INTERNATIONAL STANDARD

IEC 61511-3

First edition
2003-03

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

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

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 requis

Reference number
IEC 61511-3:2003(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 61511-3

First edition
2003-03

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

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

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 requis

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XA

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 3: Guidance for the determination of the required 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 specifications, 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 61511-3 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/367/FDIS	65A/370/RVD

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

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

IEC 61511 series has been developed as a process sector implementation of IEC 61508 series.

IEC 61511 consists of the following parts, under the general title *Functional safety – Safety Instrumented Systems for the process industry sector* (see Figure 1):

Part 1: Framework, definitions, system, hardware and software requirements

Part 2: Guidelines for the application of IEC 61511-1

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

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

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

The contents of the corrigendum of October 2004 have been included in this copy.

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.

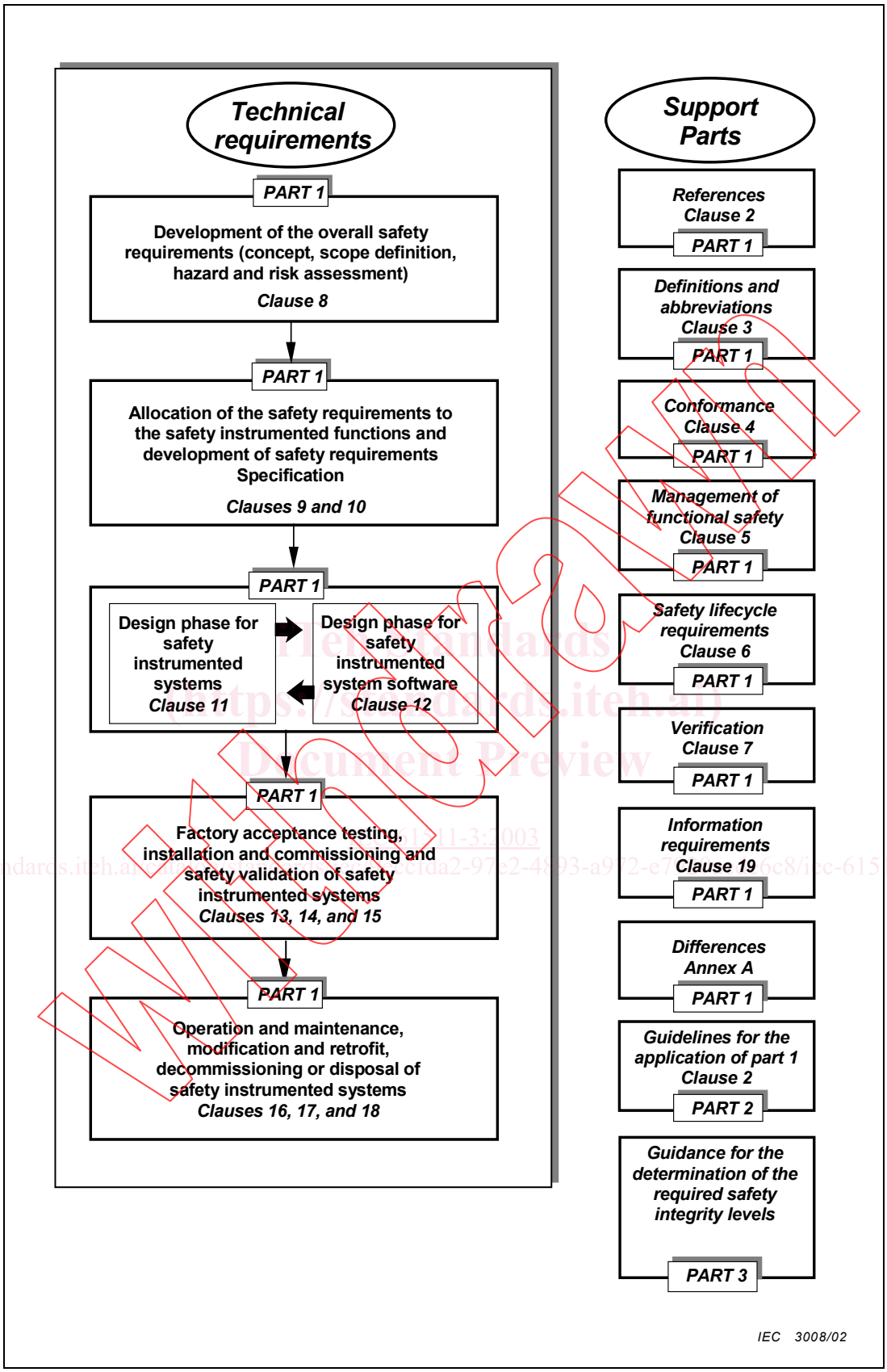

Figure 1 – Overall framework of this standard

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.

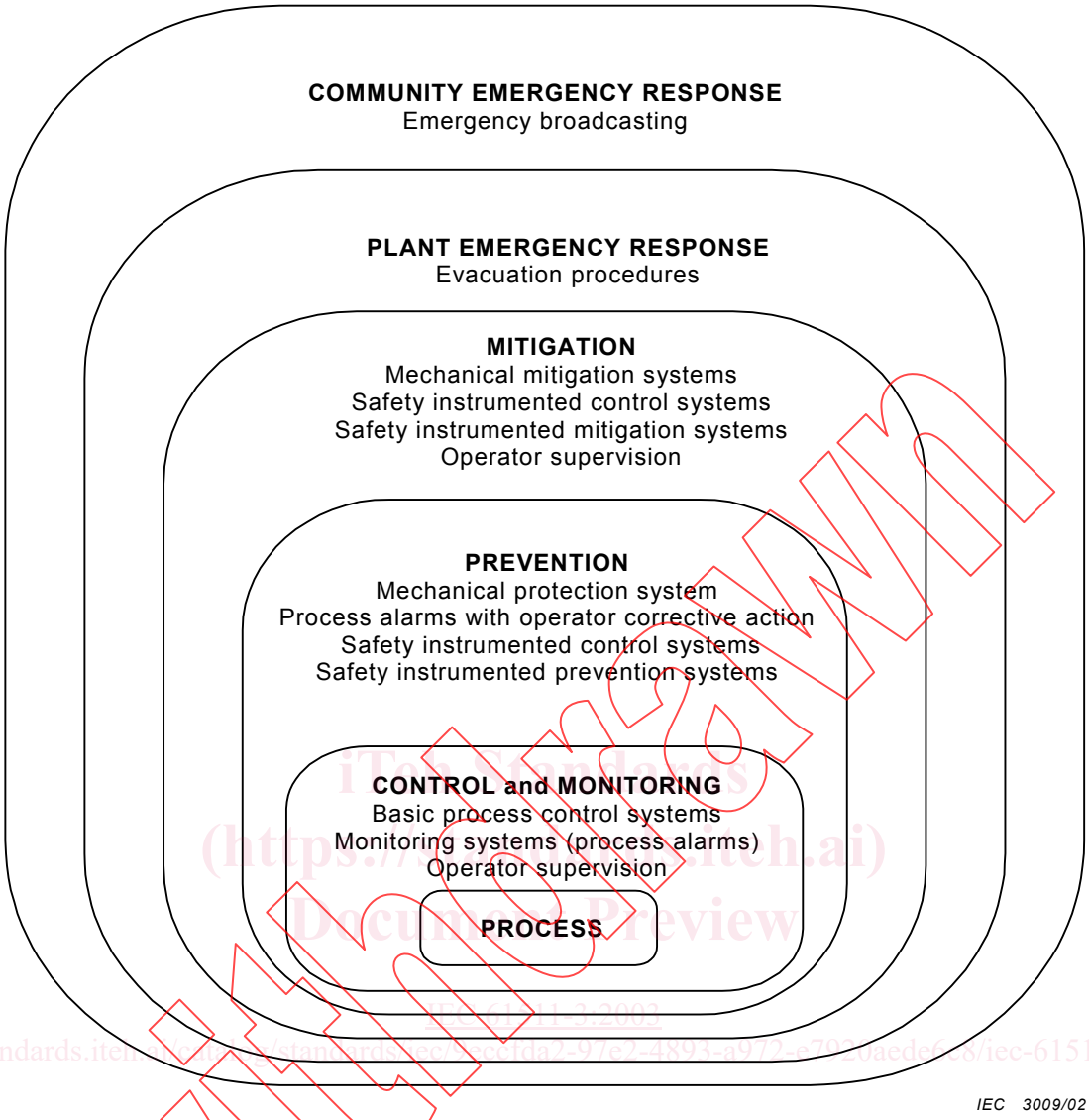

Figure 2 – Typical risk reduction methods found in process plants (for example, protection layer model)

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 qualitatively[1] or quantitatively[2]) 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.