

Functional safety — Safety instrumented systems for the process industry sector —

Part 3: Guidance for the determination of the required safety integrity levels

The European Standard EN 61511-3:2004 has the status of a
British Standard

ICS 25.040.01

National foreword

This British Standard is the official English language version of EN 61511-3:2004. It was derived by CENELEC from IEC 61511-3:2003, including Corrigendum October 2004.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, Systems considerations, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 52, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments
15578	16 May 2005	Implementation of the European Standard

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2003

© BSI 16 May 2005

ISBN 0 580 41752 2

**Functional safety –
Safety instrumented systems for the process industry sector
Part 3: Guidance for the determination
of the required safety integrity levels
(IEC 61511-3:2003 + corrigendum 2004)**

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité
pour le secteur des industries
de transformation
Partie 3: Conseils pour la détermination
des niveaux d'intégrité de sécurité
(CEI 61511-3:2003)

Funktionale Sicherheit -
Sicherheitstechnische Systeme
für die Prozessindustrie
Teil 3: Anleitung für die Bestimmung
der erforderlichen Sicherheits-
Integritätslevel
(IEC 61511-3:2003 + Corrigendum 2004)

This European Standard was approved by CENELEC on 2004-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of the International Standard IEC 61511-3:2003, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61511-3 on 2004-10-01 without any modification.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2005-10-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2007-10-01

Endorsement notice

The text of the International Standard IEC 61511-3:2003 + corrigendum October 2004 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION	5
1 Scope	8
2 Terms, definitions and abbreviations.....	9
3 Risk and safety integrity – general guidance	9
3.1 General	9
3.2 Necessary risk reduction.....	10
3.3 Role of safety instrumented systems	10
3.4 Safety integrity	10
3.5 Risk and safety integrity	12
3.6 Allocation of safety requirements	13
3.7 Safety integrity levels	13
3.8 Selection of the method for determining the required safety integrity level	14
 Annex A (informative) As Low As Reasonably Practicable (ALARP) and tolerable risk concepts.....	15
Annex B (informative) Semi-quantitative method	18
Annex C (informative) The safety layer matrix method.....	26
Annex D (informative) Determination of the required safety integrity levels – a semi-qualitative method: calibrated risk graph	32
Annex E (informative) Determination of the required safety integrity levels – a qualitative method: risk graph.....	40
Annex F (informative) Layer of protection analysis (LOPA).....	45
 Figure 1 – Overall framework of this standard	7
Figure 2 – Typical risk reduction methods found in process plants	9
Figure 3 – Risk reduction: general concepts	12
Figure 4 – Risk and safety integrity concepts	12
Figure 5 – Allocation of safety requirements to the Safety Instrumented Systems, non-SIS prevention/mitigation protection layers and other protection layers	13
Figure A.1 – Tolerable risk and ALARP	16
Figure B.1 – Pressurized Vessel with Existing Safety Systems.....	19
Figure B.2 – Fault Tree for Overpressure of the Vessel.....	22
Figure B.3 – Hazardous Events with Existing Safety Systems	23
Figure B.4 – Hazardous Events with Redundant Protection Layer	24
Figure B.5 – Hazardous Events with SIL 2 SIS Safety Function.....	25
Figure C.1 – Protection Layers	26
Figure C.2 – Example Safety Layer Matrix.....	30
Figure D.1 – Risk graph: general scheme.....	33
Figure D.2 – Risk Graph: Environmental Loss	38
Figure E.1 – DIN V 19250 Risk graph – personnel protection (see Table E.1)	43
Figure E.2 – Relationship IEC 61511, DIN 19250 and VDI/VDE 2180	44
Figure F.1 – Layer of Protection Analysis (LOPA) Report	46

Table A.1 – Example of risk classification of incidents.....	17
Table A.2 – Interpretation of risk classes.....	17
Table B.1 – HAZOP analysis results.....	20
Table C.1 – Frequency of hazardous event likelihood (without considering PLs)	29
Table C.2 – Criteria for rating the severity of impact of hazardous events	29
Table D.1 – Descriptions of process industry risk graph parameters.....	33
Table D.2 – Example calibration of the general purpose risk graph	36
Table D.3 – General environmental consequences.....	38
Table E.1 – Data relating to risk graph (see Figure E.1)	43
Table F.1 – HAZOP developed data for LOPA.....	46
Table F.2 – Impact event severity levels.....	47
Table F.3 – Typical protection layer (prevention and mitigation) PFDs	47
Table F.4 – Initiation Likelihood.....	48

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels.

This International Standard addresses the application of safety instrumented systems for the Process Industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This International Standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This International Standard addresses safety instrumented systems which are based on the use of Electrical (E)/Electronic (E)/Programmable Electronic (PE) technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of IEC 61508 (see Annex A of IEC 61511-1).

This International Standard sets out an approach for safety lifecycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy be used.

In most situations, safety is best achieved by an inherently safe process design. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy should consider each individual safety instrumented system in the context of the other protective systems. To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This International Standard on safety instrumented systems for the process industry:

- addresses all safety life cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

This standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

This standard deals with guidance in the area of determining the required SIL in hazards and risk analysis (H & RA). The information herein is intended to provide a broad overview of the wide range of global methods used to implement H & RA. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of safety integrity level(s) (SIL) provided in IEC 61511-1 should be reviewed. The annexes in this standard address the following:

- Annex A provides an overview of the concepts of tolerable risk and ALARP.
- Annex B provides an overview of a semi-quantitative method used to determine the required SIL.
- Annex C provides an overview of a safety matrix method to determine the required SIL.
- Annex D provides an overview of a method using a semi-qualitative risk graph approach to determine the required SIL.
- Annex E provides an overview of a method using a qualitative risk graph approach to determine the required SIL.
- Annex F provides an overview of a method using a layer of protection analysis (LOPA) approach to select the required SIL.

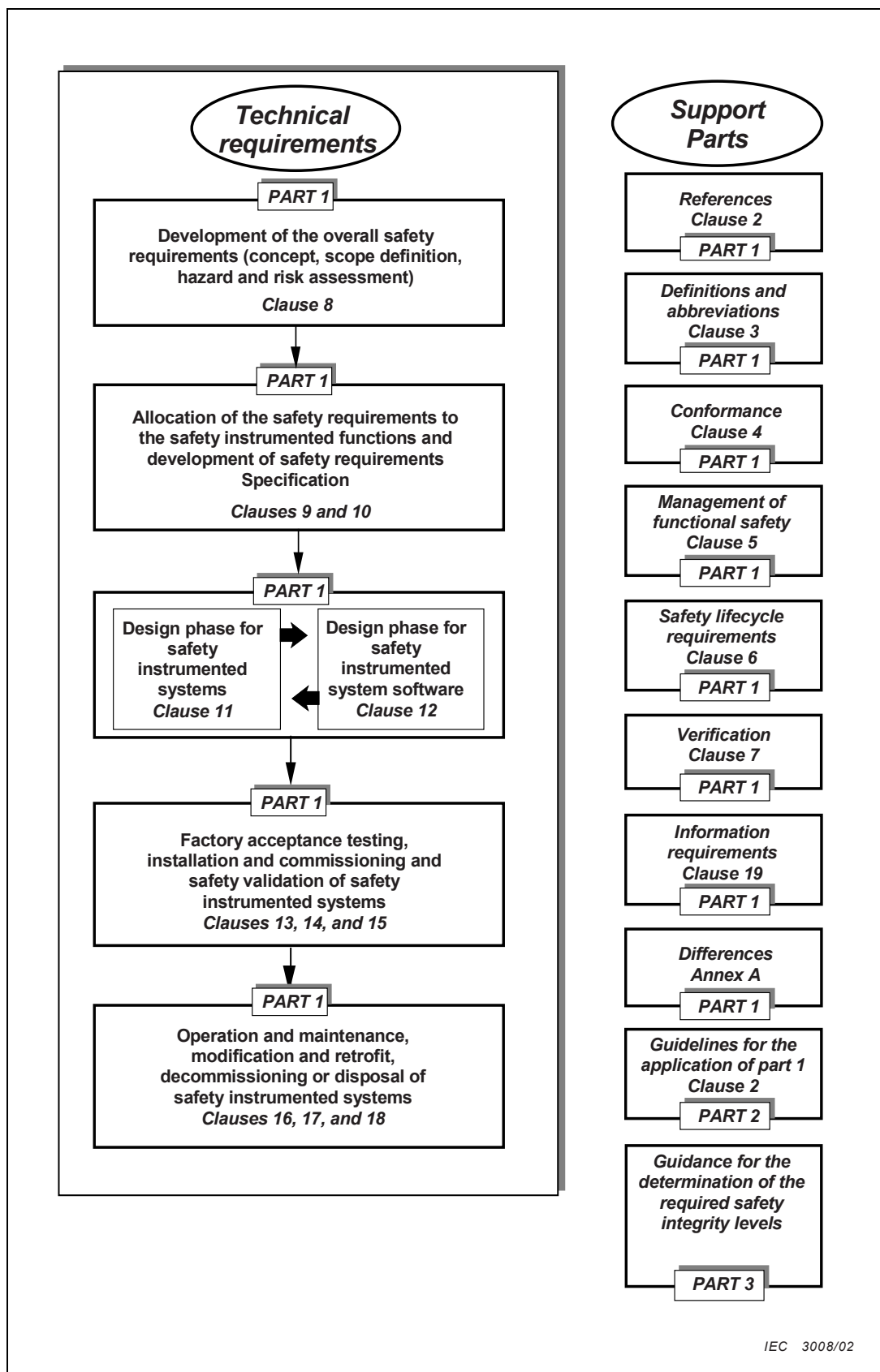


Figure 1 – Overall framework of this standard

FUNCTIONAL SAFETY– SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 3: Guidance for the determination of the required safety integrity levels

1 Scope

1.1 This part provides information on

- the underlying concepts of risk, the relationship of risk to safety integrity, see Clause 3;
- the determination of tolerable risk, see Annex A;
- a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined, see Annexes B, C, D, E, and F.

In particular, this part

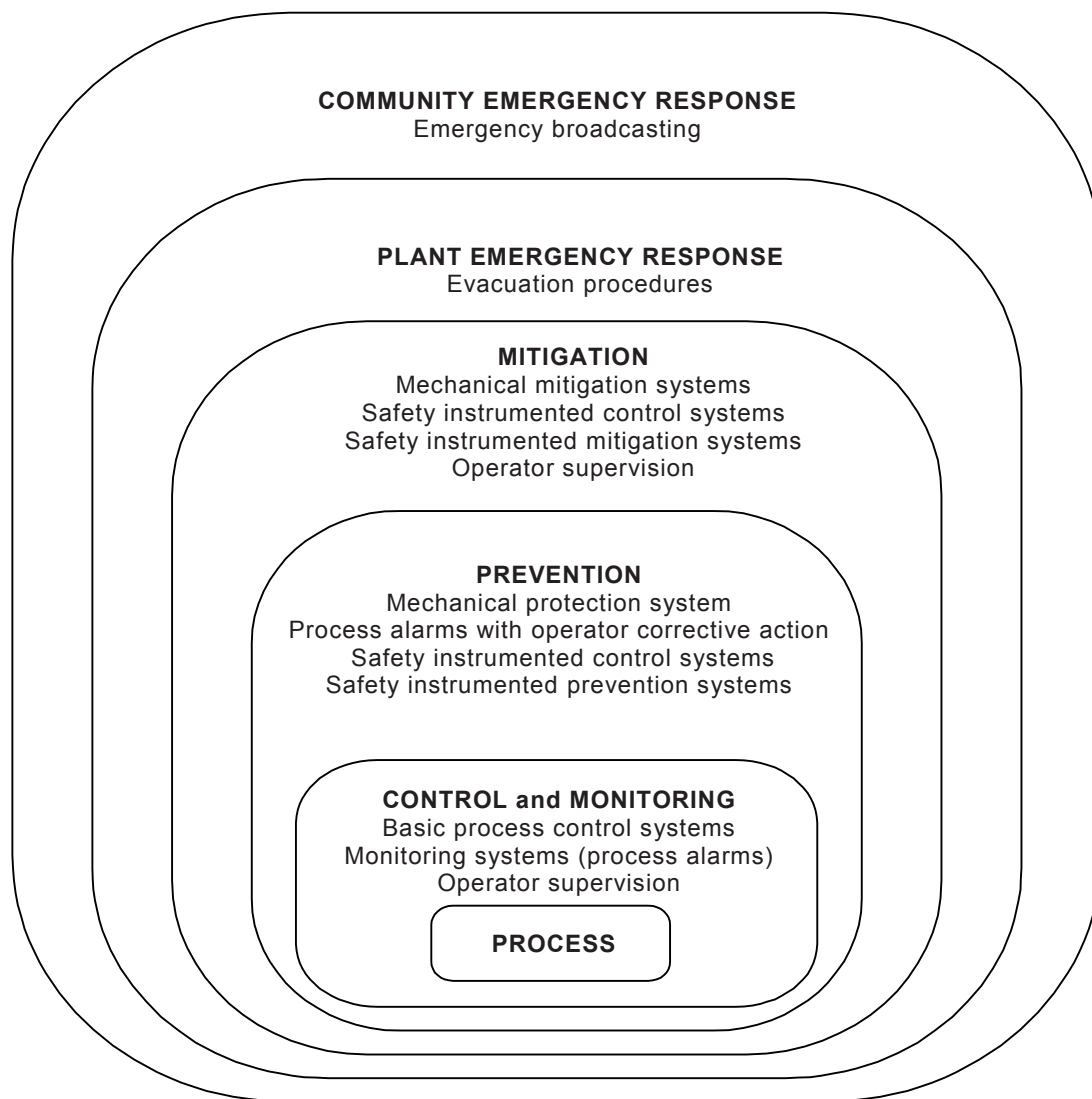
- a) applies when functional safety is achieved using one or more safety instrumented functions for the protection of either personnel, the general public, or the environment;
- b) may be applied in non-safety applications such as asset protection;
- c) illustrates typical hazard and risk assessment methods that may be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;
- d) illustrates techniques/measures available for determining the required safety integrity levels;
- e) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications;
- f) does not give examples of determining the requirements for other methods of risk reduction.

1.2 Annexes B, C, D, E, and F 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.

NOTE Those intending to apply the methods indicated in these annexes should consult the source material referenced in each annex.

1.3 Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that this standard plays in the achievement of functional safety for safety instrumented systems.

Figure 2 gives an overview of risk reduction methods.



IEC 3009/02

**Figure 2 – Typical risk reduction methods found in process plants
(for example, protection layer model)**

2 Terms, definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in Clause 3 of IEC 61511-1 apply.

3 Risk and safety integrity – general guidance

3.1 General

This clause provides information on the underlying concepts of risk and the relationship of risk to safety integrity. This information is common to each of the diverse hazard and risk analysis (H & RA) methods shown herein.

3.2 Necessary risk reduction

The necessary risk reduction (which may be stated either qualitatively¹ or quantitatively²) is the reduction in risk that has to be achieved to meet the tolerable risk (process safety target level) for a specific situation. The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the Safety Instrumented Function (SIF) (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk (process safety target level) for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency of the hazardous event and its specific consequences. Protection layers (see Figure 3) are designed to reduce the frequency of the hazardous event and/or the consequences of the hazardous event.

Important factors in assessing tolerable risk include 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 can be considered. These may include:

- guidelines from the appropriate regulatory authorities;
- discussions and agreements with the different parties involved in the application;
- industry standards and guidelines;
- industry, expert and scientific advice;
- legal and regulatory requirements – both general and those directly relevant to the specific application.

3.3 Role of safety instrumented systems

A safety instrumented system implements the safety instrumented functions required to achieve or to maintain a safe state of the process and, as such, contributes towards the necessary risk reduction to meet the tolerable risk. For example, the safety functions requirements specification may state that when the temperature reaches a value of x , valve y opens to allow water to enter the vessel.

The necessary risk reduction may be achieved by either one or a combination of Safety Instrumented Systems (SIS) or other protection layers.

A person could be an integral part of a safety function. For example, a person could receive information, on the state of the process, and perform a safety action based on this information. If a person is part of a safety function, then all human factors should be considered.

Safety instrumented functions can operate in a demand mode of operation or a continuous mode of operation.

3.4 Safety integrity

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

- a) **Hardware safety integrity** – that part of safety integrity relating to random hardware failures in a dangerous mode of failure. The achievement of the specified level of hardware safety integrity can be estimated to a reasonable level of accuracy, and the requirements can therefore be apportioned between subsystems using the established rules for the combination of probabilities and considering common cause failures. It may be necessary to use redundant architectures to achieve the required hardware safety integrity.

¹ In determining the necessary risk reduction, the tolerable risk needs 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 a hazardous event, leading to a specific consequence, would typically be expressed as a maximum frequency of occurrence per year.

- b) **Systematic safety integrity** – that part of safety integrity relating to systematic failures in a dangerous mode of failure. Although the contribution due to some systematic failures may be estimated, 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 SIS). Therefore a judgement has to be made on the selection of the best techniques to minimize this uncertainty. Note that taking measures to reduce the probability of random hardware failures may not necessarily reduce 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 total risk reduction provided by the safety instrumented function(s) together with any other protection layers has to be such as to ensure that:

- the failure frequency of the safety functions is sufficiently low to prevent the hazardous event frequency from exceeding that required to meet the tolerable risk; and/or
- the safety functions modify the consequences of failure to the extent required to meet the tolerable risk.

Figure 3 illustrates the general concepts of risk reduction. The general model assumes that:

- there is a process and an associated basic process control system (BPCS);
- there are associated human factor issues;
- the safety protection layers features comprise:
 - 1) mechanical protection system;
 - 2) safety instrumented systems;
 - 3) mechanical mitigation system.

NOTE Figure 3 is a generalized risk model to illustrate the general principles. The risk model for a specific application needs to be developed taking into account the specific manner in which the necessary risk reduction is actually being achieved by the Safety Instrumented Systems and/or other protection layers. The resulting risk model may therefore differ from that shown in Figure 3.

The various risks indicated in Figures 3 and 4 are as follows:

- **Process risk** – the risk existing for the specified hazardous events for the process, the basic process control system and associated human factor issues – no designated safety protective features are considered in the determination of this risk;
- **Tolerable risk** (process safety target level) – the risk which is accepted in a given context based on the current values of society;
- **Residual risk** – in the context of this standard, the residual risk is the risk of hazardous events occurring after the addition of protection layers.

The process risk is a function of the risk associated with the process itself but it takes into account the risk reduction brought about by the process control system. To prevent unreasonable claims for the safety integrity of the basic process control system, this standard places constraints on the claims that can be made.

The necessary risk reduction is the minimum level of risk reduction that has to be achieved to meet the tolerable risk. It may be achieved by one or a combination of risk reduction techniques. The necessary risk reduction to achieve the specified tolerable risk, from a starting point of the process risk, is shown in Figure 3.

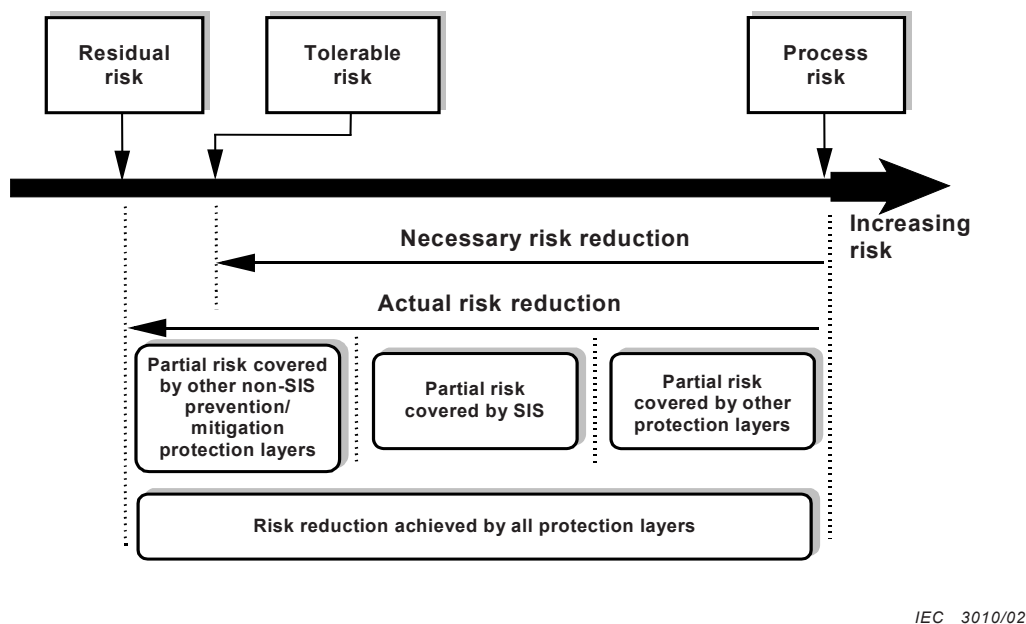


Figure 3 – Risk reduction: general concepts

3.5 Risk and safety integrity

It is important that the distinction between risk and safety integrity is fully appreciated. Risk is a measure of the frequency and consequence of a specified hazardous event occurring. This can be evaluated for different situations (process risk, tolerable risk, residual risk - see Figure 3). The tolerable risk involves consideration of societal and political factors. Safety integrity is a measure of the likelihood that the SIF and other protection layers will achieve the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the SIS can be allocated.

NOTE The allocation may be iterative in order to optimise the design to meet the various requirements.

The role that safety functions play in achieving the necessary risk reduction is illustrated in Figures 3 and 4.

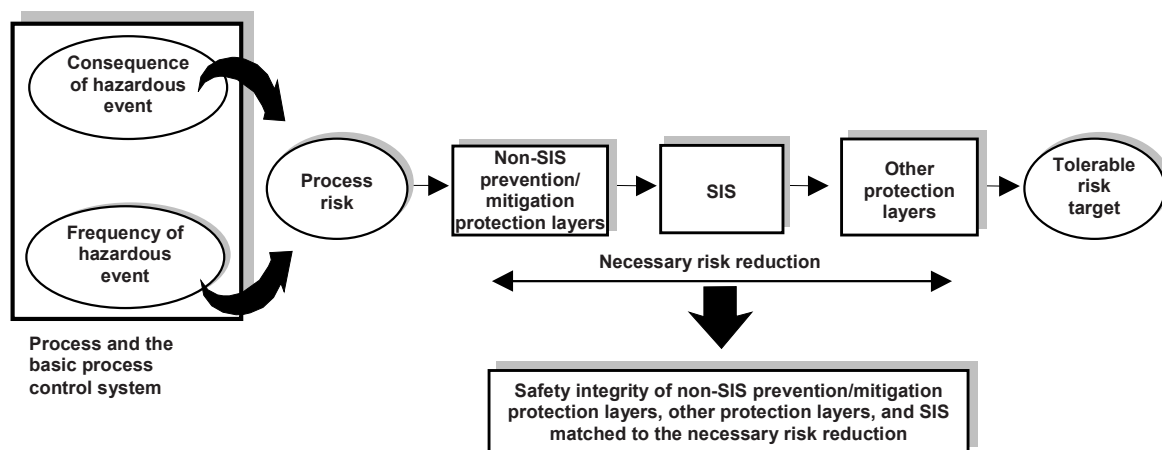


Figure 4 – Risk and safety integrity concepts

3.6 Allocation of safety requirements

The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the safety instrumented systems and other protection layers is shown in Figure 5. The requirements for the safety requirements allocation phase are given in Clause 9 of IEC 61511-1.

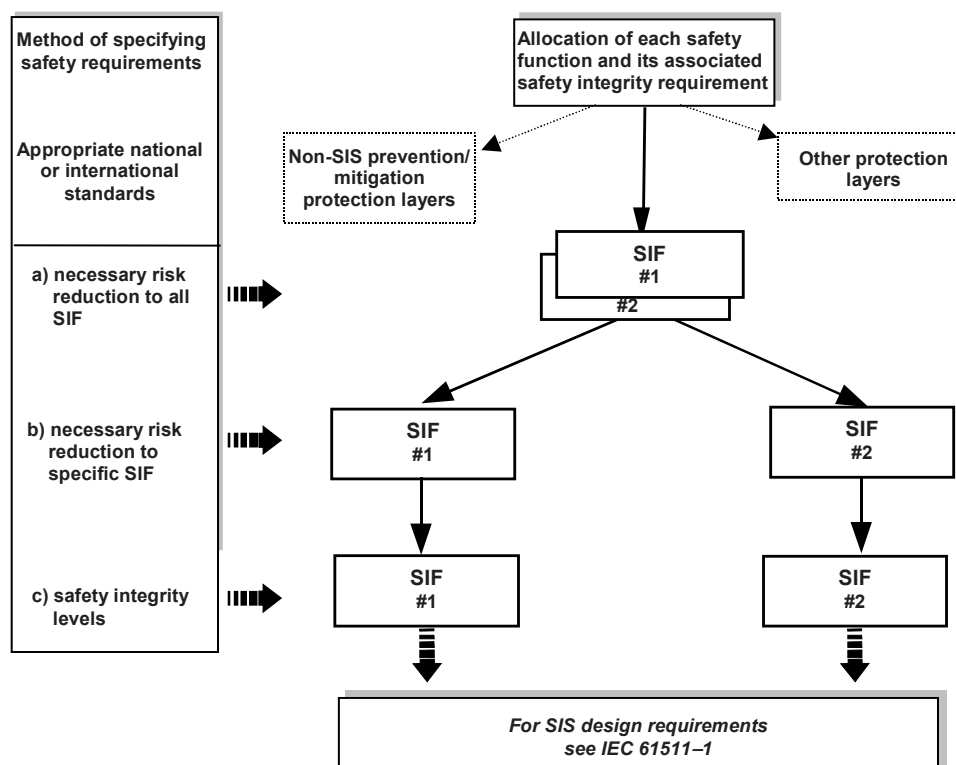
The methods used to allocate the safety integrity requirements to the safety instrumented systems, other technology safety-related systems and external risk reduction facilities depend, primarily, upon whether the necessary risk reduction is specified explicitly in a numerical manner or in a qualitative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

3.7 Safety integrity levels

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 3 and 4 of IEC 61511-1. Two parameters are specified, one for SIS operating in a demand mode of operation and one for SIS operating in a continuous mode of operation.

NOTE For SIS operating in a demand mode of operation, the safety integrity measure of interest is the average probability of failure to perform its designed function on demand. For SIS operating in a continuous mode of operation, the safety integrity measure of interest is the frequency of a dangerous failure per hour, see 3.2.43 of IEC 61511-1.



IEC 3012/02

NOTE Safety integrity requirements are associated with each safety instrumented function before allocation (see IEC 61511-1, Clause 9).

Figure 5 – Allocation of safety requirements to the safety instrumented systems, non-SIS prevention/mitigation protection layers and other protection layers

3.8 Selection of the method for determining the required safety integrity level

There are a number of ways of establishing the required safety integrity level for a specific application. Annexes B to F present information on a number of methods that have been used. The method selected for a specific application will depend on many factors, including:

- the complexity of the application;
- the guidelines from regulatory authorities;
- the nature of the risk and the required risk reduction;
- the experience and skills of the persons available to undertake the work;
- the information available on the parameters relevant to the risk.

In some applications more than one method may be used. A qualitative method may be used as a first pass to determine the required SIL of all SIFs. Those which are assigned a SIL 3 or 4 by this method should then be considered in greater detail using a quantitative method to gain a more rigorous understanding of their required safety integrity.

Annex A (informative)

As Low As Reasonably Practicable (ALARP) and tolerable risk concepts

A.1 General

This annex considers one particular principle (ALARP) which can be applied during the determination of tolerable risk and safety integrity levels. ALARP is a concept which can be applied during the determination of safety integrity levels. It is not, in itself, a method for determining safety integrity levels. Those intending to apply the principles indicated in this annex should consult the following references:

Reducing Risks, Protecting People, HSE, London, 2001 (ISBN 0 7176 2151 0)

Assessment principles for offshore safety cases, HSE London, 1998 (ref. HSG 181) (ISBN 0 7176 1238 4)

Safety assessment principles for nuclear plants, HSE London, 1992 (ISBN 0 11 882043 5)

Tolerability of risks from nuclear power stations, HMSO, London, 1992 (ISBN 0 11 886368 1)

The use of computers in safety-critical applications, Health and Safety Commission, London, 1998 (ISBN 0 7176 1620 7)

A.2 ALARP model

A.2.1 Introduction

Subclause 3.2 outlines the main criteria that are applied in regulating industrial risks and indicates that the activities involve determining whether:

- a) the risk is so great that it is 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 recommends that risks be reduced “so far as is reasonably practicable,” or to a level which is “As Low As Reasonably Practicable” (ALARP). If a risk falls between the two extremes (that is, 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. According to this approach, a risk is considered to fall into one of 3 regions classified as “unacceptable”, “tolerable” or “broadly acceptable” (see Figure A.1).

Above a certain level, a risk is regarded as unacceptable. Such a risk cannot be justified in any ordinary circumstances. If such a risk exists it should be reduced so that it falls in either the “tolerable” or “broadly acceptable” regions, or the associated hazard has to be eliminated.

Below that level, a risk is considered to be “tolerable” provided that it has been reduced to the point where the benefit gained from further risk reduction is outweighed by the cost of achieving that risk reduction, and provided that generally accepted standards have been applied towards the control of the risk. The higher the risk, the more would be expected to be spent to reduce it. A risk which has been reduced in this way is considered to have been reduced to a level which is as “low as is reasonably practicable” (ALARP).