IEC 61508-5

Edition 1.0 1998-12

INTERNATIONAL STANDARD

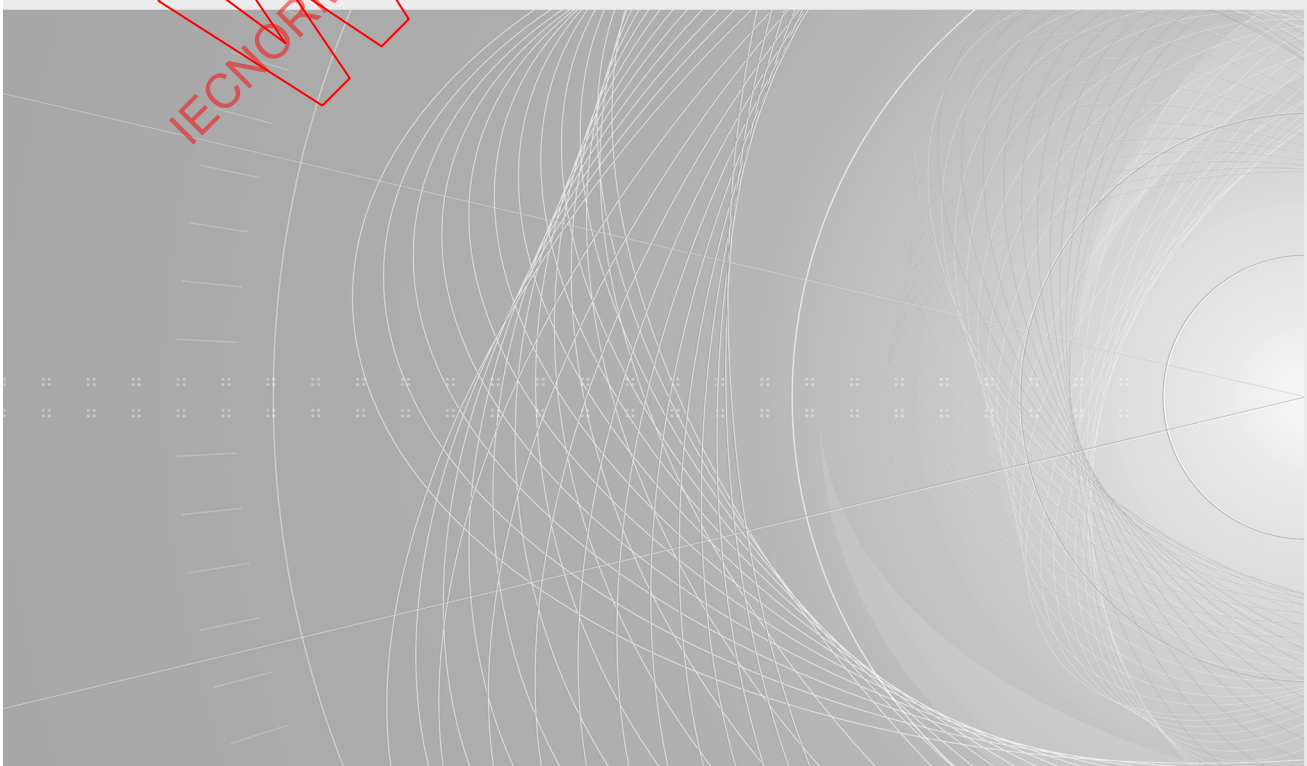
NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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 de détermination des niveaux d'intégrité de sécurité



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 It also gives information on projects, withdrawn and replaced publications.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 1.0 1998-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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 de détermination des niveaux d'intégrité de sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX U

ICS 25.040.40

ISBN 2-8318-4596-3

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 IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The 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 and control.

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

FDIS	Report on voting
65A/266/FDIS	65A/276/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.

Annexes A, B, C, D, E and F are for information only.

IEC 61508 consists of the following parts, under the general title Functional safety of electrical/ electronic/programmable electronic safety-related systems:

– Part 1: General requirements
– Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
– Part 3: Software requirements
– Part 4: Definitions and abbreviations
– Part 5: Examples of methods for the determination of safety integrity levels
– Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
– Part 7: Overview of techniques and measures

This part 5 shall be read in conjunction with part 1.

It has the status of a basic safety publication in accordance with IEC Guide 104.

The contents of the corrigendum of April 1999 have been included in this copy.

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) 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 those 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 components (electrical/electronic/ programmable electronic systems (E/E/PESs)) 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 application sector standards.

In most situations, safety is achieved by a number of protective 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 electrical/electronic/programmable electronic (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 recognised that there is a great variety of E/E/PES applications 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 Standard, by being generic, will enable such measures to be formulated in future application sector international standards.

This International Standard:

– considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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 application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this International 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;

– uses 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;

– adopts a risk-based approach for the determination of the safety integrity level requirements;

– sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for 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 failure of 10^{-5} to perform its design function on demand;

  – a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not use the concept of fail safe which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

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, other technology safety-related systems and external risk reduction facilities to be determined (see annexes B, C, D and E).

1.2 The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes B, C, D and E 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, D and E, see references [4], [2] and [3] respectively in annex F. See also reference [5] in annex F for a description of an additional approach.

1.3 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 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*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

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.

NOTE – In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard in the USA and Canada, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-5 plays in the achievement of functional safety for E/E/PE safety-related systems.

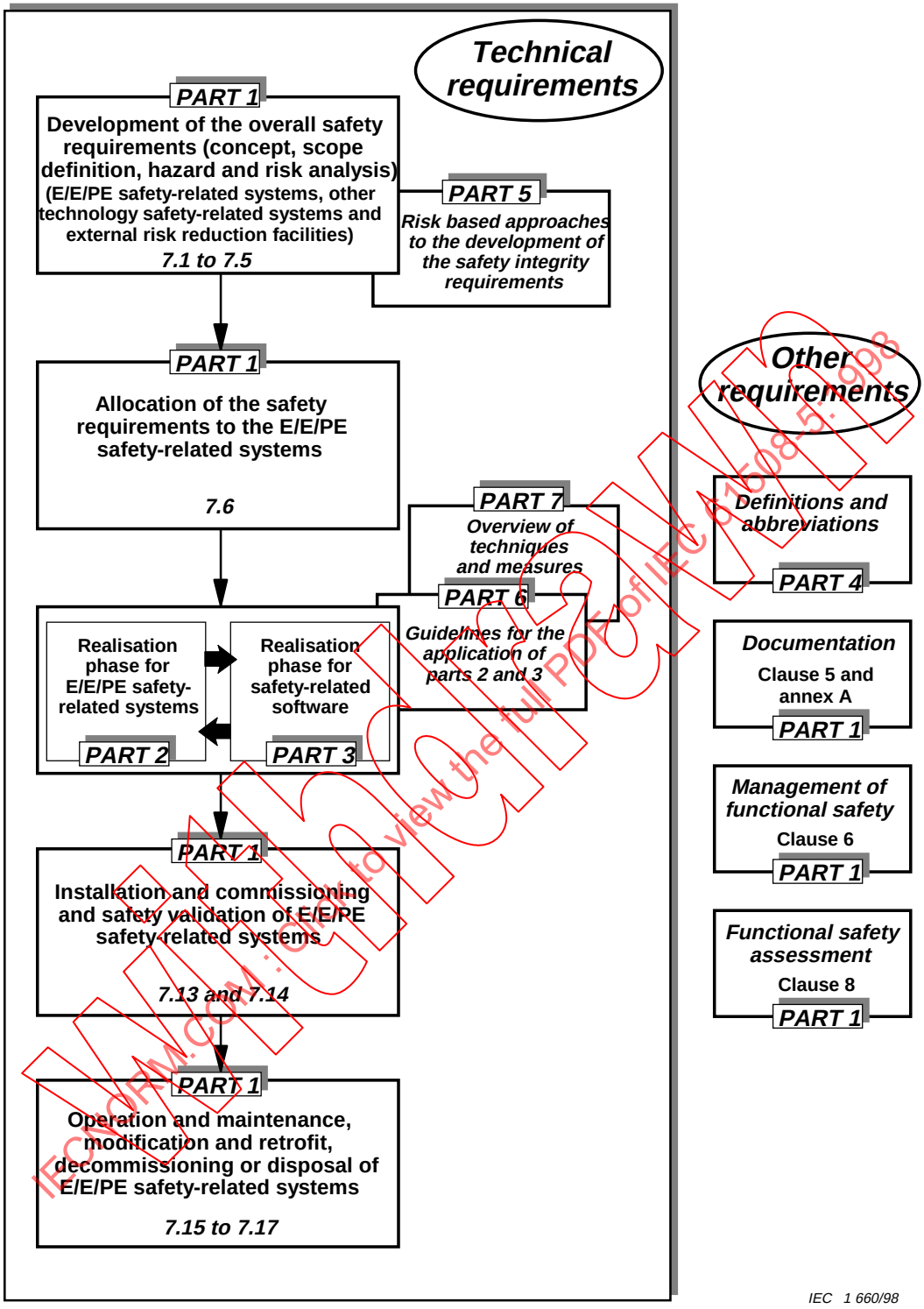


Figure 1 – Overall framework of this standard

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61508-1:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2,— *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronical/programmable electronic safety-related systems* [1)]

IEC 61508-3:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-6,— *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3* [1)]

IEC 61508-7,— *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* [1)]

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

3 Definitions and abbreviations

For the purposes of this standard, the definitions and abbreviations given in part 4 apply.

1) To be published.

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 3.5.14 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:

– 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 are becoming increasingly important in arriving at tolerable risk criteria for specific applications;
– the best independent industrial, expert and scientific advice from advisory bodies;
– legal requirements, both general and those directly relevant to the specific application.

---

1) In achieving the tolerable risk, the necessary risk reduction will need to be established. Annexes D and E of IEC 61508-5 outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly rather than stated explicitly.

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

E/E/PE safety-related systems contribute towards meeting 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, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions (3.4.1 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 3.5.12 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 (3.5.2 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 3.5.5 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 3.5.4 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). A judgement therefore has to be made on the selection of the best techniques to minimise this uncertainty. Note that it is not necessarily 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.

The required safety integrity of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, must be of such a level so as to ensure that

– the failure frequency 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 an EUC control system;
– there are associated human factor issues;
– the safety protective features comprise
  – external risk reduction facilities,
  – E/E/PE safety-related systems,
  – other technology safety-related systems.

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 technology safety-related systems and/or external risk reduction facilities. The resulting risk model may therefore differ from that shown in figure A.1.

The various risks indicated in figure A.1 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 3.2.4 of IEC 61508-4);
– tolerable risk; the risk which is accepted in a given context based on the current values of society (see 3.1.6 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 external risk reduction facilities, E/E/PE safety-related systems and other technology safety-related systems (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.

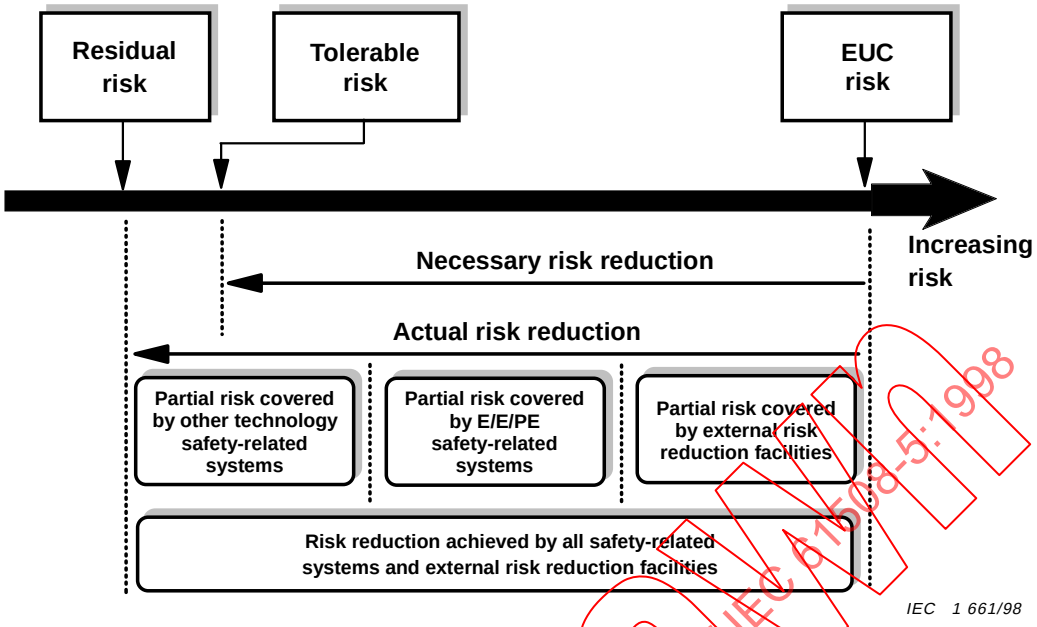


Figure A.1 – Risk reduction: general concepts

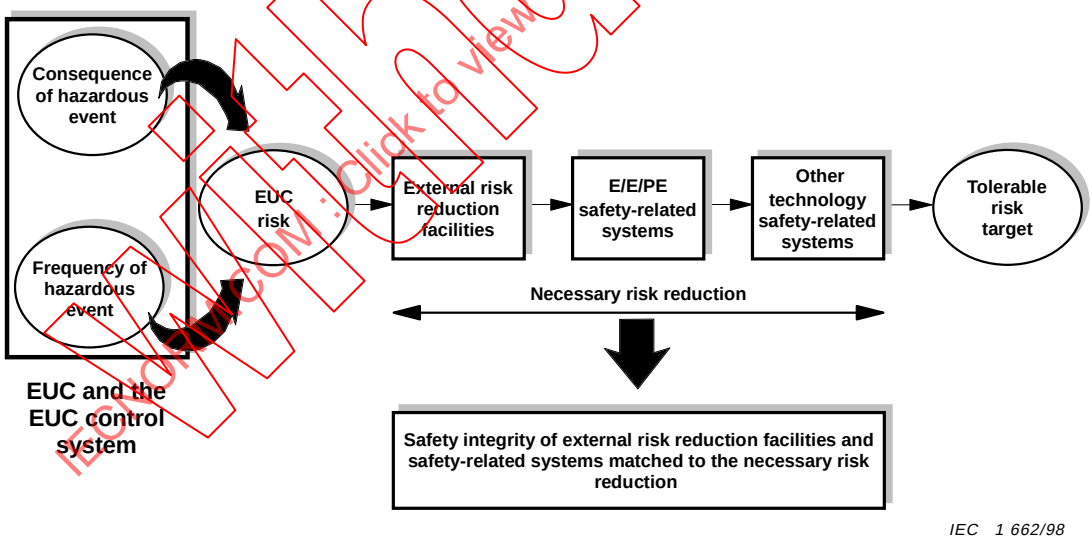


Figure A.2 – Risk and safety integrity concepts

A.5 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 required to meet the tolerable risk, actual risk (see figure A.1)). The tolerable risk is determined on a societal basis and involves consideration of societal and political factors. Safety integrity applies solely to the E/E/PE safety-related systems, other technology safety related-systems and external risk reduction facilities 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.

The role that safety-related systems play in achieving the necessary risk reduction is illustrated in figures A.1 and A.2.

A.6 Safety integrity levels and software safety integrity levels

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 safety integrity levels are used as the basis of specifying the safety integrity requirements of the safety functions implemented 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.

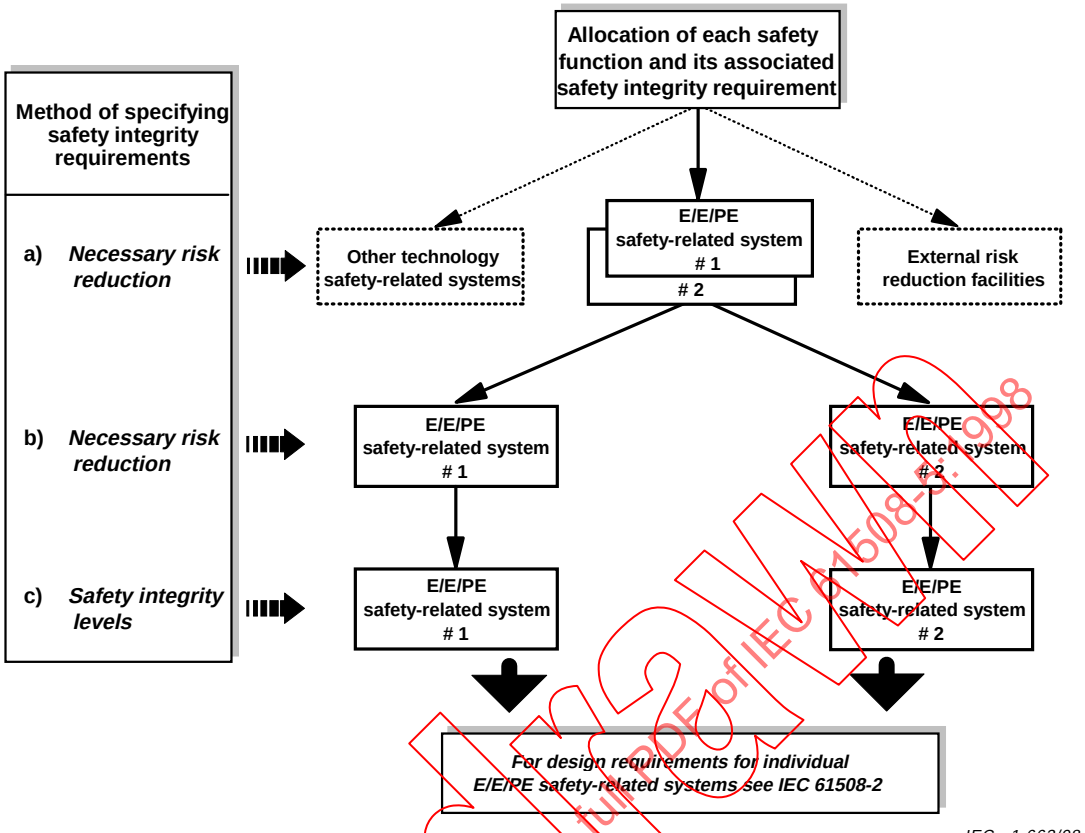
The safety integrity level target failure measures for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1. Two parameters are specified, one for safety-related systems operating in a low demand mode of operation and one for safety-related systems operating in a high demand 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 3.5.12 and 3.5.13 of IEC 61508-4).

A.7 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 external risk reduction facilities is shown in figure A.3 (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 external risk reduction facilities 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 B, C, D and E).



NOTE 1 – Safety integrity requirements are associated with each safety function before allocation (see 7.5.2.6 of IEC 61508-1).

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

Figure A.3 – Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

Annex B
(informative)

ALARP and tolerable risk concepts

B.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. Those intending to apply the methods indicated in this annex should consult the source material referenced.

B.2 ALARP model

B.2.1 Introduction

Subclause A.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 must 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 must 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 B.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, the less proportionately, need be spent to reduce them and at the lower end of the tolerability region, a balance between costs and benefits will suffice.

Below the tolerability region, the levels of risk are regarded as so insignificant that the regulator need not ask for further improvements. This 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.

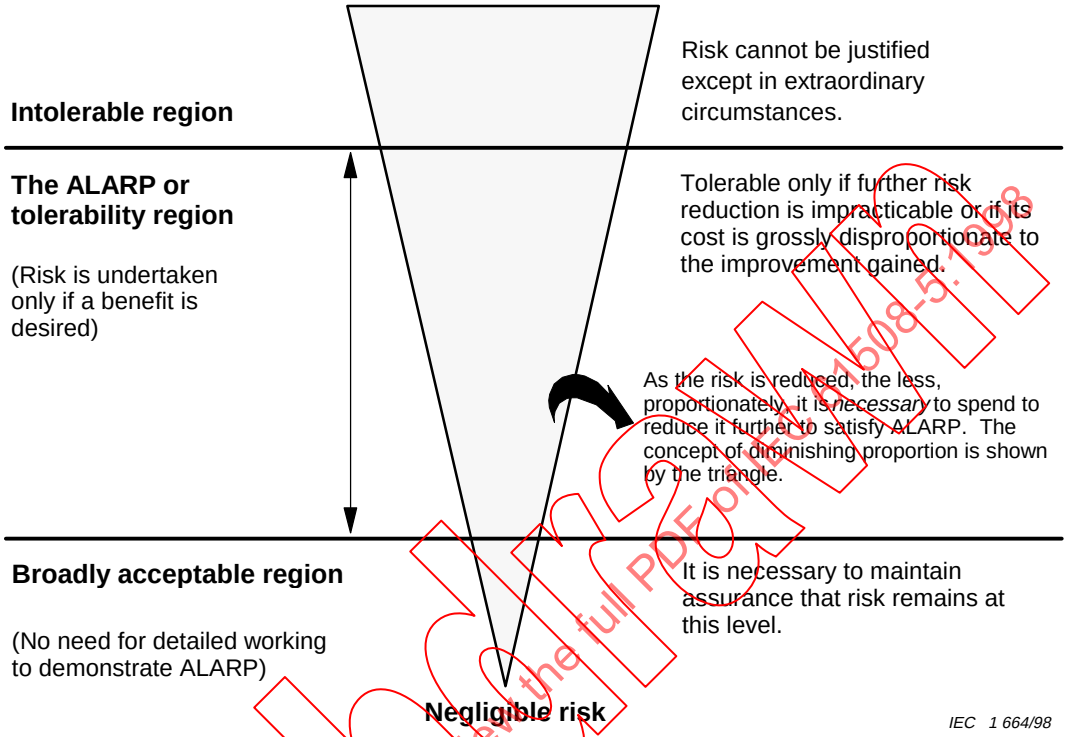


Figure B.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Subclause B.2.2 outlines a method for quantitative risk targets. (Annex C outlines a quantitative method and annexes D and E 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 [4] in annex F.

B.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 B.1 is an example showing four risk classes (I, II, III, IV) for a number of consequences and frequencies. Table B.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 B.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 B.1, the risk classes are as follows:

– risk class I is in the unacceptable 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 B.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 B.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 B.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 C.

Table B.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 C
(informative)

Determination of safety integrity levels: a quantitative method

C.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 B.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.

C.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 B.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 external risk reduction facilities (see 7.6 of IEC 61508-1).

Table B.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.

C.3 Example calculation

Figure C.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 safety integrity failure measure for safety-related protection systems operating in a low demand mode of operation (see table 2 of IEC 61508-1 and 3.5.12 of IEC 61508-4);

F_t is the tolerable risk frequency;

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

Also in figure C.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 C.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 B.1, whether for frequency F_{np} and consequence C a tolerable risk level is achieved. If, through the use of table B.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 B.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, $PFD_{avg} = (F_t / F_{np}) = \Delta R$;

– for $PFD_{avg} = (F_t / F_{np})$, 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).

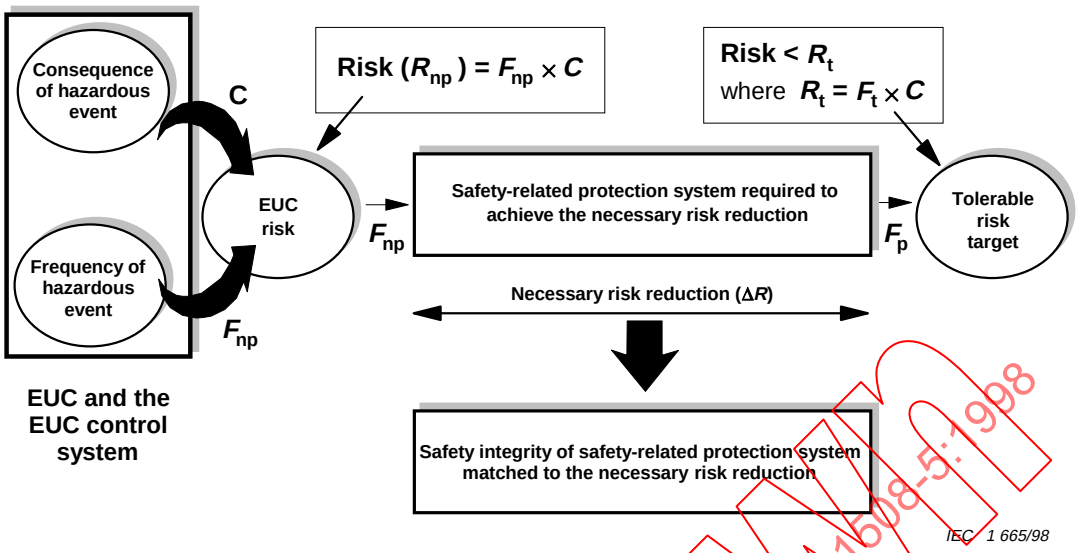


Figure C.1 – Safety integrity allocation: example for safety-related protection system

Annex D
(informative)

Determination of safety integrity levels – A qualitative method: risk graph

D.1 General

This annex describes the risk graph method, which is a qualitative 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.

Where a qualitative 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-related systems. 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. Those intending to apply the methods indicated in this annex should consult the source material referenced.

D.2 Risk graph synthesis

The following simplified procedure is based on the following equation:

$$R = f \times C$$

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 external 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*).

D.3 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. For example, the use of new technologies in the EUC and the EUC control system. The purpose of the additional parameters would be to more accurately estimate the necessary risk reduction (see figure A.1).

D.4 Risk graph implementation: general scheme

The combination of the risk parameters described above enables a risk graph such as that shown in figure D.1 to be developed. With respect to figure D.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 D.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 W_1, W_2 or W_3 allows the contribution of other risk reduction measures to be made. The offset feature of the scales for W_1, W_2 and W_3 is to allow for three different levels of risk reduction from other measures. That is, scale W_3 provides the minimum risk reduction contributed by other measures (i.e. the highest probability of the unwanted occurrence taking place), scale W_2 a medium contribution and scale W_1 the maximum contribution. For a specific intermediate output of the risk graph (i.e. X_1, X_2... or X_6) and for a specific *W* scale (i.e. W_1, W_2 or W_3) 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 external risk reduction facilities) which are taken into account by the *W* scale mechanism, gives the necessary risk reduction for the specific situation.

The parameters indicated in figure D.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.

D.5 Risk graph example

An example of a risk graph implementation based on the example data in table D.1, is shown in figure D.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 (W_1, W_2 and W_3). 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.

NOTE – Further information on this risk graph implementation is given in reference [2] in annex F.

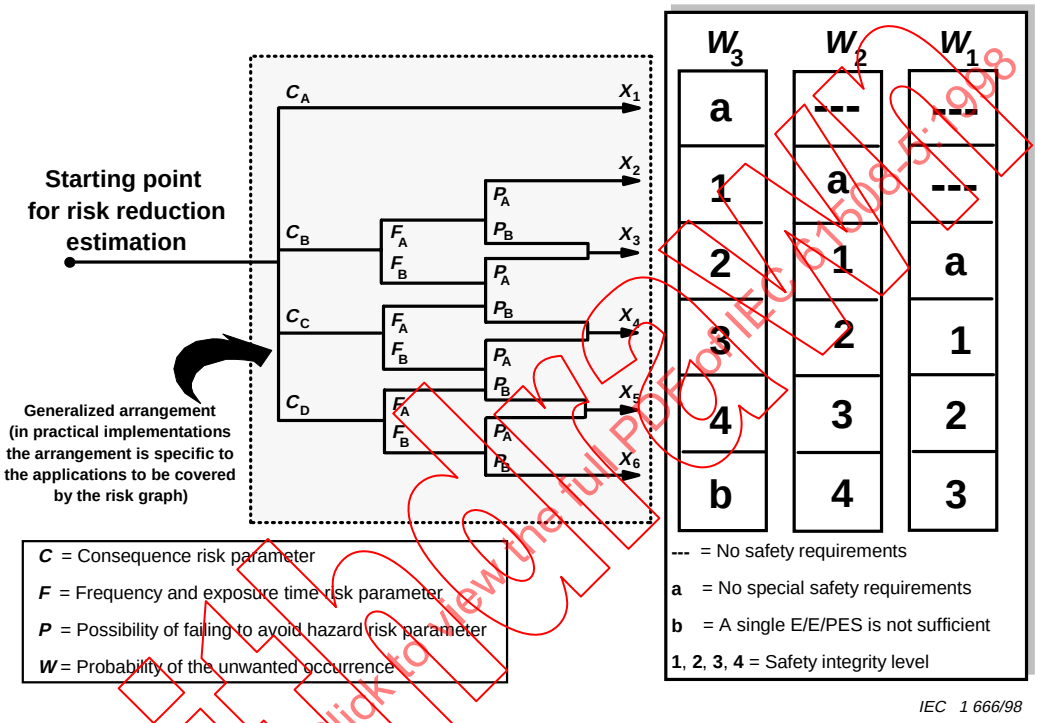
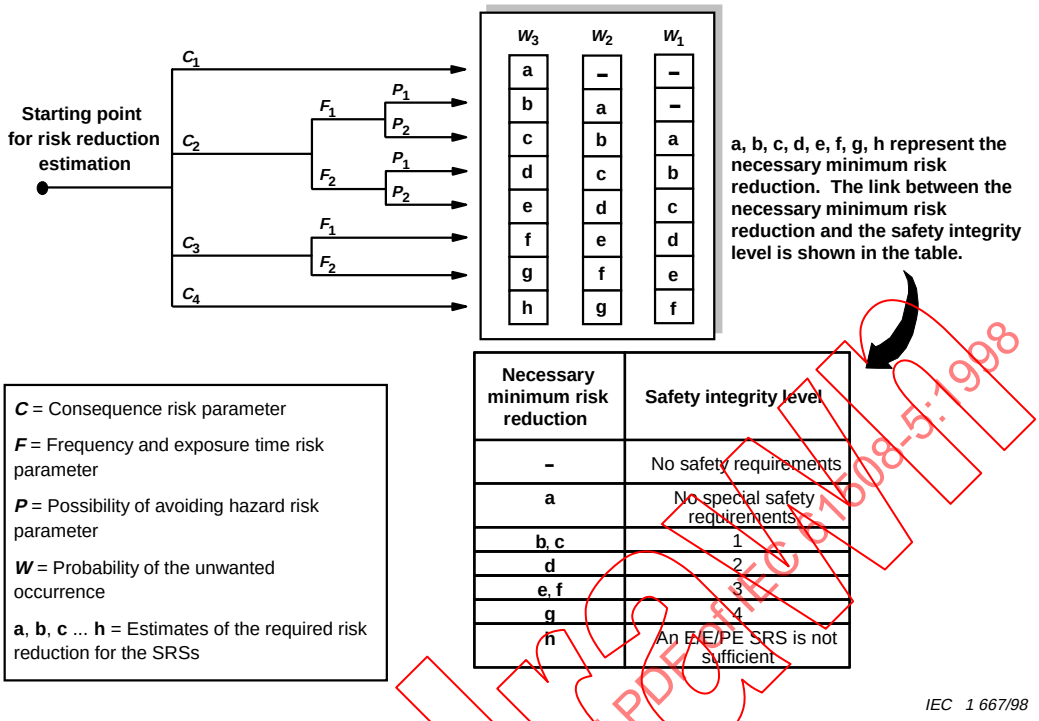


Figure D.1 — Risk graph: general scheme



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 SRS is not sufficient

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

Table D.1 – Example data relating to example risk graph (figure D.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 external risk reduction facilities.
	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	

Annex E
(informative)

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

E.1 General

The numeric method described in annex C 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 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 scheme outlined in this annex assumes that each safety-related system and external reduction facility 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 [3] in annex F.

E.2 Hazardous event severity matrix

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

a) the safety-related systems (E/E/PE and other technology) together with the external risk reduction facilities are independent;

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

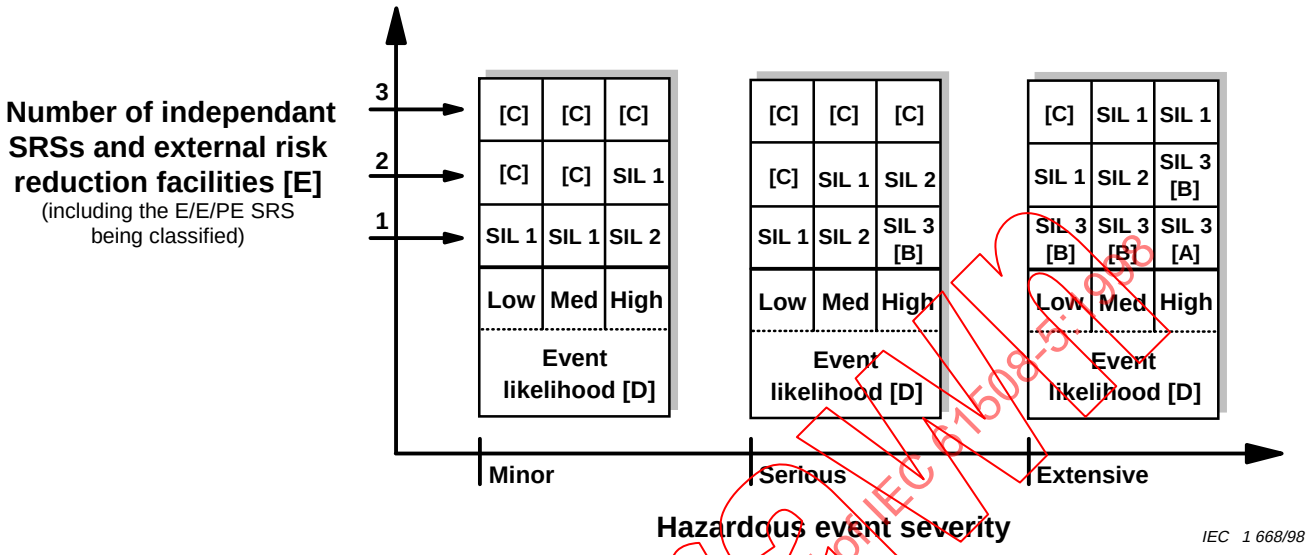
NOTE 1 – This assumption is valid only if regular proof tests of the protection layers are carried out.

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 external risk reduction facilities 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 external risk reduction facilities), for which this method establishes the necessary safety integrity level.

The above considerations lead to the hazardous event severity matrix shown in figure E.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 E.1 would be developed.



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

[B] One SIL 3 E/E/PE safety-related system 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-related system is probably not required.

[D] Event likelihood is the likelihood that the hazardous event occurs without any safety related systems or external risk reduction facilities.

[E] SRS = safety-related system. Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

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

Annex F
(informative)

Bibliography

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

[2] *Grundlegende Sicherheitberatungunge für MSR – Schutzeinrichtungen* DIN V 19250, Beuth Verlag, Berlin, FRG, 1994

[3] *Guidelines for safe automation of chemical process,* published by the Center for Chemical Process safety of the American Institute of Chemical Engineering, ISBN 0-8969-0554-1, 1993

[4] *Tolerability of risk from nuclear power stations,* Health and Safety Executive (UK) publication, ISBN 011 886368 1

[5] *Development guidelines for vehicle based software,* The Motor Industry Reliability Association, Watling St, Nuneation, Warwickshire, CV10 0TU, United Kingdom, 1994, ISBN 09524156 0 7

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité

AVANT-PROPOS

1) La CEI (Commission Electrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale 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 et commande dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/266/FDIS	65A/276/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.

Les annexes A, B, C, D, E et F sont données uniquement à titre d'information.

La CEI 61508 est composée des parties suivantes, regroupées sous le titre général Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité:

– Partie 1: Prescriptions générales
– Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
– Partie 3: Prescriptions concernant les logiciels
– Partie 4: Définitions et abréviations
– Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité
– Partie 6: Lignes directives pour l'application de la CEI 61508-2 et de la CEI 61508-3
– Partie 7: Présentation de techniques et mesures

La partie 5 doit être lue conjointement avec la partie 1.

Elle a le statut d'une publication fondamentale de sécurité conformément au Guide CEI 104.

Le contenu du corrigendum d'avril 1999 a été pris en considération dans cet exemplaire.

INTRODUCTION

Les systèmes électriques/électroniques sont utilisés depuis des années pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique (que l'on nommera de façon générique systèmes électroniques programmables (PES)) sont utilisés dans tous les secteurs d'application pour exécuter des fonctions non liées à la sécurité, mais aussi de plus en plus souvent liées 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 liés 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/électroniques/électroniques programmables (E/E/PES) 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 appareils électriques liés à la sécurité. L'un des principaux objectifs poursuivis consiste à faciliter l'élaboration de normes par secteur d'application.

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes de protection 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, les actionneurs), mais elle doit aussi considérer tous les systèmes relatifs à la sécurité comme des éléments individuels d'un ensemble complexe. C'est pourquoi la présente Norme internationale, bien que traitant essentiellement des E/E/PES, fournit néanmoins un cadre de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur des technologies différentes.

Personne n'ignore la grande variété des applications E/E/PES. Celles-ci recouvrent, à des degrés de complexité très divers, un fort potentiel de danger et de risques dans tous les secteurs d'application. Pour chaque application, la nature exacte des mesures de sécurité envisagées dépendra de plusieurs facteurs propres à l'application. La présente Norme internationale, de par son caractère général, rendra désormais possible la prescription de ces mesures dans des normes internationales par secteur d'application.

La présente Norme internationale:

– concerne toutes les phases du cycle de vie de sécurité (depuis la conceptualisation initiale, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service) lorsque les E/E/PES exécutent des fonctions de sécurité;

– a été élaborée dans le souci de l'évolution rapide des technologies; le cadre fourni par cette Norme internationale est suffisamment solide et étendu pour pourvoir aux évolutions futures;

– permet l'élaboration de Normes internationales par secteur d'application concernant les E/E/PES relatifs à la sécurité. L'élaboration de normes internationales par secteur d'application à partir de la présente Norme internationale devrait permettre d'atteindre un haut niveau de cohérence (par exemple pour ce qui est des principes sous-jacents, de la terminologie, de la documentation, etc.) à la fois au sein de chaque secteur d'application, et d'un secteur à l'autre. La conséquence en est une amélioration en termes de sécurité et de bénéfices économiques;

– fournit une méthode de développement des prescriptions de sécurité nécessaires pour réaliser la sécurité fonctionnelle requise des systèmes de sécurité E/E/PE;

– utilise des niveaux d'intégrité de sécurité afin de spécifier les niveaux cibles d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes de sécurité E/E/PE;

– adopte une approche basée sur le risque encouru pour déterminer les niveaux d'intégrité de sécurité prescrits;

– fixe des objectifs quantitatifs pour les mesures de défaillances des systèmes de sécurité E/E/PE qui sont en rapport avec les niveaux d'intégrité de sécurité;

– fixe une limite inférieure pour les mesures de défaillances, dans le cas d'un mode de défaillance dangereux, cette limite pouvant être exigée pour un système de sécurité E/E/PE unique. Dans le cas d'un système de sécurité E/E/PE fonctionnant

  – dans un mode de faible sollicitation, la limite inférieure est fixée à une probabilité moyenne de défaillance de 10^{-5} afin que les fonctions pour lesquelles le système a été conçu soient exécutées lorsqu'elles sont requises;

  – dans un mode de fonctionnement continu ou de forte sollicitation, la limite inférieure est fixée à une probabilité de défaillance dangereuse de 10^{-9} par heure.

  NOTE – Un système de sécurité E/E/PE unique n'implique pas nécessairement une architecture à une seule voie.

– adopte une large gamme de principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes de sécurité E/E/PE, mais n'utilise pas le concept de «sécurité intrinsèque» qui a un sens particulier lorsque les modes de défaillances sont bien définis et que le niveau de complexité est relativement faible. Ce concept a été considéré comme inadéquat en raison de l'immense gamme de complexité des systèmes de sécurité E/E/PE qui entrent dans le domaine d'application de la présente norme.

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ –

Partie 5: Exemples de méthodes de 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);

– des méthodes qui permettront d'assurer le niveau d'intégrité de sécurité des systèmes E/E/PE relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur d'autres technologies et des dispositifs externes de réduction de risque (voir annexes B, C, D et E).

1.2 La méthode retenue dépendra du secteur d'application et des conditions spécifiques à prendre en considération. Les annexes B, C, D et E 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 explication définitive. Pour utiliser les méthodes indiquées dans ces annexes, il convient de consulter les sources indiquées.

NOTE – Pour plus d'informations concernant les approches illustrées par les annexes B, D et E, voir respectivement les références [4], [2] et [3] qui se trouvent en annexe F. Voir aussi la référence [5] de l'annexe F qui décrit une autre approche.

1.3 Les parties 1, 2, 3 et 4 de la présente norme sont des publications fondamentales de sécurité, bien qu'un tel statut ne soit pas applicable dans le contexte des systèmes E/E/PE de faible complexité relatifs à la sécurité (voir 3.4.4 de la partie 4). En tant que publications fondamentales de sécurité, ces normes sont prévues pour être utilisées par les comités techniques pour la préparation des normes selon les principes contenus dans le *Guide CEI 104* et le *Guide ISO/CEI 51*. Les parties 1, 2, 3 et 4 sont également destinées à être utilisées comme publications autonomes.

Une des responsabilités incombant à un comité technique est, dans la mesure du possible, d'utiliser les publications fonda-mentales de sécurité, pour la préparation de ses publications. Dans ce contexte les prescriptions, les méthodes d'essai ou 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 techniques.

NOTE – Aux Etats-Unis d'Amérique et au Canada, les normes nationales de sécurité des processus existantes, basées sur la CEI 61508 (par exemple l'ANSI/ISA S84.01-1996, voir référence [8] à l'annexe C) peuvent être appliquées dans le domaine des processus, à la place de la CEI 61508, et cela jusqu'à ce que les normes internationales concernant la mise en œuvre de la CEI 61508 dans le domaine des processus soient publiées.

1.4 La figure 1 montre la structure générale des parties 1 à 7 de la CEI 61508 et indique le rôle de la CEI 61508-5 dans la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité.

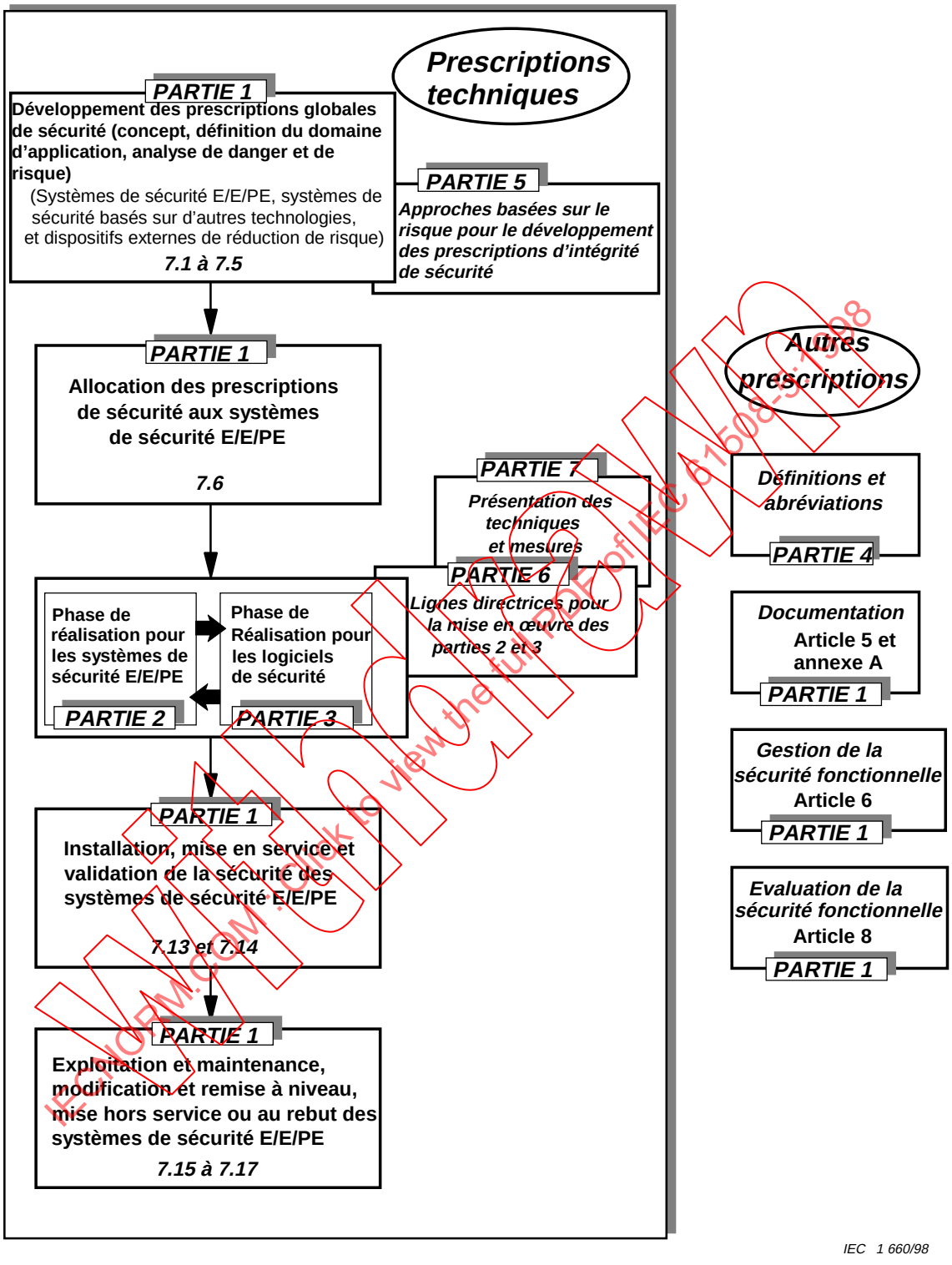


Figure 1 – Structure générale de la présente norme

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de sa publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 61508-1:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité* [1)]

CEI 61508-3:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998, *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-6,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application des parties 2 et 3* [1)]

CEI 61508-7,— *Sûreté fonctionelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures* [1)]

Guide ISO/CEI 51:1990, *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité*

Guide CEI 104:1997, *Guide pour la rédaction des normes de sécurité et rôle des comités chargés de fonctions pilotes de sécurité et de fonctions groupées de sécurité*

3 Définitions et abréviations

Pour les besoins de la présente norme, les définitions et les abréviations données à la partie 4 s'appliquent.

[1)] A publier.

Annexe A
(informative)

Risques et intégrité de sécurité – Concepts généraux

A.1 Généralités

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

A.2 Réduction nécessaire du risque

La réduction nécessaire du risque (voir 3.5.14 de la CEI 61508-4) est la réduction du risque qui doit être réalisée pour atteindre le risque tolérable dans une situation spécifique (qui peut être définie soit qualitativement [1] soit quantitativement [2]). Le concept de réduction nécessaire du risque est d'une importance fondamentale dans la réalisation des spécifications de prescriptions de sécurité pour les systèmes E/E/PE relatifs à la sécurité (en particulier, les prescriptions d'intégrité de sécurité qui font partie de la spécification des prescriptions de sécurité). La détermination du risque tolérable pour un événement dangereux a pour but d'établir ce qui est jugé raisonnable eu égard à la fréquence (ou probabilité) de l'événement dangereux et à 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 niveau de sécurité requis dépend de nombreux facteurs (par exemple la gravité des blessures, le nombre de personnes exposées au risque, 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 au danger seront des facteurs importants. Pour définir le risque tolérable d'une application spécifique, les points suivants sont considérés:

– les lignes directrices émises par l'autorité réglementaire 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 sécurité appropriés pour les applications spécifiques;
– les avis indépendants les plus pertinents émis par des organismes consultatifs représentant l'industrie, les experts et les scientifiques;
– les prescriptions légales, générales et celles relevant du domaine spécifique.

---

[1] Lors de la détermination du risque tolérable, la réduction nécessaire du risque devra être établie. Les annexes D et E de la CEI 61508-5 décrivent les grandes lignes des méthodes qualitatives, bien que dans les exemples donnés, la réduction nécessaire du risque soit incluse implicitement plutôt que clairement explicitée.

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

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

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

Un système relatif à la sécurité

– met en oeuvre les fonctions de sécurité requises et nécessaires pour parvenir à un état de sécurité de l'équipement commandé, ou maintient l'équipement commandé dans un état de sécurité, et

– permet d'atteindre, par lui-même ou en liaison avec d'autres systèmes E/E/PE relatifs à la sécurité ou des systèmes relatifs à la sécurité basés sur d'autres technologies ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire pour la mise en oeuvre des fonctions de sécurité (voir 3.4.1 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 peuvent être spécifiées dans la spécification des prescriptions de fonctions de sécurité. Par exemple, la spécification des prescriptions de fonctions de sécurité peut spécifier que quand la température atteint X, la vanne Y doit s'ouvrir pour permettre à l'eau d'entrer.

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, pour permettre d'atteindre le risque tolérable.

Une personne pourrait être partie intégrante d'un système E/E/PE relatif à la sécurité. Par exemple, une personne pourrait recevoir des informations sur l'état de l'équipement commandé depuis un écran et accomplir une activité de sécurité sur la base de cette information.

Les systèmes E/E/PE relatifs à la sécurité peuvent fonctionner en mode demande faible ou en mode demande élevé ou mode continu (voir 3.5.12 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 (3.5.2 de la CEI 61508-4). L'intégrité de sécurité renvoie aux performances de systèmes relatifs à la sécurité lors de l'exécution de fonctions de sécurité (les fonctions de sécurité à mettre en oeuvre seront présentées dans la spécification des prescriptions relatives aux 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 dans un mode dangereux de défaillances (voir 3.5.5 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 spécifications peuvent être réparties entre les sous-systèmes en utilisant les règles usuelles de combinaison de probabilité. 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 dans un mode de défaillance dangereux (voir 3.5.4 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'une anomalie de conception ou 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.

L'intégrité de sécurité requise d'un système E/E/PE relatif à la sécurité, ou de systèmes relatifs à la sécurité basés sur d'autres technologies et des dispositifs externes de réduction de risque, doit être à un niveau tel que

– la fréquence de défaillance des système relatif à la sécurité soit suffisamment basse pour éviter que la fréquence des événements dangereux n'excède la valeur requise pour atteindre le risque tolérable, et/ou
– les systèmes relatifs à la sécurité aient une action suffisante sur les conséquences des défaillances pour atteindre un niveau de risque tolérable.

La figure A.1 illustre les concepts généraux de réduction de risque. Le modèle général précise que

– il y a un EUC et un système de commande de l'EUC;
– il y a des problèmes liés au facteur humain;
– les équipements de sécurité comprennent
  – des dispositifs externes de réduction de risque;
  – des E/E/PES relatifs à la sécurité;
  – des systèmes relatifs à la sécurité basés sur d'autres technologies.

NOTE – La figure A.1 est un modèle de risque pour illustrer les principes généraux. Le modèle de risque pour une application spécifique nécessitera d'être développé en tenant compte des manières spécifiques dans lesquelles la réduction nécessaire du risque est accomplie par les systèmes E/E/PE relatifs à la sécurité et/ou par les systèmes relatifs à la sécurité basés sur d'autres technologies et/ou par 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 à la figure A.1 sont les suivants:

– risque EUC**:** risque encouru par l'EUC, son système de commande, et les facteurs humains associés pour les événements dangereux spécifiés. Aucun dispositif de protection spécifique n'est pris en compte dans la détermination de ce risque (voir 3.2.4 de la CEI 61508-4);
– risque tolérable: risque accepté dans un certain contexte fondé sur les valeurs actuelles de la société (voir 3.1.6 de la CEI 61508-4);
– risque résiduel effectif: risque encouru par l'EUC, son système de commande et les facteurs humains associés pour les événements dangereux spécifiés, y compris les dispositifs externes de réduction de risque, les E/E/PES relatifs à la sécurité et les systèmes relatifs à la sécurité basés sur d'autres technologies (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. Pour les demandes déraisonnables, de manière à prévenir des exigences déraisonnables pour l'intégrité de sécurité du système de commande de l'EUC, la présente norme définit des contraintes régissant les exigences qui peuvent être formulées (voir 7.5.2.5 de la CEI 61508-1).

La réduction nécessaire du risque est atteinte par combinaison de tous les dispositifs de protection relatifs à la sécurité. La réduction nécessaire du risque pour atteindre le risque tolérable spécifié, à partir du point initial du risque associé à l'EUC, est représentée à la figure A.1.

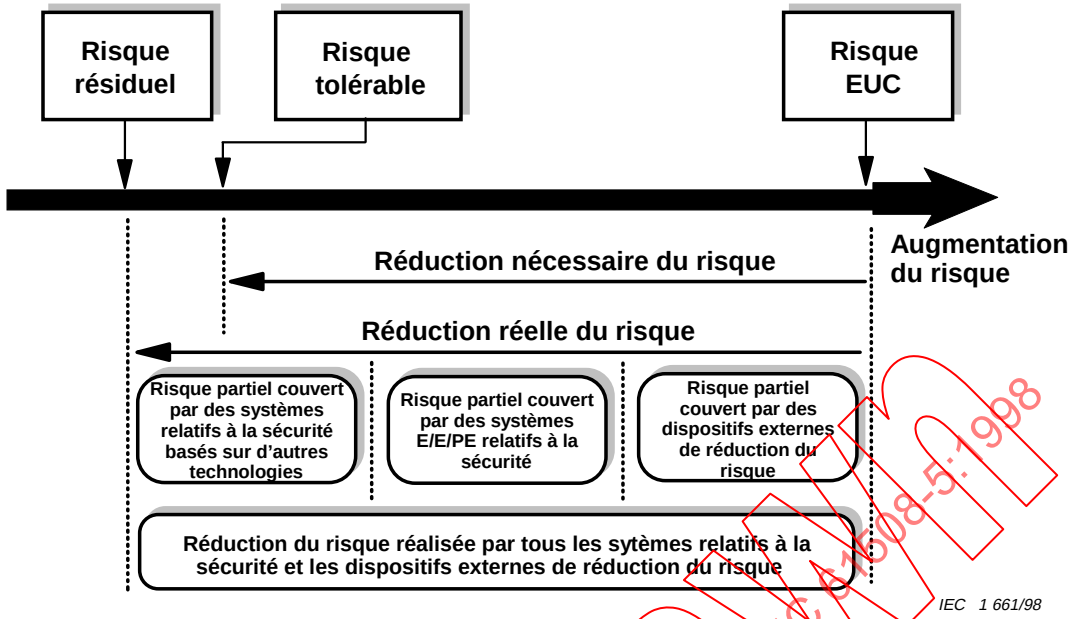


Figure A.1 – Réduction du risque: concepts généraux

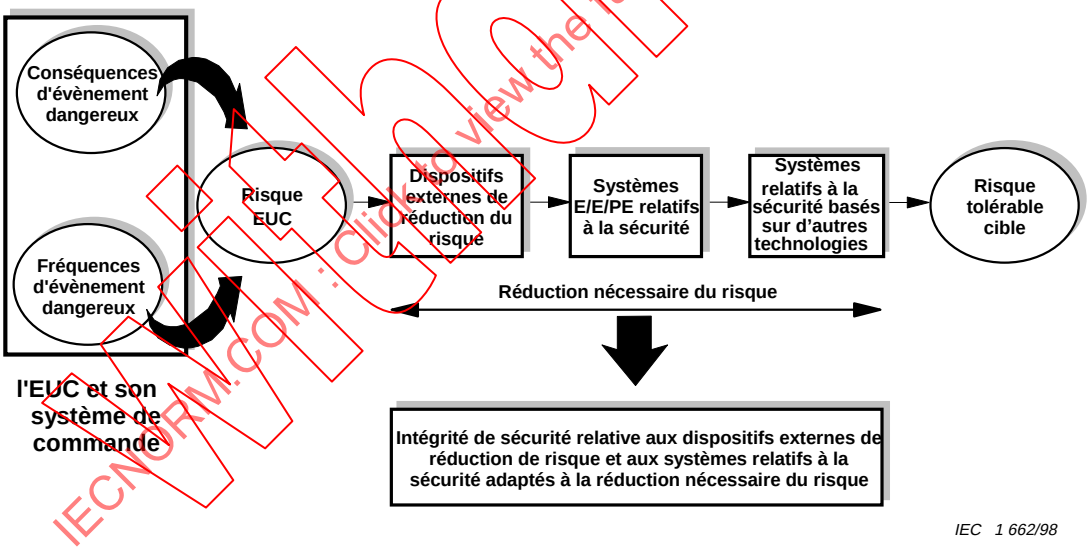


Figure A.2 – Concepts de risque et d'intégrité de sécurité

A.5 Risque et intégrité de sécurité

Il est important de faire pleinement la distinction entre risque et intégrité de sécurité. Le risque est une mesure de la probabilité pour qu'un événement dangereux spécifié se produise. Il peut être évalué pour différentes situations, par exemple le risque lié à l'EUC, le risque permettant d'atteindre le niveau de sécurité spécifié, le risque effectif (voir figure A.1). Le risque tolérable est déterminé au niveau de la société et inclut la prise en compte de facteurs politiques et sociaux. L'intégrité de sécurité s'applique exclusivement aux systèmes relatifs à la sécurité et correspond à la probabilité pour qu'un système relatif à la sécurité remplisse de manière satisfaisante les fonctions de sécurité requises. Une fois le niveau de sécurité défini et la réduction nécessaire du risque estimée, les prescriptions 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 prescriptions.

Le rôle joué par les systèmes relatifs à la sécurité dans la réduction nécessaire du risque est illustré aux figures A.1 et A.2.

A.6 Niveaux d'intégrité de sécurité et niveaux d'intégrité de sécurité du logiciel

Pour répondre au grand nombre de réductions de risques 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 prescriptions d'intégrité de sécurité des fonctions de sécurité allouées aux systèmes relatifs à la sécurité. Les niveaux d'intégrité de sécurité du logiciel sont à la base des spécifications des prescriptions d'intégrité de sécurité des fonctions de sécurité remplies par les logiciels relatifs à la sécurité. Il convient que les spécifications de prescriptions d'intégrité de sécurité spécifient 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.

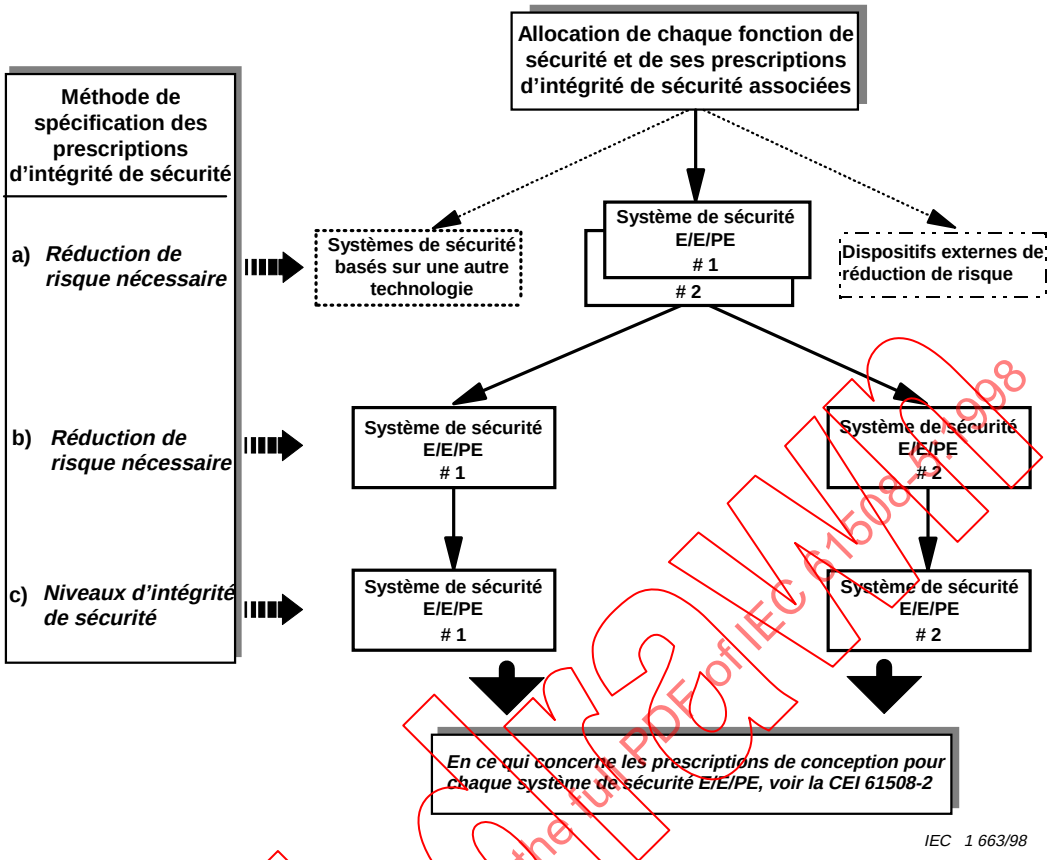
Les objectifs en matière d'intégrité de sécurité pour les quatre niveaux d'intégrité de sécurité sont spécifiés dans les tableaux 2 et 3 de la CEI 61508-1. Deux paramètres sont spécifiés, un pour les systèmes relatifs à la sécurité fonctionnant en mode demande basse et un pour les systèmes relatifs à la sécurité fonctionnant en mode demande continue ou élevée.

NOTE – Pour les systèmes relatifs à la sécurité fonctionnant en mode demande faible, la mesure de l'intégrité de sécurité est la probabilité de défaillance dans l'accomplissement sur demande de sa fonction. Pour les systèmes relatifs à la sécurité fonctionnant en mode demande continue ou élevée, la mesure de l'intégrité de sécurité est la probabilité moyenne d'une défaillance dangereuse par heure (voir 3.5.12 et 3.5.13 de la CEI 61508-4).

A.7 Allocation des prescriptions de sécurité

L'allocation des prescriptions de sécurité (les fonctions de sécurité et les prescriptions 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 est présentée à la figure A.3 (identique à la figure 6 de la CEI 61508-1). Les prescriptions pour la phase d'allocation des prescriptions de sécurité sont données en 7.6 de la CEI 61508-1.

Les méthodes utilisées pour allouer les prescriptions 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 du fait que la réduction nécessaire du risque est spécifiée d'une manière numérique ou qualitative. Ces approches sont appelées méthodes quantitatives ou qualitatives (voir annexes B, C, D et E).



NOTE 1 – Les prescriptions d'intégrité de sécurité sont associées à chaque fonction de sécurité avant l'allocation (voir 7.5.2.6 de la CEI 61508-1).

NOTE 2 – Une fonction de sécurité peut être allouée sur plusieurs systèmes de sécurité.

Figure A.3 – Allocation des prescriptions 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

Annexe B
(informative)

Concepts d'ALARP et de risque tolérable

B.1 Généralités

La présente annexe propose une approche particulière permettant de parvenir à un risque tolérable. Le but n'est pas de donner une explication définitive mais plutôt une illustration des principes généraux. Pour les personnes désirant mettre en application ces méthodes, il serait souhaitable de consulter les sources référencées.

B.2 Modèle ALARP

B.2.1 Introduction

Le paragraphe A.2 présente les principaux tests appliqués à la régulation des risques industriels et indique qu'il s'agit de déterminer si

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

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

c) le risque se situe entre les niveaux a) et b) définis ci-dessus et s'il a été ramené au plus bas niveau possible, eu égard aux bénéfices résultant de son acceptation et au coût qu'engendrerait toute réduction supplémentaire.

Si l'on considère le point c), le principe ALARP nécessite que tout risque soit ramené au plus bas niveau possible ou jusqu'à un niveau qui soit aussi faible que possible de manière raisonnable. 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 le risque tolérable pour l'application concernée. Cette approche des trois zones est illustrée à la figure B.1.

A partir 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 y a une zone tolérable où une activité peut avoir lieu si les risques associés sont aussi faibles que possible. Tolérable a ici une signification différente d'acceptable – cela indique un désir de vivre avec un risque dans le but d'assurer certains bénéfices, tout en supposant qu'il soit examiné et réduit quand il peut l'être. L'évaluation du bénéfice est demandée soit explicitement, soit implicitement pour mesurer le coût 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, les dépenses disproportionnées au bénéfice seraient justifiées. Ici le risque peut être considéré comme substantiel et l'équité demande qu'un effort considérable soit 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 de tolérabilité, il suffira d'équilibrer les coûts et les bénéfices.

Au-dessous de la zone tolérable, les niveaux de risque sont considérés comme tellement insignifiants que le besoin régulateur ne demande pas d'autres améliorations. C'est la zone étendue dans laquelle les risques sont faibles en comparaison avec les risques de tous les jours. Puisque ces risques sont dans la zone acceptable, il n'y a pas besoin d'un travail détaillé pour démontrer ALARP; il est nécessaire tout de même de rester vigilant pour s'assurer que le risque reste à ce niveau.

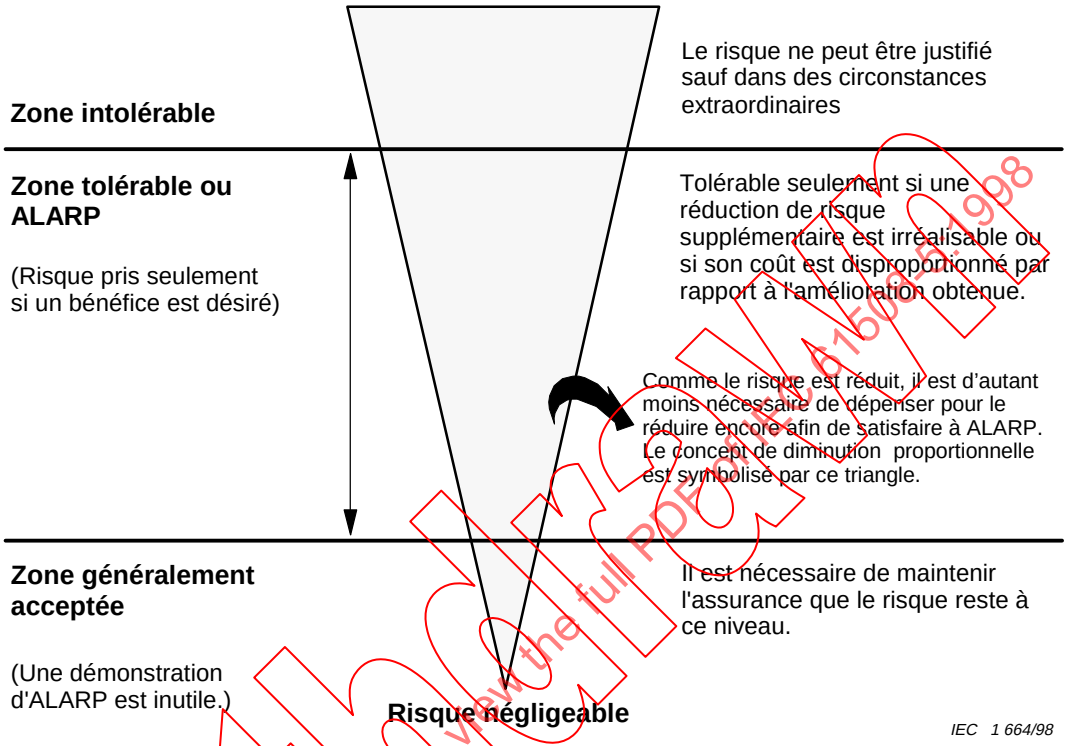


Figure B.1 – Risque tolérable et ALARP

Le concept d'ALARP peut être employé lorsque des objectifs de risque qualitatifs ou quantitatifs sont adoptés. Le paragraphe B.2.2 présente une méthode adaptée aux objectifs de risque quantitatifs. (L'annexe C présente une méthode quantitative et les annexes D et E des méthodes qualitatives pour la détermination de réduction nécessaire de risque pour un risque spécifique. Les méthodes indiquées pourraient incorporer le concept d'ALARP dans la prise de décision.)

NOTE – Des informations supplémentaires sur ALARP figurent en annexe F, référence [4].

B.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 d'une conséquence avec une fréquence tolérable peut se faire par l'intermédiaire de classes de risque. Le tableau B.1 présente quatre classes de risque (I, II, III, IV) pour un certain nombre de conséquences et de fréquences. Le tableau B.2 interprète chacune des classes de risque qui mettent en jeu le concept d'ALARP. La description de chacune des quatre classes de risque est basée sur la figure B.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 B.1, les classes de risque sont les suivantes:

– la classe de risque I se situe dans la zone inacceptable;

– les classes de risque II et III sont dans la zone ALARP; la classe de risque II est juste à l'intérieur de la zone ALARP;

– la classe de risque IV se situe dans la zone globalement acceptable.

Pour chaque situation spécifique, ou industrie de secteur comparable, un tableau comparable au tableau B.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 à un tableau comprenant les classes à risque. Par exemple, «fréquent» au tableau B.1 pourrait désigner un événement qui surviendrait en permanence, ce qui pourrait être spécifié par une fréquence supérieure à 10 fois par an. Une conséquence critique pourrait correspondre à un décès et/ou de multiples blessures graves ou une maladie professionnelle grave.

Tableau B.1 — Exemple de la classification 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 C.

Tableau B.2 — Interprétation des classes de risque

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

Annexe C
(informative)

Détermination des niveaux d'intégrité de sécurité: une méthode quantitative

C.1 Généralités

Cette 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 B.1 peut être utilisée. Une approche quantitative présente une valeur ajoutée, particulièrement dans les cas suivants:

– le risque tolérable doit été 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).

Cette annexe n'a pas pour objectif de figer la méthode mais elle illustre les principes généraux. Elle est particulièrement applicable lorsque le modèle de risque est tel qu'indiqué aux figures A.1 et A.2.

C.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-dessus et doivent être accomplies pour chaque fonction de sécurité réalisée par le système E/E/PE relatif à la sécurité:

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

– déterminer le risque EUC;

– déterminer la réduction nécessaire du risque pour atteindre le risque tolérable;

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

Le tableau B.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 déterminé

– 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.