Disclosure to Promote the Right To Information

Whereas the Parliament of India has set out to provide a practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, and whereas the attached publication of the Bureau of Indian Standards is of particular interest to the public, particularly disadvantaged communities and those engaged in the pursuit of education and knowledge, the attached public safety standard is made available to promote the timely dissemination of this information in an accurate manner to the public.

“जानने का अधिकार, जीने का अधिकार”
Mazdoor Kisan Shakti Sangathan
“The Right to Information, The Right to Live”

“पुराने को छोड नये के तरफ”
Jawaharlal Nehru
“Step Out From the Old to the New”

Indian Standard

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

PART 5 EXAMPLES OF METHODS FOR THE DETERMINATION OF SAFETY INTEGRITY LEVELS

ICS 25.040.40
CONTENTS

Clause

1 Scope ........................................................................................................ 1
2 Normative references .................................................................................. 3
3 Definitions and abbreviations ..................................................................... 3

Annexes

A Risk and safety integrity – General concepts ............................................ 4
B ALARP and tolerable risk concepts ............................................................. 10
C Determination of safety integrity levels: a quantitative method .............. 13
D Determination of safety integrity levels – A qualitative method: risk graph .. 16
E Determination of safety integrity levels – A qualitative method: hazardous event severity matrix ................................................................. 21
F Bibliography .................................................................................................. 23

Figures

1 Overall framework of this standard ............................................................ 2
A.1 Risk reduction: general concepts ............................................................ 7
A.2 Risk and safety integrity concepts ............................................................ 7
A.3 Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities .......... 9
B.1 Tolerable risk and ALARP ....................................................................... 11
C.1 Safety integrity allocation: example for safety-related protection system 15
D.1 Risk graph: general scheme ..................................................................... 18
D.2 Risk graph: example (illustrates general principles only) ......................... 19
E.1 Hazardous event severity matrix: example (illustrates general principles only) .................................................................................. 22

Tables

B.1 Risk classification of accidents ................................................................. 12
B.2 Interpretation of risk classes ................................................................... 12
D.1 Example data relating to example risk graph (figure D.2) ......................... 20
NATIONAL FOREWORD


The text of IEC Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker, while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, references appear to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards, which are to be substituted in their respective places, are listed below along with their degree of equivalence for the editions indicated:

<table>
<thead>
<tr>
<th>International Standard</th>
<th>Corresponding Indian Standard</th>
<th>Degree of Equivalence</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Standard</td>
<td>Corresponding Indian Standard</td>
<td>Degree of Equivalence</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>

The technical committee has reviewed the provisions of the following International Standard referred in this adopted standard and has decided that it is acceptable for use in conjunction with this standard:

International Standard | Title
--- | ---

Only the English language text in the International Standard has been retained while adopting it in this Indian Standard, and as such the page numbers given here are not the same as in the IEC Standard.

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test, shall be rounded off in accordance with IS 2 : 1960 'Rules for rounding off numerical values (revised)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.
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.
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.


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 IEC 61508-4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its own publications. IEC 61508 is also intended for use as a stand-alone standard.

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.
**PART 1**

Development of the overall safety requirements (concept, scope definition, hazard and risk analysis) (E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities)

7.1 to 7.5

**PART 1**

Allocation of the safety requirements to the E/E/PE safety-related systems

7.6

**PART 2**

Realisation phase for E/E/PE safety-related systems

**PART 3**

Realisation phase for safety-related software

**PART 4**

Overview of techniques and measures

Guidelines for the application of parts 2 and 3

**PART 5**

Risk based approaches to the development of the safety integrity requirements

**PART 6**

Installation and commissioning and safety validation of E/E/PE safety-related systems

7.13 and 7.14

**PART 7**

Operation and maintenance, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems

7.15 to 7.17

---

**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.


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 qualitatively1) or quantitatively2). 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
IS/IEC 61508-5: 1998

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.

### Intolerable region

Risk cannot be justified except in extraordinary circumstances.

**The ALARP or tolerability region**

(Risk is undertaken only if a benefit is desired)

Tolerable only if further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained.

As the risk is reduced, the less proportionately, it is necessary to spend to reduce it further to satisfy ALARP. The concept of diminishing proportion is shown by the triangle.

### Broadly acceptable region

(No need for detailed working to demonstrate ALARP)

It is necessary to maintain assurance that risk remains at this level.

### Negligible risk

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.2. 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.2, 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>
<thead>
<tr>
<th>Frequency</th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Marginal</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>II</td>
</tr>
<tr>
<td>Probable</td>
<td>I</td>
<td>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>III</td>
</tr>
<tr>
<td>Remote</td>
<td>II</td>
<td>III</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Improbable</td>
<td>III</td>
<td>III</td>
<td>IV</td>
<td>IV</td>
</tr>
<tr>
<td>Incredible</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Risk class</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class I</td>
<td>Intolerable risk</td>
</tr>
<tr>
<td>Class II</td>
<td>Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained</td>
</tr>
<tr>
<td>Class III</td>
<td>Tolerable risk if the cost of risk reduction would exceed the improvement gained</td>
</tr>
<tr>
<td>Class IV</td>
<td>Negligible risk</td>
</tr>
</tbody>
</table>
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

\[ PFD_{\text{avg}} \leq \frac{F_t}{F_{np}} \]

where

- \( PFD_{\text{avg}} \) 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 \( PFD_{\text{avg}} \) 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 (\( PFD_{\text{avg}} \)) to meet the necessary risk reduction (\( \Delta R \)). For a constant consequence in the specific situation described, \( PFD_{\text{avg}} = \frac{F_t}{F_{np}} = \Delta R \);
- for \( PFD_{\text{avg}} = \frac{F_t}{F_{np}} \), the safety integrity level can be obtained from table 2 of IEC 61508-1 (for example, for \( PFD_{\text{avg}} = 10^{-2} - 10^{-3} \), 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
Figure D.2 – Risk graph: example (illustrates general principles only)
### Table D.1 – Example data relating to example risk graph (figure D.2)

<table>
<thead>
<tr>
<th>Risk parameter</th>
<th>Classification</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence (C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C₁</td>
<td>Minor injury</td>
<td>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.</td>
</tr>
<tr>
<td>C₂</td>
<td>Serious permanent injury to one or more persons;</td>
<td>2 For the interpretation of C₁, C₂, C₃ and C₄, the consequences of the accident and normal healing shall be taken into account.</td>
</tr>
<tr>
<td>death to one person</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C₃</td>
<td>Death to several people</td>
<td></td>
</tr>
<tr>
<td>C₄</td>
<td>Very many people killed</td>
<td></td>
</tr>
<tr>
<td>Frequency of, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exposure time in,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the hazardous zone (F)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F₁</td>
<td>Rare to more often exposure in the hazardous zone</td>
<td>3 See comment 1 above.</td>
</tr>
<tr>
<td>F₂</td>
<td>Frequent to permanent exposure in the hazardous</td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possibility of avoiding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the hazardous event (P)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P₁</td>
<td>Possible under certain conditions</td>
<td>4 This parameter takes into account - operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised);</td>
</tr>
<tr>
<td>P₂</td>
<td>Almost impossible</td>
<td>- rate of development of the hazardous event (for example suddenly, quickly or slowly);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).</td>
</tr>
<tr>
<td>Probability of the unwanted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>occurrence (W)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>W₁</td>
<td>A very slight probability that the unwanted</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>occurrences will come to pass and only a few</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unwanted occurrences are likely</td>
<td>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.</td>
</tr>
<tr>
<td>W₂</td>
<td>A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely</td>
<td></td>
</tr>
<tr>
<td>W₃</td>
<td>A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely</td>
<td></td>
</tr>
</tbody>
</table>
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.

Number of independent SRSs and external risk reduction facilities [E] (including the E/E/PE SRS being classified)

![Hazardous event severity matrix]

- **Low**, **Medium**, **High**
- **Event likelihood [D]**
- **Event likelihood [D]**
- **Event likelihood [D]**
- **Minor**, **Serious**, **Extensive**

**Number of independent SRSs and external risk reduction facilities [E]**

- **[C]** [C] [C]
- **[C]** [C] SIL 1
- **SIL 1** [SIL 1] SIL 2
- Low, Medium, High

**Event likelihood [D]**

- **[C]** [C] [C]
- **[C]** SIL 1 SIL 2
- **SIL 1** SIL 2 SIL 3 [B]
- Low, Medium, High

**Event likelihood [D]**

- **[C]** SIL 1 SIL 1
- **SIL 1** [SIL 3] SIL 3 [B]
- **SIL 3** SIL 3 SIL 3 [A]
- Low, Medium, High

**Hazardous event severity**

- **Minor**
- **Serious**
- **Extensive**

[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


Bureau of Indian Standards

BIS is a statutory institution established under the Bureau of Indian Standards Act, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of ‘BIS Catalogue’ and ‘Standards: Monthly Additions’.

This Indian Standard has been developed from Doc: No. ETD 18 (5683).

Amendments Issued Since Publication

<table>
<thead>
<tr>
<th>Amendment No.</th>
<th>Date of Issue</th>
<th>Text Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

BUREAU OF INDIAN STANDARDS

Headquarters:
Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110 002
Telephones: 2323 0131, 2323 3375, 2323 9402
Website: www.bis.org.in

Regional Offices:

Central: Manak Bhavan, 9 Bahadur Shah Zafar Marg
NEW DELHI 110 002
Telephones: 2323 7617, 2323 3841

Eastern: 1/14, C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi
KOLKATA 700 054
2337 8499, 2337 8561
2337 8626, 2337 9120

Northern: SCO 335-336, Sector 34-A, CHANDIGARH 160 022
260 3843
260 9285

Southern: C.I.T. Campus, IV Cross Road, CHENNAI 600 113
2254 1216, 2254 1442
2254 2519, 2254 2315

Western: Manakalaya, E9 MIDC, Marol, Andheri (East)
MUMBAI 400 093
2832 9295, 2832 7858
2832 7891, 2832 7892

Branches: AHMEDABAD, BANGALORE, BHOPAL, BHUBANESHWAR, COIMBATORE, FARIDABAD, GHAZIABAD, GUWAHATI, HYDERABAD, JAIPUR, KANPUR, LUCKNOW, NAGPUR, PARWANOO, PATNA, PUNE, RAJKOT, THIRUVANANTHAPURAM, VISAKHAPATNAM.

Printed by the Manager, Govt. of India Press, Faridabad