estimer la fréquence d'occurrence du danger survenant sans systèmes E/E/PE relatifs à la sécurité supplémentaires Si le taux de sollicitation est très élevé, le SIL doit être déterminé par une autre méthode ou le graphe de risque doit de nouveau être étalonné. Il convient de noter que la méthode du graphe de risque peut ne pas constituer la meilleure approche dans le cas d'applications fonctionnant en mode continu (voir 3.5.16 de la CEI 61508-4). 6 Il convient de déterminer la valeur de D sur la base des critères d'exploitation en termes de risque tolérable en tenant compte des autres risques auxquels les personnes sont exposées
NOTE Il s'agit d'un exemple qui illustre l'application des principes de conception des graphes de risque. Les graphes de risque applicables à des applications particulières et à des dangers particuliers font l'objet d'un accord avec les personnes impliquées, en tenant compte du risque tolérable, voir E.1 à E.6.			

Annexe F
(informative)

Méthode semi-quantitative utilisant l'analyse des couches de protection (LOPA)

F.1 Généralités

F.1.1 Description

La présente annexe décrit une méthode appelée analyse des couches de protection (LOPA). Elle n'a pas pour objectif de donner une interprétation figée de la méthode, mais illustre en revanche les principes généraux.

F.1.2 Référence de l'annexe

La présente annexe se fonde sur une méthode détaillée dans une publication AIChE (voir [8] dans la Bibliographie). Cette référence explicite en détail les nombreuses façons d'utiliser les techniques LOPA.

Dans une approche, tous les paramètres significatifs sont arrondis à l'étendue de base dix supérieure (par exemple, une probabilité de $5 \cdot 10^{-2}$ est arrondie à 10^{-1}. Il s'agit d'une approche très prudente pouvant aboutir à des niveaux SIL sensiblement plus élevés. Il convient cependant de déterminer l'incertitude des données en arrondissant toutes les valeurs de paramètres au chiffre significatif le plus élevé suivant (il convient, par exemple, d'arrondir $5{,}4 \cdot 10^{-2}$ à $6 \cdot 10^{-2}$).

F.1.3 Description de la méthode

La méthode LOPA analyse les dangers afin de déterminer si les fonctions de sécurité sont nécessaires et si tel est le cas, le niveau SIL requis pour chaque fonction de sécurité. La méthode LOPA doit être adaptée pour satisfaire aux critères d'acceptation de risque à appliquer. La méthode commence avec les données élaborées au cours de l'identification des dangers et considère chaque danger identifié en documentant les causes initiatrices et les couches de protection qui préviennent ou limitent le danger. L'étendue de la réduction du risque peut ensuite être déterminée et la nécessité d'une réduction de risque supplémentaire analysée. Si une réduction de risque supplémentaire est nécessaire et si elle doit être assurée par un système E/E/PE relatif à la sécurité, la méthode LOPA permet de déterminer le SIL approprié. Pour chaque danger, un SIL approprié est déterminé pour ramener les risques à des niveaux tolérables. Le Tableau F.1 ci-après illustre un format type de LOPA.

F.2 Evénement résultant redouté

En utilisant le Tableau F.1, chaque description de l'événement résultant redouté (conséquence) déterminée à partir de l'identification des dangers est reportée dans la colonne 1 du Tableau F.1.

F.3 Niveau de gravité

Le niveau de gravité de l'événement est reporté dans la colonne 2 du Tableau F.1. Il est déduit à partir d'un tableau spécifiant les descriptions générales des niveaux de conséquences, par exemple, mineur, grave, catastrophique, avec des étendues de conséquences spécifiées et la fréquence maximale pour chaque niveau de gravité. Ce tableau établit les critères de tolérance de l'utilisateur. Des informations sont nécessaires pour

pouvoir déterminer les niveaux de gravité et les fréquences maximales pour des événements ayant des conséquences sur la sécurité et l'environnement.

F.4 Cause initiatrice

Toutes les causes initiatrices de l'événement résultant redouté sont répertoriées dans la colonne 3 du Tableau F.1. Les événements résultant redoutés peuvent avoir de nombreuses causes initiatrices, et il convient de toutes les répertorier.

F.5 Probabilité d'événement initiateur

Les valeurs de probabilité de chacune des causes initiatrices répertoriées dans la colonne 3 du Tableau F.1, exprimées en événements par an, sont reportées dans la colonne 4 du Tableau F.1.

La probabilité d'événement initiateur peut être calculée à partir des données génériques sur les taux de défaillance du matériel et sur les intervalles entre essais périodiques connus, ou sur la base des enregistrements de l'installation. Il convient de n'utiliser la probabilité d'événement initiateur faible que s'il existe une base statistique suffisante pour les données.

Tableau F.1 – Rapport LOPA

[a]	1	2	3	4	5			6	7	8	9	10	11
					Couches de protection (PL)								
	Description de l'événement résultant redouté F.2	Niveau de gravité F.3	Cause initiatrice F.4	Probabilité d'événe-ment initiateur F.5	Concepti on générale F.6.1	Système-me de comman de F.6.2	Alarmes, etc. F.6.3	Limitation supplément aire, accès limité F.7	Limitation supplément aire F.8	Probabilité d'événement intermédiaire F.9	PFD_{avg} requise pour E/E/PES (et SIL) F.10	Probabilité d'événement limitée tolérable F.11	Notes
1	Survitesse du rotor provoquant la rupture du carter	Mort des personne s situées à côté du carter, le nombre d'acci-dents mortels ne dépasse pas 2	Système de comman de de vitesse défaillant	0,1	1	1	1	0,1	0,1	10^{-3}	$5{\cdot}10^{-3}$ (SIL 2 avec une PFD_{avg} minimale de $5{\cdot}10^{-3}$)	10^{-5}	
			Perte de charge	1	1	0,1	1	0,1	0,1	10^{-3}			
			Défaillan ce de l'embray age	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						Crédit de 0,1 alloué au système de comman de		Occupation limitée, absence des personnes 90 % du temps	accident mortel uniquement si des fragments atteignent les personnes	Total $2{,}1{\cdot}10^{-3}$		tolérable si le nombre d'accidents mortels ne dépasse pas 5	
2	Répéter le cas ci-dessus pour l'analyse de risque environnemental												
3				Poursuivi selon le cas.									
.													
.													
N													

NOTE 1 Les niveaux de gravité peuvent être classés en C (catastrophique), E (étendu), S (grave) ou M (mineur). La probabilité d'événement limitée tolérable dépend du niveau de gravité.

NOTE 2 Les unités indiquées dans les colonnes 4, 8 et 10 représentent des événements par an.

NOTE 3 Les unités indiquées dans les colonnes 5 à 7 et 9 sont adimensionnelles. Les nombres compris entre 0 et 1 sont les facteurs qu'il est possible de multiplier avec la probabilité d'événement pour représenter l'effet de limitation de la couche de protection associée. Ainsi, 1 correspond à aucun effet de limitation, et 0,1 correspond à un facteur de réduction de risque de 10.

[a] Les numéros de colonnes et de lignes sont précisés car des explications sont données dans la suite de l'Annexe F.

F.6 Couches de protection (PL)

F.6.1 Généralités

Chaque PL est constituée d'un ensemble d'équipements et/ou de contrôles administratifs qui fonctionnent indépendamment des autres couches.

Les caractéristiques de conception qui réduisent la probabilité d'occurrence d'un événement résultant redouté en présence d'une cause initiatrice sont répertoriées tout d'abord dans la colonne 5 du Tableau F.1.

Il convient que les PL présentent les caractéristiques importantes suivantes:

– Spécificité: Une PL est conçue uniquement pour prévenir ou limiter les conséquences d'un événement potentiellement dangereux (par exemple, réaction d'emballement, dégagement de substance toxique, perte de contenu ou incendie). Plusieurs causes peuvent donner lieu au même événement dangereux et par conséquent, plusieurs scénarios d'événement peuvent déclencher l'action d'une PL.

– Efficacité: Une PL doit être capable, en elle-même, de préserver l'utilisateur des conséquences de toute source de préoccupation en cas d'échec complet de toutes les autres mesures

– Indépendance: Une PL est indépendante des autres PL associées à l'événement dangereux identifié.

– Sûreté de fonctionnement: Une PL peut être considérée comme devant faire ce pour quoi elle est conçue. Les modes de défaillance aléatoires et systématiques sont traités dans la conception.

– Contrôlabilité: Une PL est conçue pour faciliter la validation régulière des fonctions de protection. Les essais périodiques et la maintenance du système de sécurité sont nécessaires.

F.6.2 Système de commande de base

L'élément suivant de la colonne 5 du Tableau F.1 est le système de commande de l'EUC. Si une fonction de commande prévient l'occurrence de l'événement résultant redouté en présence de la cause initiatrice, le crédit basé sur sa PFD_{avg} est déclaré. Il convient de ne déclarer aucun crédit pour une fonction de commande si la défaillance de cette fonction risque de provoquer une sollicitation sur le système E/E/PE relatif à la sécurité. Il convient également de noter qu'il convient de limiter à une valeur minimale de 0,1 la PFD_{avg} déclarée d'une fonction de commande, si cette dernière n'est pas conçue et actionnée comme un système de sécurité.

F.6.3 Alarmes

Le dernier élément de la colonne 5 du Tableau F.1 concerne les alarmes qui avertissent l'opérateur et utilisent l'intervention de ce dernier. Il convient de n'accorder un crédit aux alarmes que dans les situations suivantes:

– Le matériel et le logiciel utilisés sont séparés et indépendants de ceux utilisés pour le système de commande (par exemple, il convient de ne pas partager les cartes d'entrée et les processeurs).

– L'alarme est affichée avec un haut niveau de priorité dans un emplacement surveillé en permanence. Il convient que le crédit accordé aux alarmes tienne compte des éléments suivants:

  - l'efficacité d'une alarme dépend de la complexité de la tâche à accomplir en cas d'alarme et des autres tâches devant être réalisées en même temps,
  - il convient de limiter le crédit à une PFD_{avg} minimale de 0,1,

- l'opérateur doit disposer de suffisamment de temps et d'installations indépendantes pour pouvoir mettre fin au danger. En règle générale, il convient de ne pas accorder de crédit sauf si le temps disponible entre l'alarme et le danger dépasse 20 min.

F.7 et F.8 Limitation supplémentaire

Les couches de limitation sont généralement d'ordre mécanique, structural ou procédural. Des exemples comprennent:

– un accès limité,

– la réduction de la probabilité d'inflammation,

– tous les autres facteurs qui réduisent la vulnérabilité des personnes exposées au danger.

Les couches de limitation peuvent réduire la gravité de l'événement résultant redouté, mais ne préviennent pas l'occurrence de l'événement. Des exemples comprennent:

– les systèmes d'inondation en cas d'incendie,

– les avertisseurs de fuite de gaz,

– les procédures d'évacuation qui peuvent réduire la probabilité d'exposition des personnes à un événement en escalade.

Dans le cadre de la limitation, il est possible de tenir compte du pourcentage d'occupation de la personne la plus exposée dans la zone dangereuse. Il convient de déterminer ce pourcentage en établissant le nombre d'heures passées dans la zone dangereuse par an et en le divisant par 8,760 h par an.

Il convient de déterminer la PFD_{avg} appropriée ou la valeur équivalente pour toutes les couches de limitation, et de la reporter dans les colonnes 6 et 7 du Tableau F.1.

F.9 Probabilité d'événement intermédiaire

La probabilité d'événement intermédiaire pour chaque cause est calculée en multipliant les facteurs suivants et le résultat de fréquence par an reporté dans la colonne 8 du Tableau F.1:

– vulnérabilité de la personne la plus exposée,

– probabilité d'événement initiateur (colonne 4),

– PFD_{avg} des couches de protection (PL) et des couches de limitation (colonnes 5, 6 et 7).

Il convient de calculer la fréquence d'événement intermédiaire totale en ajoutant les fréquences d'événement intermédiaire pour chaque cause.

Il convient de comparer la fréquence d'événement intermédiaire totale à la fréquence de risque tolérable pour le niveau de gravité associé. Si la fréquence d'événement intermédiaire totale dépasse la fréquence tolérable, une réduction de risque est alors nécessaire. Il convient de considérer les méthodes et les solutions de sécurité intrinsèquement plus sûres avant d'appliquer des couches de protection supplémentaires sous la forme d'un système E/E/PE relatif à la sécurité.

Si les valeurs de la probabilité d'événement intermédiaire ne peuvent être ramenées à un niveau inférieur aux critères de fréquence maximale, un système E/E/PE relatif à la sécurité est alors nécessaire.

F.10 Niveaux d'intégrité de sécurité (SIL)

Si une fonction de sécurité est nécessaire, le SIL requis peut être déterminé comme suit:

– Diviser la fréquence maximale du niveau de gravité associé par la probabilité d'événement intermédiaire totale pour déterminer la PFD_{avg} requise,
– La valeur numérique cible de la PFD_{avg} peut alors être utilisée dans la spécification des exigences de sécurité avec le SIL associé. Le SIL associé peut être obtenu à partir du Tableau 2 de la CEI 61508-1,
– Si la valeur numérique de PFD_{avg} ne doit pas figurer dans la spécification des exigences de processus et que seul le SIL requis doit être spécifié, il convient que le SIL soit supérieur d'un niveau afin d'obtenir la réduction de risque appropriée avec toutes les valeurs de PFD_{avg} associées au SIL spécifié,

Si la valeur de la PFD_{avg} requise pour le risque tolérable est supérieure à 0,1, le classement « Aucune exigence d'intégrité de sécurité spéciale » est alloué à la fonction.

F.11 Probabilité d'événement limitée tolérable

Cette probabilité dépend du niveau de gravité des conséquences. Ce niveau dépend pour sa part des critères de risque tolérable adoptés (voir A.2 pour les critères de risque tolérable).

Annexe G
(informative)

Détermination des niveaux d'intégrité de sécurité – Une méthode qualitative – Matrice de gravité des événements dangereux

G.1 Généralités

La méthode numérique décrite à l'Annexe D n'est pas applicable lorsque le risque (ou son élément fréquence) ne peut pas être quantifié. La présente annexe décrit la méthode dite matrice de gravité des événements dangereux. Il s'agit d'une méthode qualitative développée dans le but de déterminer le niveau d'intégrité de sécurité d'un système E/E/PE relatif à la sécurité à partir des facteurs de risque connus associés à l'EUC et à son système de commande. Cette méthode est particulièrement applicable lorsque le modèle de risque est comparable à celui décrit aux Figures A.1 et A.2.

Le plan présenté dans la présente annexe suppose l'indépendance de chaque système relatif à la sécurité et de chaque dispositif externe de réduction de risque.

La présente annexe n'a pas pour objectif de figer la méthode, mais elle illustre en revanche les principes généraux de développement d'une matrice de ce genre par les personnes disposant d'une connaissance précise des paramètres spécifiques applicables à la construction de ladite matrice. Il convient que les personnes souhaitant appliquer les méthodes décrites dans la présente annexe consultent les sources documentaires référencées.

NOTE Des informations supplémentaires sur les matrices de gravité des événements dangereux sont données dans la référence [4] dans la Bibliographie.

G.2 Matrice de gravité des événements dangereux

Les exigences suivantes sont à la base de la construction d'une matrice et il est nécessaire de se conformer à chacune d'elle pour que la méthode soit valable:

a) les systèmes E/E/PE relatifs à la sécurité et les dispositifs externes de réduction de risque sont indépendants,

b) chaque système relatif à la sécurité (E/E/PE et ceux basés sur d'autres technologies), ainsi que les dispositifs externes de réduction de risque, sont considérés comme des couches de protection qui procurent, par eux-mêmes, des réductions partielles de risque, comme indiqué à la Figure A.1,

NOTE 1 Cette hypothèse est valable uniquement si des essais périodiques des couches de protection sont effectués régulièrement.

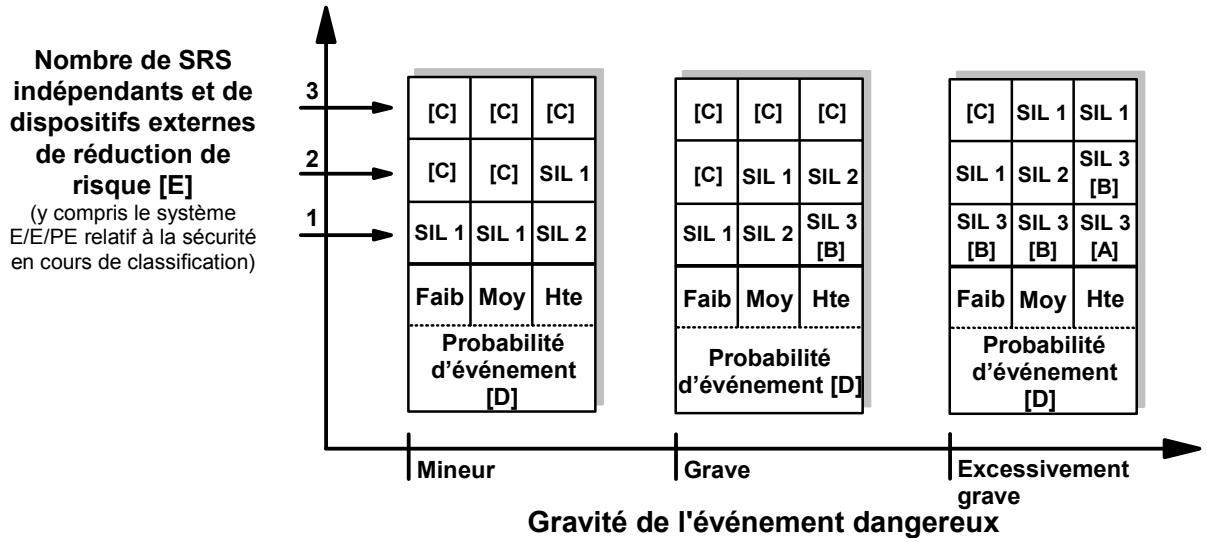
c) lorsqu'une couche de protection (voir b) ci-dessus) est ajoutée, elle réalise alors une amélioration d'un ordre de grandeur de l'intégrité de sécurité,

NOTE 2 Cette hypothèse est valable uniquement si les systèmes relatifs à la sécurité et les dispositifs externes de réduction de risque ont un niveau d'indépendance approprié.

d) un seul système E/E/PE relatif à la sécurité est utilisé (mais cela peut être en combinaison avec un système relatif à la sécurité basé sur une autre technologie et/ou des dispositifs externes de réduction de risque), pour lequel cette méthode établit le niveau d'intégrité de sécurité nécessaire,

e) Les considérations ci-dessus conduisent à la matrice de gravité des événements dangereux présentée à la Figure G.1. Il convient de noter que cette matrice a été enrichie avec des données pour exemple afin d'illustrer les principes généraux. Pour chaque situation spécifique ou pour des industries de secteurs comparables, une matrice similaire

à celle de la Figure G.1 est développée et étalonnée selon les critères de risque tolérable applicables à la situation.



[A] Une fonction de sécurité E/E/PE SIL 3 n'apporte pas une réduction suffisante de risque à ce niveau de risque. Des mesures supplémentaires de réduction de risque sont nécessaires.

[B] Une fonction de sécurité E/E/PE SIL 3 peut ne pas apporter une réduction suffisante de risque à ce niveau de risque. L'analyse des risques et des dangers est requise pour déterminer si des mesures supplémentaires de réduction de risque sont nécessaires.

[C] Une fonction de sécurité E/E/PE indépendante n'est probablement pas nécessaire.

[D] La probabilité d'événement est la probabilité que l'événement dangereux survienne sans fonction de sécurité ou sans dispositif externe de réduction de risque.

[E] La probabilité d'événement et le nombre total de couches de protection indépendantes sont définis en relation avec l'application spécifique.

Figure G.1 – Matrice de gravité des événements dangereux – exemple (illustre uniquement les principes généraux)

Bibliographie

[1] CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[2] CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[3] CEI 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional* (disponible en anglais seulement)

[4] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries* (disponible en anglais seulement)

[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> (disponible en anglais seulement)

[6] The Motor Industry Research Association, 1994, ISBN 09524156 0 7, *Development guidelines for vehicle based software* (disponible en anglais seulement)

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

[8] CCPS ISBN 0-8169-0811-7, *Layer of Protection Analysis – Simplified Process Risk Assessment* (disponible en anglais seulement)

[9] ISO/CEI 31010, *Gestion des risques – Techniques d'évaluation des risques*[3]

[10] ISO 10418:2003, *Industries du pétrole et du gaz naturel – Plates-formes de production en mer — Analyse, conception, installation et essais des systèmes essentiels de sécurité de surface*

[11] ISO/TR 14121-2, *Sécurité des machines – Appréciation du risque – Partie 2: Lignes directrices pratiques et exemples de méthodes*

[12] ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

[13] CEI 60601 (toutes les parties), *Appareils électromédicaux*

[14] CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques /électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences concernant les systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*

[15] CEI 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

[16] CEI 61508-6, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

[17] CEI 61508-7, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

3 A publier.

[18] CEI 61511-1, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel*

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