BRITISH STANDARD

BS IEC
61511-3:2003

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

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

ICS 25.040.01

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW
COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

National foreword

This British Standard reproduces verbatim IEC 61511-3:2003 and implements it as the UK national standard.

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 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.

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

Summary of pages

This document comprises a front cover, an inside front cover, the IEC title page, pages 2 to 53 and a back cover.

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

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 30 April 2003

ISBN 0 580 41752 2

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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)

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

CONTENTS

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

--`,,,`,,,,``,,,,``,,,,,,,,,,-`-`,,`,,`,`,,`---

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

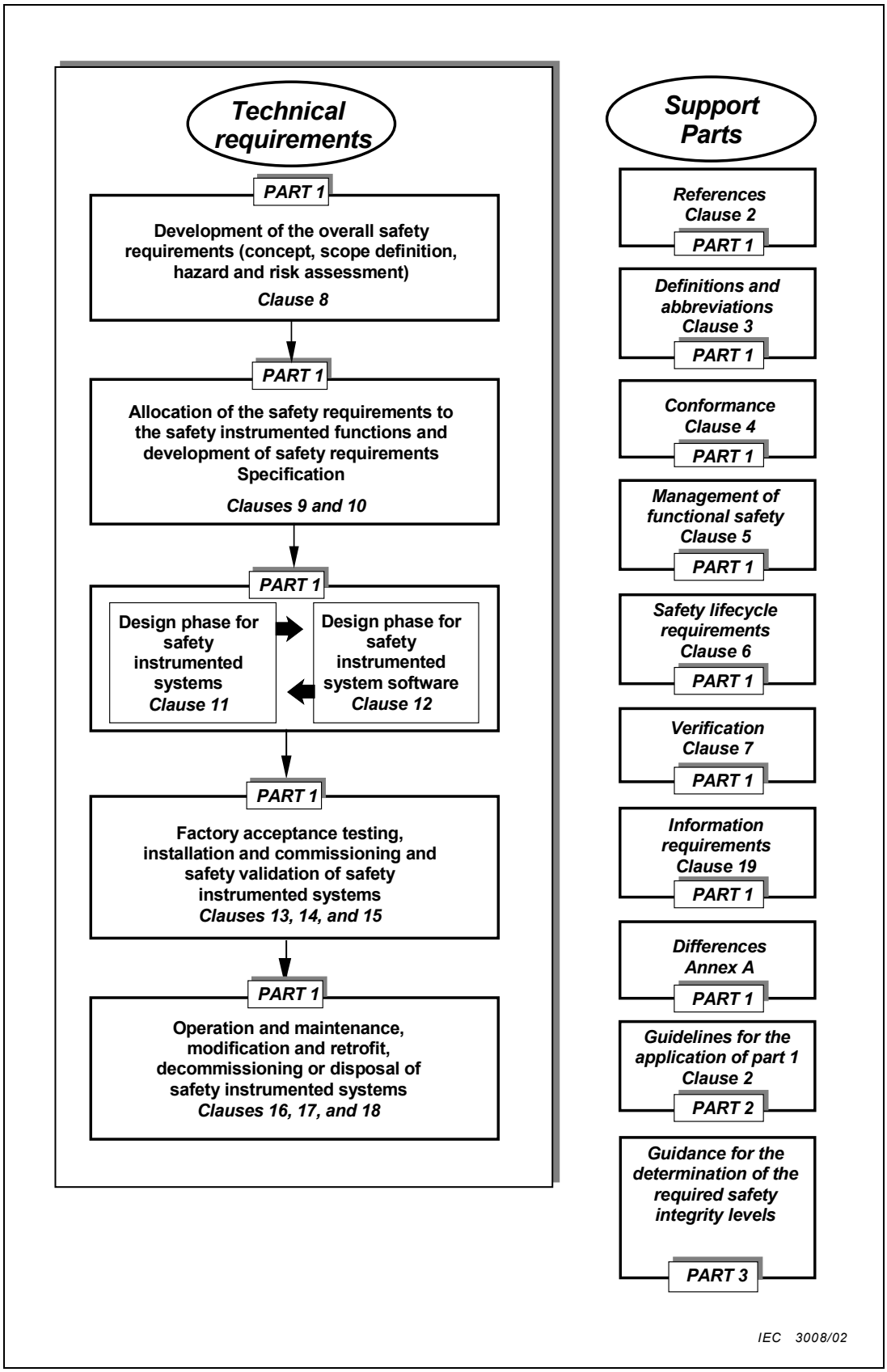


Figure 1 – Overall framework of this standard

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

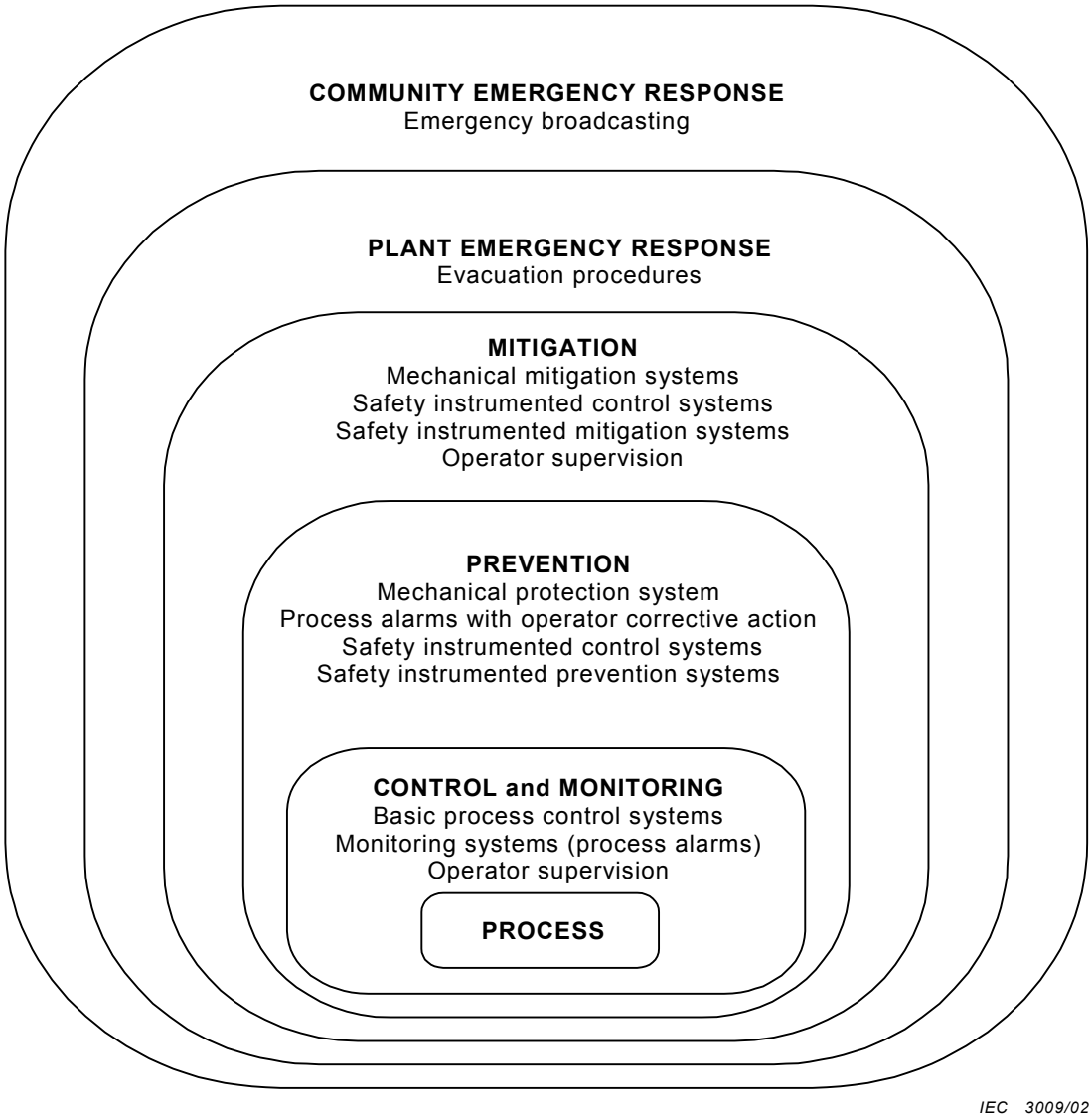


Figure 2 – Typical risk reduction methods found in process plants (for example, protection layer model)

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

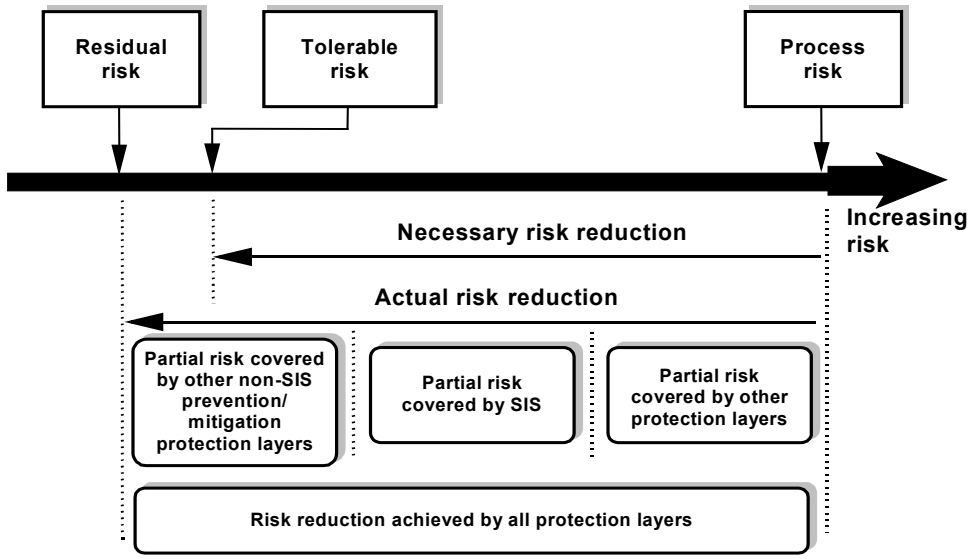


Figure 3 – Risk reduction: general concepts

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.

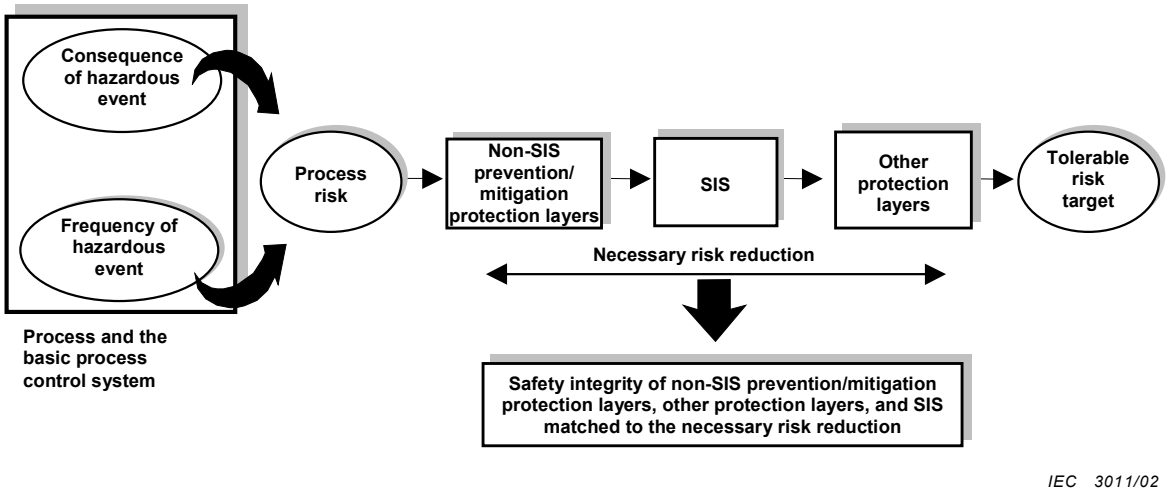


Figure 4 – Risk and safety integrity concepts

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

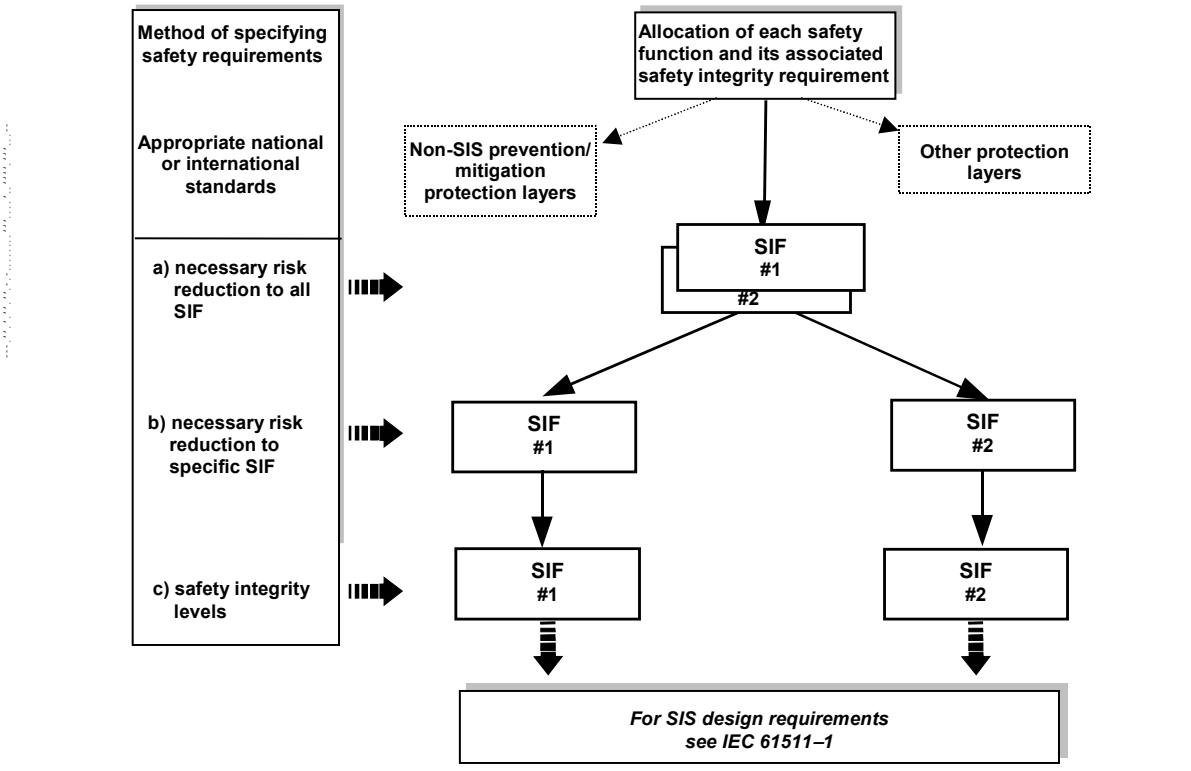
The methods used to allocate the safety integrity requirements to the safety instrumented systems, other technology safety-related systems and external risk reduction facilities depend, primarily, upon whether the necessary risk reduction is specified explicitly in a numerical manner or in a qualitative 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.



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

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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).

--`,,`,,,,`-`-`,,`,,`,`,,`---

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Below the tolerable 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; however, it is necessary to remain vigilant to ensure that the risk remains at this level.

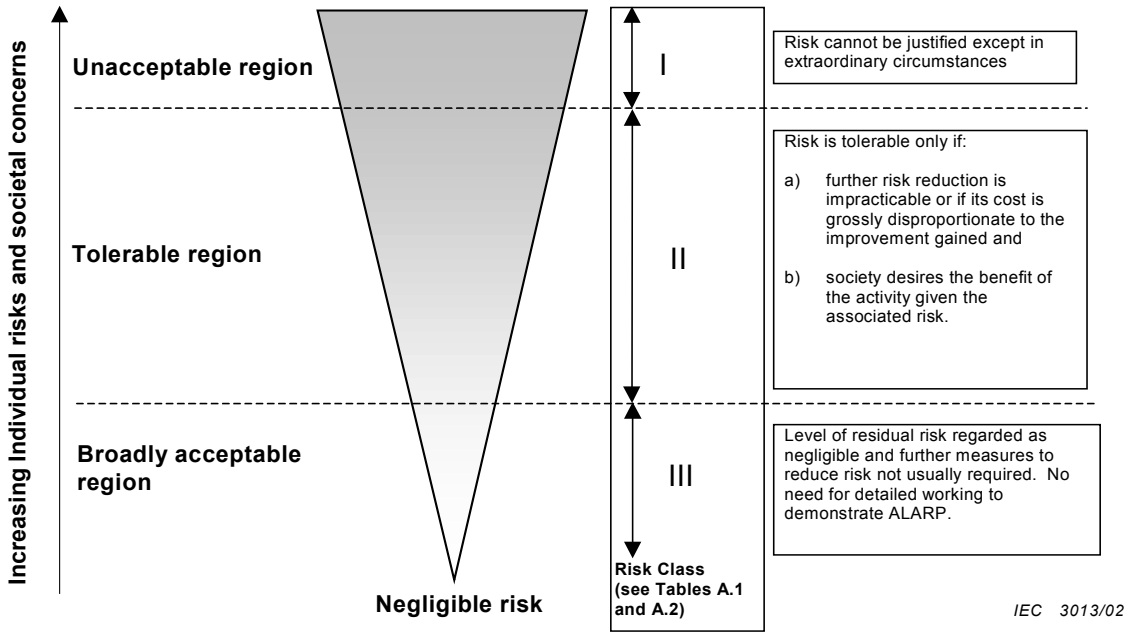


Figure A.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Subclause A.2.2 outlines a method for quantitative risk targets. (Annex C outlines a semi-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).

When using the ALARP principle, care should be taken to ensure that all assumptions are justified and documented.

A.2.2 Tolerable risk target

In order to apply the ALARP principle, it is necessary to define the 3 regions of Figure A.1 in terms of the probability and consequence of an incident . This definition 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 A.1 is an example showing three risk classes (I, II, III) for a number of consequences and frequencies. Table A.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 A.1. The risks within these risk class definitions are the risks that are present when risk reduction measures have been put in place. With respect to Figure A.1, the risk classes are as follows:

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

– risk class I is in the unacceptable region;
– risk class II is in the ALARP region;
– risk class III is in the broadly acceptable region.

For each specific situation, or industry sub-sectors, a table similar to Table A.1 would be developed taking into account a wide range of social, political and economic factors. Each consequence would be matched against a probability and the table populated by the risk classes. For example, likely in Table A.1 could denote an event that is likely to be experienced at a frequency greater than 10 per year. A critical consequence could be a single death and/or multiple severe injuries or severe occupational illness.

Having determined the tolerable risk target, it is then possible to determine the safety integrity levels of safety instrumented functions using, for example, one of the methods outlined in Annexes C to F.

Table A.1 – Example of risk classification of incidents

Probability	Risk class			
	Catastrophic consequence	Critical consequence	Marginal consequence	Negligible consequence
Likely	I	I	I	II
Probable	I	I	II	II
Possible	I	II	II	II
Remote	II	II	II	III
Improbable	II	III	III	III
Incredible	II	III	III	III
NOTE 1 See Table A.2 for interpretation or risk classes I to III. NOTE 2 The actual population of this table with risk classes I, II and III will be application dependent and also depends upon what the actual probabilities are for likely, 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.				

Table A.2 – Interpretation of risk classes

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Negligible risk
NOTE There is no relationship between risk class and safety integrity level (SIL). SIL is determined by the risk reduction associated with a particular safety instrumented function, see Annexes B to F.	

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Annex B
(informative)

Semi-quantitative method

B.1 General

This annex outlines how the safety integrity levels can be determined if a semi-quantitative approach is adopted. A semi-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 1 in 100 years).

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is based on a method described in more detail in the following reference:

CONTINI, S., *Benchmark Exercise on Major Hazard Analysis*, Commission of European Communities, 1992.

B.2 Compliance to IEC 61511-1

The overall objective of the annex is to outline a procedure to identify the required safety instrumented functions and establish their SILs. The basic steps required to comply are the following:

1) Establish the safety target (tolerable risk) of the process.
2) Perform a hazard and risk analysis to evaluate existing risk.
3) Identify safety function(s) needed.
4) Allocate safety function(s) to protection layers.
   NOTE Protection layers are independent from each other.
5) Determine if a SIF is required.
6) Determine required SIL of SIF.

Step 1 establishes the safety target of the process. Step 2 focuses on the risk analysis of the process, and Step 3 derives from the risk analysis what safety functions are required and what risk reduction they need to meet the safety target. After allocating these safety functions to protection layers in Step 4, it will become clear whether a safety instrumented function is required (Step 5) and what SIL it will need to meet (Step 6).

This annex proposes the use of a semi-quantitative risk assessment technique to meet the objectives of the IEC 61511 series. A technique is illustrated through a simple example.

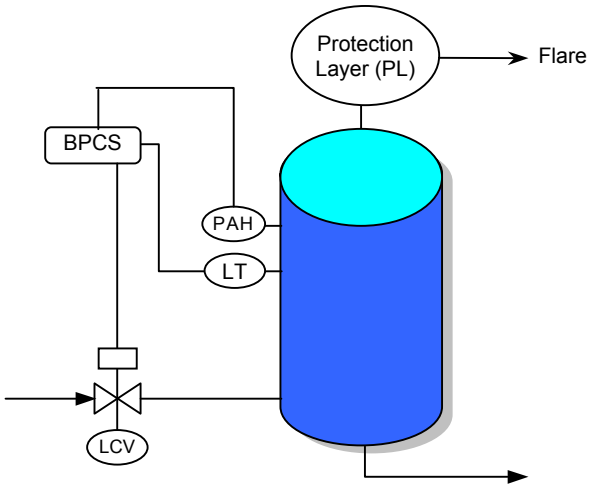
COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

B.3 Example

Consider a process comprised of a pressurized vessel containing volatile flammable liquid with associated instrumentation (see Figure B.1). Control of the process is handled through a Basic Process Control System (BPCS) that monitors the signal from the level transmitter and controls the operation of the valve. The engineered systems available are: a) an independent pressure transmitter to initiate a high pressure alarm and alert the operator to take appropriate action to stop inflow of material; and b) in case the operator fails to respond, a non-instrumented protection layer to address the hazards associated with high vessel pressure. Releases from the protection layer are piped to a knock out tank that relieves the gases to a flare system. It is assumed in this example that the flare system is under proper permit and designed, installed and operating properly; therefore potential failures of the flare system are not considered in this example.

NOTE Engineered systems refer to all systems available to respond to a process demand including other automatic protection layers and operator(s).



Key

PL Protection Layer for additional mitigation (that is, dikes, pressure relief, restricted areas, holding tank)
PAH Pressure Alarm High
LT Level Transmitter
LCV Level Control Valve
BPCS Basic Process Control System

Figure B.1 – Pressurized vessel with existing safety systems

B.3.1 Process safety target level

A fundamental requirement for the successful management of industrial risk is the concise and clear definition of a desired process safety target level (tolerable risk). This may be defined using national and International Standards and regulations, corporate policies, and input from concerned parties such as the community, local jurisdiction and insurance companies supported by good engineering practices. The process safety target level is specific to a process, a corporation or industry. Therefore, it should not be generalized unless existing regulations and standards provide support for such generalisations. For the illustrative example, assume that the process safety target is set as an average release rate of less than 10^{-4} per year based on the expected consequence of a release to environment.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

B.3.2 Hazard analysis

A hazard analysis to identify hazards, potential process deviations and their causes, available engineered systems, initiating events, and potential hazardous events (accidents) that may occur should be performed for the process. This can be accomplished using several qualitative techniques:

– Safety reviews;
– Checklists;
– What if analysis;
– HAZOP studies;
– Failure mode and effects analysis;
– Cause-consequence analysis.

One such technique that is widely applied is a Hazard and Operability (HAZOP study) analysis. The hazard and operability analysis (or study) identifies and evaluates hazards in a process plant, and non-hazardous operability problems that compromise its ability to achieve design productivity.

As a second step, a HAZOP study is performed for the illustrative example shown in Figure B.1. The objective of this HAZOP study analysis is to evaluate hazardous events that have the potential to release the material to the environment. An abridged list is shown in Table B.1 to illustrate the HAZOP results.

The results of the HAZOP study identified that an overpressure condition could result in a release of the flammable material to the environment. This is an initiating event that could propagate into a hazardous event scenario depending on the response of the available engineered systems. If a complete HAZOP was conducted for the process, other initiating events that could lead to a release to the environment may include leaks from process equipment, full bore rupture of piping, and external events such as a fire. For this illustrative example, the overpressure condition is examined.

Table B.1 – HAZOP study results

Item	Deviation	Causes	Consequences	Safeguards	Action
Vessel	**High level**	**Failure of BPCS**	**High pressure**	**Operator**	
	High pressure	1) High level, 2) External fire	Release to environment	1) Alarm, operator, protection layer 2) Deluge system	Evaluate conditions for release to environment
	Low/no flow	Failure of BPCS	No consequence of interest		
	Reverse flow		No consequence of interest		

B.3.3 Semi-quantitative risk analysis technique

An estimate of the process risk is accomplished through a semi-quantitative risk analysis that identifies and quantifies the risks associated with potential process accidents or hazardous events. The results can be used to identify necessary safety functions and their associated SIL in order to reduce the process risk to an acceptable level. The assessment of process risk using semi-quantitative techniques can be distinguished in the following major steps. The first four steps can be performed during the HAZOP study.

1) Identify process hazards.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2) Identify safety layer composition.

NOTE 1 Safety layers comprise all the safety systems available to safeguard a process and it includes SISs, safety related systems of other technologies, external risk reduction facilities, and operator response.

NOTE 2 Step 2 applies since this is an existing process as given in the example.

3) Identify initiating events.
4) Develop hazardous event scenarios for every initiating event.
5) Ascertain the frequency of occurrence of the initiating events and the reliability of existing safety systems using historical data or modelling techniques (Fault Tree Analysis, Markov Modelling).
6) Quantify the frequency of occurrence of significant hazardous events.
7) Evaluate the consequences of all significant hazardous events.
8) Integrate the results (consequence and frequency of an accident) into risk associated with each hazardous event.

The significant outcomes of interest are:

– a better and more detailed understanding of hazards and risks associated with the process;
– knowledge of the process risk;
– the contribution of existing safety systems to the overall risk reduction;
– the identification of each safety function needed to reduce process risk to an acceptable level;
– a comparison of estimated process risk with the target risk.

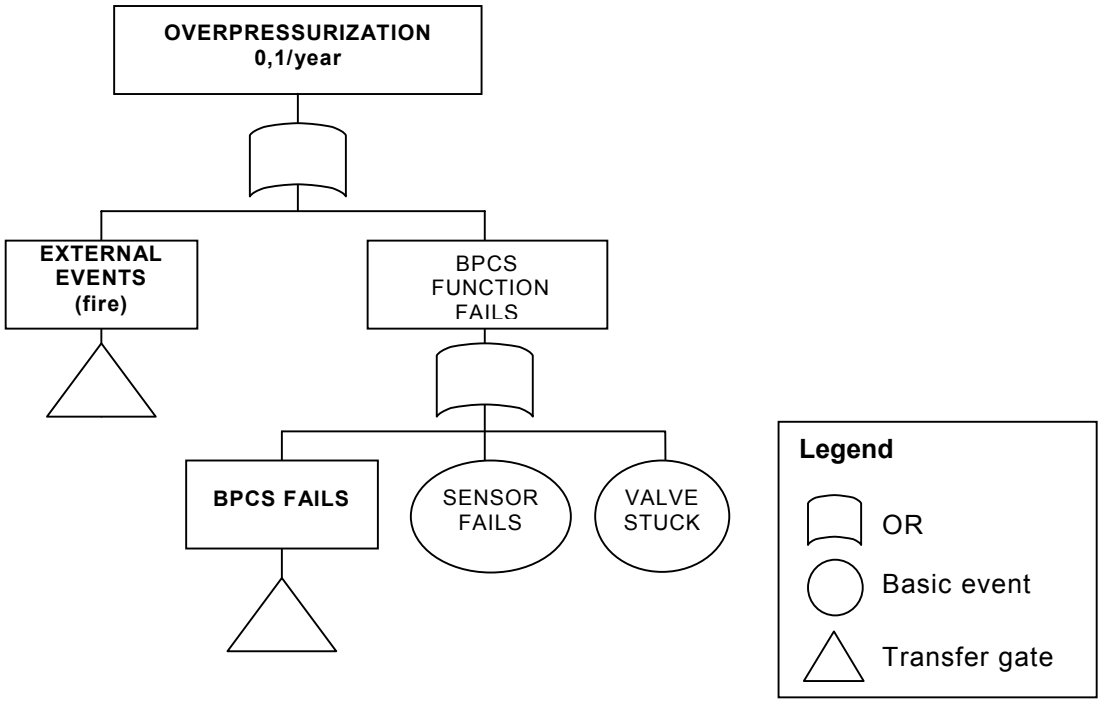
The semi-quantitative technique is resource intensive but does provide benefits that are not inherent in the qualitative approaches. The technique relies heavily on the expertise of a team to identify hazards, provides an explicit method to handle existing safety systems of other technologies, uses a framework to document all activities that have lead to the stated outcome and provides a system for lifecycle management.

For the illustrative example, one initiating event – overpressurization – was identified through the HAZOP study to have the potential to release material to the environment. It should be noted that the approach used in this section is a combination of a quantitative assessment of the frequency of the hazardous event to occur and a qualitative evaluation of the consequences. This approach is used to illustrate the systematic procedure that should be followed to identify hazardous events and safety instrumented functions.

B.3.4 Risk analysis of existing process

The next step is to identify factors that may contribute to the development of the initiating event. In Figure B.2, a simple fault tree is shown that identifies some events that contribute to the development of an overpressure condition in the vessel. The top event, vessel overpressurization, is caused due to the failure of the basic process control system (BPCS), or an external fire (see Table B.1). The fault tree is shown to highlight the impact of the failure of the BPCS on the process. The BPCS does not perform any safety functions. Its failure, however, contributes to the increase in demand for the SIS to operate. Therefore, a reliable BPCS would create a smaller demand on the SIS to operate. The fault tree can be quantified, and for this example the frequency of the overpressure condition is assumed to be in the order of 10^{-1} in one year.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



IEC 3015/02

Figure B.2 – Fault tree for overpressure of the vessel

Once the frequency of occurrence of the initiating event has been established, the success or failure of the safety systems to respond to the abnormal condition is modelled using event tree analysis. The reliability data for the performance of the safety systems can be taken from field data, published databases or predicted using reliability modelling techniques. For this example, the reliability data were assumed and should not be considered as representing published and/or predicted system performance. Figure B.2 shows the potential release scenarios that could be developed given an overpressure condition. The results of the accident modelling are: a) the frequency of occurrence of each accident sequence; and b) the qualitative consequences in terms of release of flammable material. In Figure B.3, five hazardous events are identified, each with a frequency of occurrence and a consequence in terms of potential releases. Accident scenario 1, no release, is the designed condition of the process. Furthermore, hazardous events 2 and 4 release material to the flare and are also considered as designed conditions of the process. The remainder scenarios, that is, 3 and 5, range from a frequency of occurrence in the order of 9×10^{-4} to about 1×10^{-3} per year and will release material to the environment.

NOTE Each event in Figure B.3 is assumed to be independent. Furthermore, the data shown is approximate; therefore, the sum of the frequencies of all accidents approaches the frequency of the initiating event (0,1 per year).

It should be noted that this analysis does not take into account the possibility of common cause failure of the high pressure alarm and the failure of the BPCS level sensor. Such common cause failure could lead to a significant increase in the probability of failure on demand of the alarm system and hence the overall risk. For further information consult *A process industry view of IEC 61508*, Dr A.G.King, IEE Computing and Control Engineering Journal, February 2000, Institution of Electrical Engineers, London, 2000.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

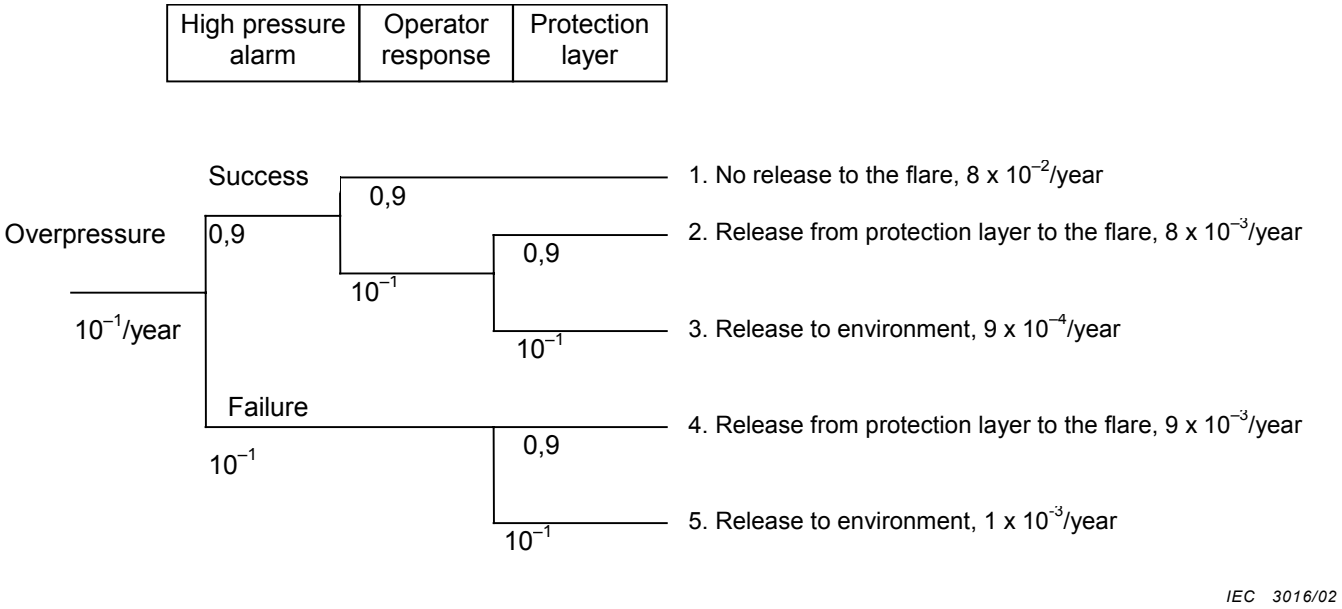


Figure B.3 – Hazardous events with existing safety systems

B.3.5 Events that do not meet the safety target level

As was stated earlier, plant specific guidelines establish the safety target level as: no release of material to the environment with a frequency of occurrence greater than 10^{-4} in one year. Given the frequency of occurrence of the hazardous events and consequence data in Figure B.3, risk reduction is necessary in order for accidents 3 and 5 to be below the safety target level.

B.3.6 Risk reduction using other protection layers

Protection layers of other technologies should be considered prior to establishing the need for a safety instrumented function implemented in a SIS. To illustrate the procedure, assume that an additional completely independent, protection layer is introduced to augment the existing safety systems. Figure B.4 shows the process with the new protection layer. Event tree analysis is employed to develop all the potential hazardous events. From Figure B.4, it can be seen that seven release accidents may occur, given the same overpressure condition.

Examination of the frequency of occurrence of the modelled hazardous events in Figure B.4 shows that the safety target level for the vessel has not been met because hazardous events 4 and 7 release material to the environment and are still at or above the safety target. In fact, the total frequency of a release to the environment is 1,9 × 10^{-4} per year. At this point the feasibility of using external risk reduction facilities should be evaluated. Given that the safety target is to minimise the risk due to a release of material to the environment, it can be assumed that external risk reduction facilities such as a dyke (bund) is not a feasible alternative risk reduction scheme. Therefore, since no other non-SIS protection can meet the safety target level, a safety instrumented function implemented in a SIS is required to protect against an overpressure and the release of the flammable material.

--`,,`,,`,,,,``,`,,`,,,`````-`-`,,`,,`,`,,`---
COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

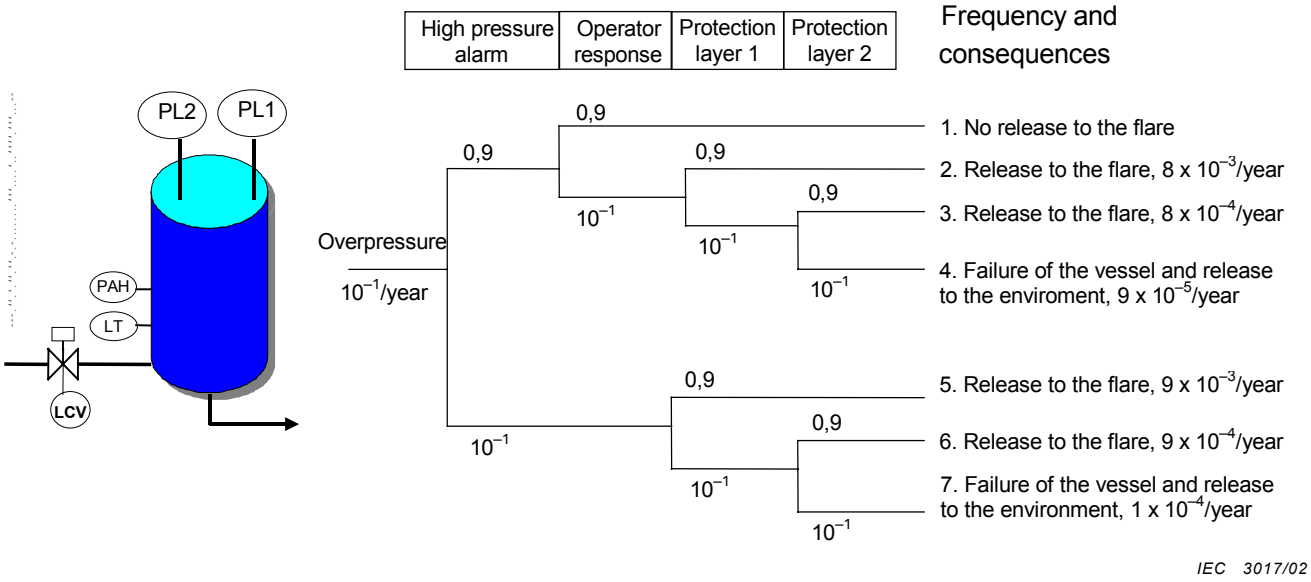


Figure B.4 – Hazardous events with redundant protection layer

B.3.7 Risk reduction using a safety instrumented function

The safety target cannot be achieved using protection layers of other technologies or external risk reduction facilities. Release scenario 7 is still at the safety target. In fact, the total frequency of releases to the environment from Figure B.4 is $1,9 \times 10^{-4}$ in a year (sum of the frequencies of scenarios 4 and 7). In order to reduce the overall frequency of releases to the atmosphere, a new SIL 2 safety instrumented function implemented in a SIS is required to meet the safety target level. The new safety instrumented function is shown in Figure B.5. It is not necessary at this point to perform a detail design on the safety instrumented function. A general SIF design concept is sufficient. The goal in this step is to determine if a SIL 2 SIF will provide the required risk reduction and allow the achievement of the safety target level Detail design of the SIF will occur after the safety target level has been achieved. For example, the new safety instrumented function can use dual, safety dedicated, pressure sensors in a 1oo2 configuration sending signals to a logic solver. The output of the logic solver controls one additional shutdown valve.

NOTE 1oo2 means that either one of the pressure sensors can send a signal to shut down the process.

The new SIL 2 safety instrumented function is used to minimize the frequency of a release from the pressurized vessel due to an overpressure. Figure B.5 presents the new safety layer and provides all the potential accident scenarios. As can be seen from this figure, the frequency of any release from this vessel can be reduced to 10^{-4} per year or lower and the safety target level can be met provided the safety instrumented function can be evaluated to be consistent with SIL 2 requirements. The total frequency or releases to the environment (sum of frequencies of scenarios 4 and 7) has been reduced to $1,9 \times 10^{-5}$ per year, below the safety target of 10^{-4} per year.

It should be noted that this event tree analysis does not take into account the possibility of common cause failure of the high pressure alarm and the SIL 2 safety Instrumented function. There may also be potential for common cause failure between both of these protective arrangements and the failure of the BPCS level sensor.

Such common cause failures lead to a highly significant increase in the probability of failure on demand of the protective functions and hence to substantial increase in the overall risk. Again, for further information consult *A process industry view of IEC 61508*, Dr A.G.King, IEE Computing and Control Engineering Journal, February 2000, Institution of Electrical Engineers, London, 2000.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

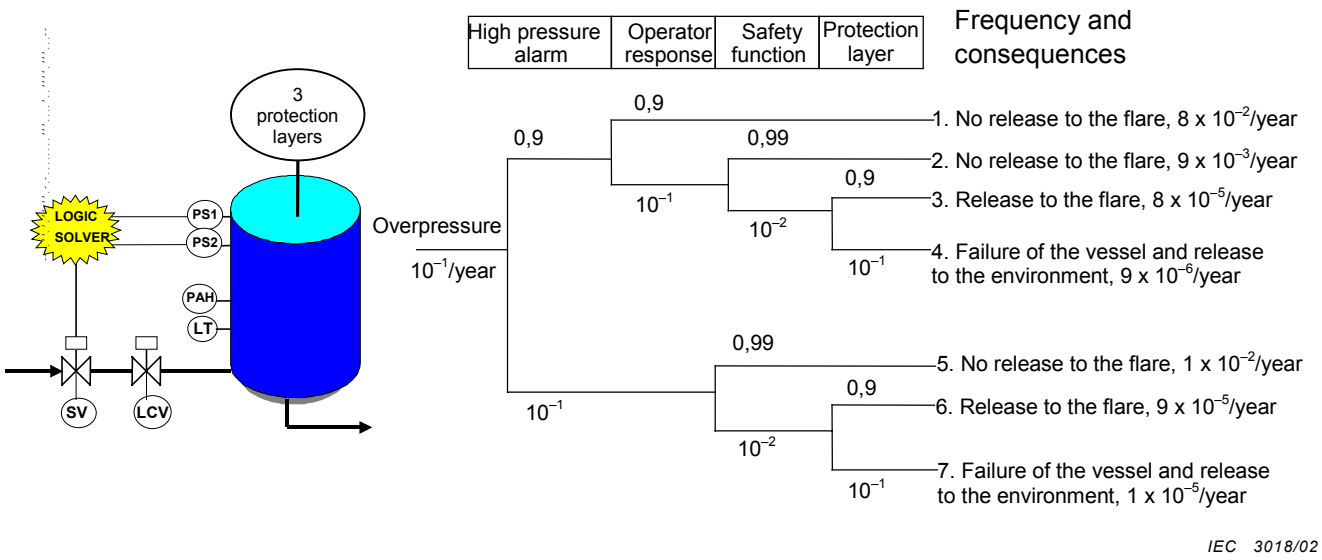


Figure B.5 – Hazardous events with SIL 2 SIS safety function

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Annex C
(informative)

The safety layer matrix method

C.1 Introduction

Within each process, risk reduction should begin with the most fundamental elements of process design: selection of the process itself, the choice of the site, and decisions about hazardous inventories and plant layout. Maintaining minimum inventories of hazardous chemicals; installing piping and heat exchange systems that physically prevent the inadvertent mixing of reactive chemicals; selecting heavy-walled vessels that can withstand the maximum possible process pressures; and selecting a heating medium with maximum temperature less than the decomposition temperatures of process chemicals are all process design decisions that reduce operational risks. Such focus on risk reduction by careful selection of the process design and operating parameters is a key step in the design of a safe process. A further search for ways to eliminate hazards and to apply inherently safe design practices in the process development activity is recommended. Unfortunately, even after this design philosophy has been applied to the fullest extent, potential hazards may still exist and additional protective measures should be applied.

In the process industries, the application of multiple protection layers to safeguard a process is used, as illustrated in Figure C.1. In this figure, each protection layer consists of equipment and/or administrative controls that function in concert with other protection layers to control and/or mitigate process risk.

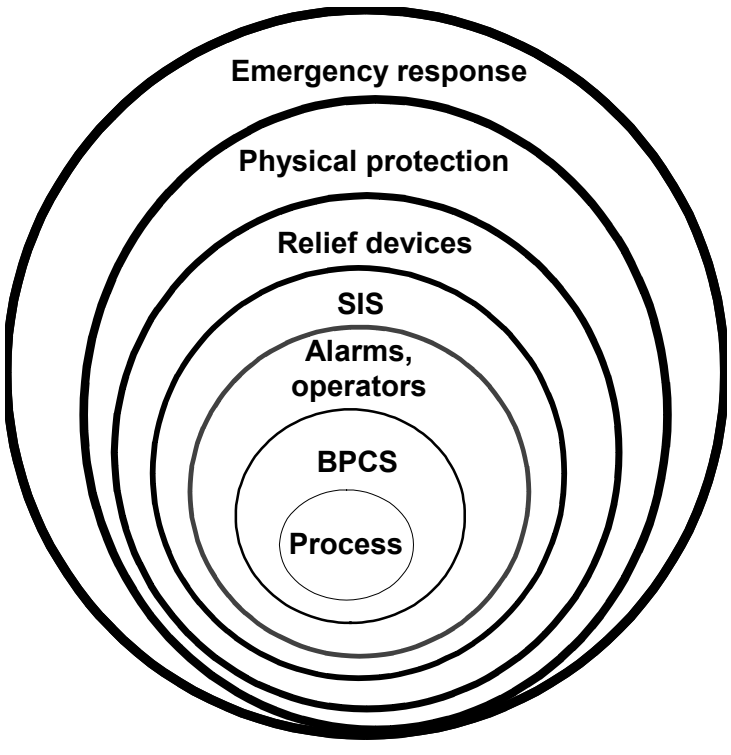


Figure C.1 – Protection layers

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003
07:19:03 MDT Questions or comments about this message: please call the Document
Policy Management Group at 1-800-451-1584.

The concept of protection layers relies on three basic concepts:

1) A protection layer consists of a grouping of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate process risk.
2) A Protection Layer (PL) meets the following criteria:
   – Reduces the identified risk by at least a factor of 10.
   – Has the following important characteristics:
     - **Specificity** – a PL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL;
     - **Independence** – a PL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed PL;
     - **Dependability** – the PL can be counted on to do what it was designed to do by addressing both random failures and systematic failures during its design;
     - **Auditability** – a PL is designed to facilitate regular validation of the protective functions.
3) Safety instrumented function protection layer is a protection layer that meets the definition of a safety instrumented system in this annex. ("SIS" was used when safety layer matrix was developed).

References:

– *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1.
– ISA-S91.01-1995, *Identification of Emergency Shutdown Systems and Controls That are Critical to Maintaining Safety in Process Industries*, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA.
– *Safety Shutdown Systems: Design, Analysis and Justification*, Gruhn and Cheddie, 1998, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA, ISBN 1-55617-665-1.
– FM Global Property Loss Prevention Data Sheet 7-45, "*Instrumentation and Control in Safety Applications*", 1998, FM Global, Johnston, RI, USA.

C.2 Process safety target

A fundamental requirement for the successful management of industrial risk is the concise and clear definition of a desired process safety target that may be defined using national and International Standards and regulations, corporate policies and input from concerned parties such as the community, local jurisdiction and insurance companies supported by good engineering practices. The process safety target level is specific to a process, a corporation or industry. Therefore, it should not be generalized unless existing regulations and standards provide support for such generalizations.

C.3 Hazard analysis

A hazard analysis to identify hazards, potential process deviations and their causes, available engineered systems, initiating events, and potential hazardous events that may occur should be performed for the process. This can be accomplished using several qualitative techniques:

– safety reviews;
– checklists;
– what if analysis;

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

– HAZOP studies;
– failure mode and effects analysis;
– cause-consequence analysis.

One such technique that is widely applied is a Hazard and Operability (HAZOP study) analysis. The Hazard and Operability analysis (or HAZOP study) identifies and evaluates hazards in a process plant, and non-hazardous operability problems that compromise its ability to achieve design productivity.

Although the technique was originally developed for evaluating a new design/application in which industry has little experience, it is also very effective with existing operations. It requires detailed knowledge and understanding of the design, operation and maintenance of a process. Generally, an experienced team leader systematically guides the analysis team through the process design using an appropriate set of “guide” words. Guide words are applied at specific points or study nodes in the process and are combined with specific process parameters to identify potential deviations from the intended operation. Checklists or process experience are also used to help the team develop the necessary list of deviations to be considered in the analysis. The team then agrees on possible causes of process deviations, the consequences of such deviations, and the required procedural and engineered systems. If the causes and consequences are significant and the safeguards are inadequate, the team may recommend an additional safety measure or a follow-up action for management consideration.

Frequently, process experience and the HAZOP study results for a particular process can be generalized so to be applicable for similar processes that exist in a company. If such generalization is possible, then the deployment of the safety layer matrix method is feasible with limited resources.

C.4 Risk analysis technique

After the HAZOP study has been performed, the risk associated with a process can be evaluated using qualitative or quantitative techniques. These techniques rely on the expertise of plant personnel and other hazard and risk analysis specialists to identify potential hazardous events and evaluate the likelihood, consequences and impact.

A qualitative approach can be used to assess process risk. Such an approach allows a traceable path of how the hazardous event develops, and the estimation of the likelihood (approximate range of occurrence) and the severity.

Typical guidance on how to estimate the likelihood of hazardous events to occur, without considering the impact of existing PLs, is provided in Table C.1. The data is generic and may be used where plant or process specific data are not available. However, company specific data, when available, should be employed to establish the likelihood of occurrence of hazardous events.

Similarly, Table C.2 shows one way of converting the severity of the impact of a hazardous event into severity ratings for a relative assessment. Again, these ratings are provided for guidance. The severity of the impact of hazardous events and the rating are developed based on plant specific expertise and experience.

--`,,`,,`,,,,``,`,```,,,`````````-`-`,,`,,`,`,,`---

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Table C.1 – Frequency of hazardous event likelihood (without considering PLs)

Type of events	Likelihood
	Qualitative ranking
Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels.	Low
Events such as dual instrument, valve failures, or major releases in loading /unloading areas.	Medium
Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	High
* The system should be in accordance with this standard when a claim that a control function fails less frequently than 10^{-1} per year is made.	

Table C.2 – Criteria for rating the severity of impact of hazardous events

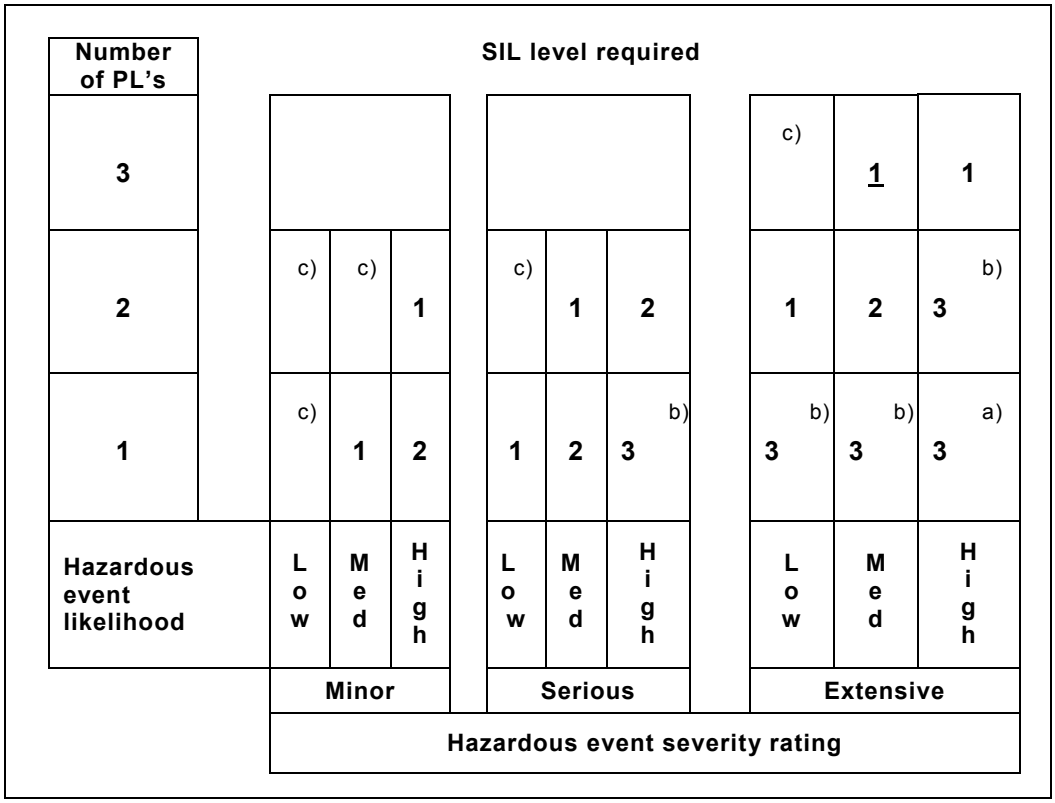
Severity rating	Impact
Extensive	Large scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment.
Serious	Damage to equipment. Short shutdown of the process. Serious injury to personnel and the environment.
Minor	Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment.

C.5 Safety layer matrix

A risk matrix can be used for the evaluation of risk by combining the likelihood and the impact severity rating of hazardous events. A similar approach can be used to develop a matrix that identifies the potential risk reduction that can be associated with the use of a SIS protection layer. Such a risk matrix is shown in Figure C.2. In Figure C.2, the safety target level has been embedded in the matrix. In other words, the matrix is based on the operating experience and risk criteria of the specific company, the design, operating and protection philosophy of the company, and the level of safety that the company has established as its safety target level.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



a) One level 3 safety instrumented function does not provide sufficient risk reduction at this risk level. Additional modifications are required in order to reduce risk (see d).

b) One level 3 safety instrumented function may not provide sufficient risk reduction at this risk level. Additional review is required (see d).

c) SIS independent protection layer is probably not needed.

d) This approach is not considered suitable for SIL 4.

Figure C.2 – Example safety layer matrix

Total number of PLs – includes all the PLs protecting the process including the SIS being classified.

Hazardous event likelihood – likelihood that the hazardous event occurs without any of the PLs in service. See Table C.1 for guidance.

Hazardous event severity – the impact associated with the hazardous event. See Table C.2 for guidance.

C.6 General procedure

1) Establish the process safety target level.
2) Perform a hazard identification (for example, HAZOP studies) to identify all hazardous events of interest.
3) Establish the hazardous event scenarios and estimate the hazardous event likelihood using company specific guidelines and data.
4) Establish the severity rating of the hazardous events using company specific guidelines.
5) Identify existing PLs. The estimated likelihood of hazardous events should be reduced by a factor of 10 for every PL.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

6) Identify the need for an additional SIS protection layer by comparing the remaining risk with the safety target level.

7) Identify the SIL from Figure C.2.

NOTE The user should assess the possible level of dependency between protection layers and attempt to minimize any such occurrence.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Annex D
(informative)

Determination of the required safety integrity levels – a semi-qualitative method: calibrated risk graph

D.1 Introduction

This annex is based on the general scheme of risk graph implementation described in Clause D.4 of IEC 61508-5. The annex has been adapted to be more suited to the needs of the process industry.

It describes the calibrated risk graph method for determining safety integrity levels of safety instrumented functions. This is a semi-qualitative method that enables the safety integrity level of a safety instrumented function to be determined from a knowledge of the risk factors associated with the process and basic process control system.

The approach uses a number of parameters, which together describe the nature of the hazardous situation when safety instrumented 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 instrumented functions. These parameters:

– allow a graded assessment of the risks to be made, and
– represent key risk assessment factors.

The risk graph approach can also be used to determine the need for risk reduction where the consequences include acute environmental damage or asset loss. The objective of this annex is to provide guidance on the above issues.

This annex starts with protection against personnel hazards. It presents one possibility of applying the general risk graph of Figure D.1 of IEC 61508-5 to the process industries. Finally, risk graph applications to environmental protection and asset protection are given.

D.2 Risk graph synthesis

Risk is defined as a combination of the probability of occurrence of harm and the severity of that harm (see Clause 3 of IEC 61511-1). Typically, in the process sector, risk is a function of the following four parameters:

– the consequence of the hazardous situation (C);
– the occupancy (probability that the exposed area is occupied) (F);
– the probability of avoiding the hazardous situation (P);
– the demand rate (number of times per year that the hazardous situation would occur in the absence of the safety instrumented function being considered) (W).

When a risk graph is used to determine the safety integrity level of a safety function acting in continuous mode, consideration will then need to be given to changing the parameters that are used within the risk graph. The parameters should represent the risk factors that relate best to the application characteristics involved. Consideration will also need to be given to the mapping of safety integrity levels to the outcome of the parameter decisions as some adjustment may be necessary to ensure risk is reduced to tolerable levels. As an example, the parameter W may be redefined as the percentage of the life of the system during which the system is on mission. Thus W1 would be selected where the hazard is not continuously

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

present and the period per year when a failure would lead to hazard is short. In this example, the other parameters would also need to be considered for the decision criteria involved and the integrity level outcomes reviewed to ensure tolerable risk.

Table D.1 – Descriptions of process industry risk graph parameters

Parameter		Description
Consequence	C	Number of fatalities and/or serious injuries likely to result from the occurrence of the hazardous event. Determined by calculating the numbers in the exposed area when the area is occupied taking into account the vulnerability to the hazardous event.
Occupancy	F	Probability that the exposed area is occupied at the time of the hazardous event. Determined by calculating the fraction of time the area is occupied at the time of the hazardous event. This should take into account the possibility of an increased likelihood of persons being in the exposed area in order to investigate abnormal situations which may exist during the build-up to the hazardous event (consider also if this changes the C parameter).
Probability of avoiding the hazard	P	The probability that exposed persons are able to avoid the hazardous situation which exists if the safety instrumented function fails on demand. This depends on there being independent methods of alerting the exposed persons to the hazard prior to the hazard occurring and there being methods of escape.
Demand rate	W	The number of times per year that the hazardous event would occur in the absence of the safety instrumented function under consideration. This can be determined by considering all failures which can lead to the hazardous event and estimating the overall rate of occurrence. Other protection layers should be included in the consideration.

D.3 Calibration

The objectives of the calibration process are as follows:

1) To describe all parameters in such a way as to enable the SIL assessment team to make objective judgements based on the characteristics of the application;
2) To ensure the SIL selected for an application is in accordance with corporate risk criteria and takes into account risks from other sources;
3) To enable the parameter selection process to be verified.

Calibration of the risk graph is the process of assigning numerical values to risk graph parameters. This forms the basis for the assessment of the process risk that exists and allows determination of the required integrity of the safety instrumented function under consideration. Each of the parameters is assigned a range of values such that when applied in combination, a graded assessment of the risk which exists in the absence of the safety particular function is produced. Thus a measure of the degree of reliance to be placed on the SIF is determined. The risk graph relates particular combinations of the risk parameters to safety integrity levels. The relationship between the combinations of risk parameters and safety integrity levels is established by considering the tolerable risk associated with specific hazards.

When considering the calibration of risk graphs, it is important to consider requirements relating to risk arising from both the owners expectations and Regulatory Authority requirements. Risks to life can be considered under two headings as follows:

– **Individual risk** – defined as the risk per year of the most exposed individual. There is normally a maximum value that can be tolerated. The maximum value is normally from all sources of hazard;
– **Societal risk** – defined as the total risk per year experienced by a group of exposed individuals. The requirement is normally to reduce societal risk to at least a maximum value which can be tolerated by society and until any further risk reduction is disproportionate to the costs of such further risk reduction**.**

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

If it is necessary to reduce individual risk to a specified maximum then it cannot be assumed that all this risk reduction can be assigned to a single SIS. The exposed persons are subject to a wide range of risks arising from other sources (for example, falls and fire and explosion risks).

When considering the extent of risk reduction required, an organization may have criteria relating to the incremental cost of averting a fatality. This can be calculated by dividing the annualised cost of the additional hardware and engineering associated with a higher level of integrity by the incremental risk reduction. An additional level of integrity is justified if the incremental cost of averting a fatality is less than a predetermined amount.

A widely used criterium for societal risk is based on the likelihood, *F*, of *N* fatalities. Tolerable societal risk criteria take the form of a line or set of lines on a log-log plot of the number of fatalities versus frequency of accident. Verification that societal risk guidelines have not been violated is accomplished by plotting the cumulative frequency versus accident consequences for all accidents (that is, the *F-N* curve), and ensuring that the *F-N* curve does not cross the tolerable risk curve.

The above issues need to be considered before each of the parameter values can be specified. Most of the parameters are assigned a range (for example, if the expected demand rate of a particular process falls between a specified decade range of demands per year then W3 may be used). Similarly, for demands in the lower decade range, W2 would apply and for demands in the next lower decade range, W1 applies. Giving each parameter a specified range assists the team in making decisions on which parameter value to select for a specific application. To calibrate the risk graph, values or value ranges are assigned to each parameter. The risk associated with each of the parameter combinations is then assessed in individual and societal terms. The risk reduction required to meet the established risk criteria (tolerable risk or lower) can then be established. Using this method, the integrity levels associated with each parameter combination can be determined. This calibration activity does not need to be carried out each time the SIL for a specific application is to be determined. It is normally only necessary for organisations to undertake the work once, for similar hazards. Adjustment may be necessary for specific projects if the original assumptions made during the calibration are found to be invalid for any specific project.

When parameter assignments are made, information should be available as to how the values were derived.

It is important that this process of calibration is agreed at a senior level within the organization taking responsibility for safety. The decisions taken determine the overall safety achieved.

In general, it will be difficult for a risk graph to consider the possibility of dependent failure between the sources of demand and the SIS. It can therefore lead to an over-estimation of the effectiveness of the SIS.

D.4 Membership and organization of the team undertaking the SIL assessment

It is unlikely that a single individual has all the necessary skills and experience to make decisions on all the relevant parameters. Normally a team approach is applied with a team being set up specifically to determine safety integrity levels. Team membership is likely to include the following:

– process specialist;
– process control engineer;
– operations management;
– safety specialist;
– person who has practical experience of operating the process under consideration.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

The team normally considers each safety instrumented function in turn. The team will need comprehensive information on the process and the likely number of persons exposed to the risk.

D.5 Documentation of results of SIL determination

It is important that all decisions taken during SIL determination are recorded in documents which are subject to configuration management. It should be clear from the documentation why the team selected the specific parameters associated with a safety function. The forms recording the outcome of, and assumptions behind, each safety function SIL determination should be compiled into a dossier. If it is established that there are a large number of systems performing safety functions in an area served by a single operations team, then it may be necessary to review the validity of the calibration assumptions. The dossier should also include additional information as follows:

– the risk graph used together with descriptions of all parameter ranges;

– the drawing and revision number of all documents used;

– references to manning assumptions and any consequence studies which have been used to evaluate parameters;

– references to the failures that lead to demands and any fault propagation models where these have been used to determine demand rates;

– references to data sources used to determine demand rates.

D.6 Example calibration based on typical criteria

Table D.2, which gives parameter descriptions and ranges for each parameter, was developed to meet typical specified criteria for chemical processes as described above. Before using this within any project context, it is important to confirm that it meets the needs of those who take responsibility for safety.

The concept of vulnerability has been introduced to modify the consequence parameter. This is because in many instances a failure does not cause an immediate fatality. A receptor's vulnerability is an important consideration in risk analysis because the dose received by a subject is sometimes not large enough to cause a fatality. A receptor's vulnerability to a consequence is a function of the concentration of the hazard to which he was exposed and the duration of the exposure. An example of this is where a failure causes the design pressure for an item of equipment to be exceeded, but the pressure will not rise higher than the equipment test pressure. The likely outcome will normally be limited to leakage through a flange gasket. In such cases, the rate of escalation is likely to be slow and operations staff will normally be able to escape the consequences. Even in cases of major leakage of liquid inventory, the escalation time will be sufficiently slow to enable there to be a high probability that operations staff may be able to avoid the hazard. There are of course cases where a failure could lead to a rupture of piping or vessels where the vulnerability of operating staff may be high.

Consideration will be given to the increased number of people being in the vicinity of the hazardous event as a result of investigating the symptoms during the build-up to the event. The worst case scenario should be considered.

It is important to recognise the difference between 'vulnerability' (V) and the 'probability of avoiding the hazardous event' (P) so that credit is not taken twice for the same factor. Vulnerability is a measure that relates to the speed of escalation after the hazard occurs, whereas the P parameter is a measure that relates to preventing the hazard. The parameter P_A should only be used in cases where the hazard can be prevented by the operator taking action, after he becomes aware that the SIS has failed to operate.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Some restrictions have been placed on how occupancy parameters are selected. The requirement is to select the occupancy factor based on the most exposed person rather than the average across all people. The reason for this is to ensure the most exposed individual is not subject to a high risk which is then averaged out across all persons exposed to the risk.

When a parameter does not fall within any of the specified ranges, then it is necessary to determine risk reduction requirements by other methods or to re-calibrate the risk graph, Figure D.1, using the methods described above.

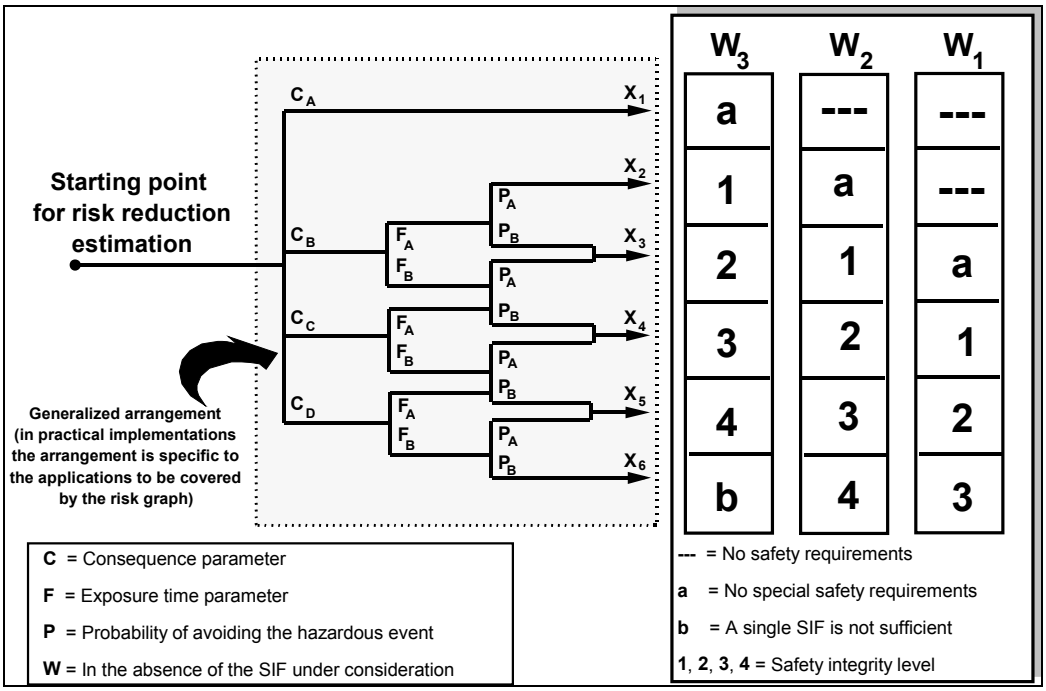


Figure D.1 – Risk graph: general scheme

Table D.2 – Example calibration of the general purpose risk graph

Risk parameter		Classification	Comments
Consequence (C) Number of fatalities	C_A	Minor injury	1 The classification system has been developed to deal with injury and death to people.
This can be calculated by determining the numbers of people present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard.	C_B	Range 0,01 to 0,1	2 For the interpretation of C_A, C_B, C_C and C_D, the consequences of the accident and normal healing should be taken into account.
	C_C	Range >0,1 to 1,0	
The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used:	C_D	Range >1,0	
V = 0,01 Small release of flammable or toxic material			
V = 0,1 Large release of flammable or toxic material			
V = 0,5 As above but also a high probability of catching fire or highly toxic material			
V = 1 Rupture or explosion			

--`,,`,,,`,,,`,`,,`,,,`,,,,,,,,`,`-`,,`,,`,`,,`---

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Risk parameter		Classification	Comments
Occupancy (F) This is calculated by determining the proportional length of time the area exposed to the hazard is occupied during a normal working period. NOTE 1 If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected. NOTE 2 It is only appropriate to use F_A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities.	F_A F_B	Rare to more frequent exposure in the hazardous zone. Occupancy less than 0,1 Frequent to permanent exposure in the hazardous zone	3 See comment 1 above.
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	P_A P_B	Adopted if all conditions in column 4 are satisfied Adopted if all the conditions are not satisfied	4 P_A should only be selected if all the following are true: – facilities are provided to alert the operator that the SIS has failed; – independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area; – the time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions.
Demand rate (W) The number of times per year that the hazardous event would occur in absence of SIF under consideration. To determine the demand rate it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61511, is limited to below the performance ranges associated with SIL1.	W_1 W_2 W_3	Demand rate less than 0,1 D per year Demand rate between 0,1 D and D per year Demand rate between D and 10 D per year For demand rates higher than 10 D per year higher integrity shall be needed	5 The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS. If the demand rate is very high, the SIL has to be determined by another method or the risk graph recalibrated. It should be noted that risk graph methods may not be the best approach in the case of applications operating in continuous mode, see 3.2.43.2 of IEC 61511–1. 6 D is a calibration factor, the value of which should be determined sio that the risk graph results in a level of residuaal risk which is tolerable taking into consideration other risks to exposed persons and corporate criteria.
NOTE This is an example to illustrate the application of the principles for the design of risk graphs. Risk graphs for particular applications and particular hazards will need to be agreed with those involved, taking into account tolerable risk, see D.1 to D.6.			

D.7 Using risk graphs where the consequences are environmental damage

The risk graph approach may also be used to determine the integrity level requirements where the consequences of failure include acute environmental loss. The integrity level needed depends on the characteristics of the substance released and the sensitivity of the environment. A general table which shows consequences in environmental terms is shown below. Each individual process plant location may have a defined quantity associated with specific substances above which notification is required to local authorities. Projects need to determine what can be accepted in a specific location.

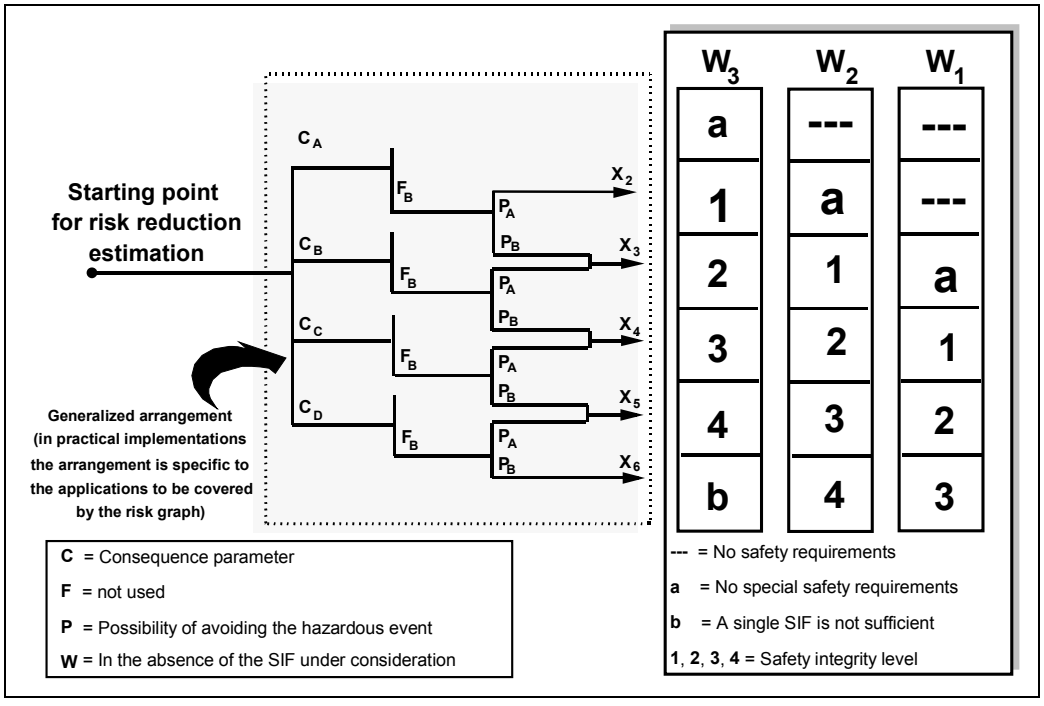
COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Table D.3 – General environmental consequences

Risk parameter		Classification	Comments
Consequence (C)	C_A	A release with minor damage that is not very severe but is large enough to be reported to plant management	A moderate leak from a flange or valve Small scale liquid spill Small scale soil pollution without affecting ground water
	C_B	Release within the fence with significant damage	A cloud of obnoxious vapour travelling beyond the unit following flange gasket blow-out or compressor seal failure
	C_C	Release outside the fence with major damage which can be cleaned up quickly without significant lasting consequences	A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna
	C_D	Release outside the fence with major damage which cannot be cleaned up quickly or with lasting consequences	Liquid spill into a river or sea A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna Solids fallout (dust, catalyst, soot, ash) Liquid release that could affect groundwater

The above consequences can be used in conjunction with the special version of the risk graph, Figure D.2, shown below. It should be noted that the F parameter is not used in this risk graph because the concept of occupancy does not apply. Other parameters P and W apply and definitions can be identical to those applied above to safety consequences.



IEC 3022/02

Figure D.2 – Risk graph: environmental loss

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

D.8 Using risk graphs where the consequences are asset loss

The risk graph approach may also be used to determine the integrity level requirements where the consequences of failure include asset loss. Asset loss is the total economic loss associated with the failure to function on demand. It includes rebuild costs if any damage is incurred and the cost of lost or deferred production. The integrity level justified for any loss consequence can be calculated using normal cost benefit analysis. There are benefits in using risks graphs for asset loss if the risk graph approach is being used to determine the integrity levels associated with safety and environmental consequences. When used to determine the integrity level associated with asset losses, the consequence parameters C_A to C_D have to be defined. These parameters may vary within a wide range from one company to another.

A similar risk graph to that used for environmental protection can be developed for asset loss. It should be noted that the F parameter should not be used as the concept of occupancy does not apply. Other parameters P and W apply and definitions can be identical to those applied above to safety consequences.

D.9 Determining the integrity level of instrument protection function where the consequences of failure involve more than one type of loss

In many cases the consequences of failure to act on demand involves more than one category of loss. Where this is the case the integrity level requirements associated with each category of loss should be determined separately. Different methods may be used for each of the separate risks identified. The integrity level specified for the function should take into account the cumulative total of all the risks involved if the function fails on demand.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Annex E
(informative)

Determination of the required safety integrity levels – a qualitative method: risk graph

E.1 General

This annex is based on methods described in greater detail in the following reference:

DIN V 19250, 1994: *Control technology: Fundamental safety aspects to be considered for measurement and control equipment*

This annex describes the risk graph method for determining safety integrity levels of safety instrumented functions. This is a qualitative method that enables the safety integrity level of a safety instrumented function to be determined from a knowledge of the risk factors associated with the process and basic process control system.

The approach uses a number of parameters which together describe the nature of the hazardous situation when safety instrumented 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 instrumented functions. These parameters:

– allow a graded assessment of the risks to be made, and
– represent key risk assessments factors.

The risk graph approach can also be used to determine the need for risk reduction where the consequences include acute environmental damage or asset loss

This annex shows the application of the above method (which is described in DIN V 19250 and VDI/VDE 2180) for process industry and the machinery sector which has been used for many years and which has been accepted by the German process industry and the machinery sector. It has been accepted by the TUV (German accredited test laboratory) and the German regulating authorities responsible for that part of industry. This graph is used to determine the safety integrity level of a safety-related system; the link between this graph and the safety integrity level is shown in Figures E.1 and E.2.

E.2 Typical implementation of instrumented functions

A clear distinction is made between safety-relevant tasks and operating requirements in the safeguarding of process plants using means of process control. Therefore, process control systems are classified as follows:

– basic process control systems;
– process monitoring systems;
– safety instrumented systems.

The objective of the classification is to have adequate requirements for each type of system to meet the overall requirements of the plant at an economically reasonable cost. The classification enables clear delineation in planning, erection and operation and also during subsequent modifications to process control systems.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Basic process control systems are used for the correct operation of the plant within its normal operating range. This includes measuring, controlling and/or recording of all the relevant process variables. Basic process control systems are in continuous operation or frequently requested to act and intervene before the reaction of a safety instrumented system is necessary (BPCS systems do not normally need to be implemented according to the requirements of this standard)

Process monitoring systems act during the specified operation of a process plant whenever one or more process variables leave the normal operating range. Process monitoring systems alarm a permissible fault status of the process plant to alert the operating personnel or induce manual interventions. (Process monitoring systems do not normally need to be implemented according to the requirements of this standard).

Safety Instrumented systems either prevent a dangerous fault state of the process plant ("protection system") or reduce the consequences of a hazardous event.

If there is no safety instrumented system, a hazardous event leading to personnel injury is possible.

In contrast to the functions of a basic process control system, the functions of safety instrumented systems normally have a low demand rate. This is primarily due to the low probability of the hazardous event. In addition BPCS and monitoring systems which are in continuous operation and reduce the demand rate of the safety instrumented system are normally present.

E.3 Risk graph synthesis

The risk graph is based on the principle that risk is proportional to the consequence and frequency of the hazardous event. It starts by assuming that no safety instrumented systems exist, although typical non safety instrumented systems such as BPCS and monitoring systems are in place.

Consequences are related to harm associated with health and safety or also harm from environmental damage

Frequency is the combination of:

– the frequency of presence in the hazardous zone and the potential exposure time;
– the possibility of avoiding the hazardous event; and
– the probability of the hazardous event taking place with no safety instrumented systems in place (but all other external risk reduction facilities are operating) – this is termed the probability of the unwanted occurrence.

This produces the following four risk parameters:

– consequence of the hazardous event (C);
– frequency of presence in the hazardous zone multiplied with the exposure time (F);
– possibility of avoiding the consequences of the hazardous event (P);
– probability of the unwanted occurrence (W).

When a risk graph is used to determine the safety integrity level of a safety function acting in continuous mode then consideration will need to be given to changing the parameters that are used within the risk graph. The parameters should represent the risk factors that relate best to the application characteristics involved. Consideration will also need to be given to the mapping of safety integrity levels to the outcome of the parameter decisions as some adjustment may be necessary to ensure risk is reduced to tolerable levels. As an example the parameter W may be redefined as the percentage of the life of the system during which the

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

system is on mission. Thus W1 would be selected where the hazard is not continuously present and the period per year when a failure would lead to hazard is short. In this example the other parameters would also need to be considered for the decision criteria involved and the integrity level outcomes reviewed to ensure tolerable risk.

E.4 Risk graph implementation: personnel protection

The combination of the risk parameters described above enables a risk graph as shown in Figure E.1. Higher parameter indices indicate higher risk ($C_1 < C_2 < C_3 < C_4$; $F_1 < F_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$). Corresponding classification of parameters for Figure E.1 are in Table E.1. The graph is used separately for each safety function to determine the safety integrity level required for it.

When determining the risk to be prevented by safety instrumented systems, the risk has to be assumed without the existence of the safety instrumented system under consideration. The main points in this review are the type and extent of the effects and the anticipated frequency of the hazardous state of the process plant.

The risk can be systematically and verifiably determined using the method detailed in DIN V 19250, which enables the requirement classes to be determined from established parameters. As a rule, the higher the ordinal number of a requirement class, the larger the part-risk to be covered by the safety instrumented system and therefore generally the more stringent the requirements and resulting measures.

For the process industry, requirement classes AK 7 and 8 are not covered by safety instrumented systems alone. Non-process control measures are needed to reduce the risk to at least requirement class AK 6.

As it is not practical to formulate individual requirements with appropriate sets of measures for each of these requirement classes, a subdivision into two areas is made in accordance with VDI/VDE 2180.

Risk area I: Lower risk to be covered (SIL 1 and 2)

Risk area II: Higher risk to be covered (SIL 3)

Figure E.1 shows the relationship between the requirement classes according to DIN V 19250 and the risk areas.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

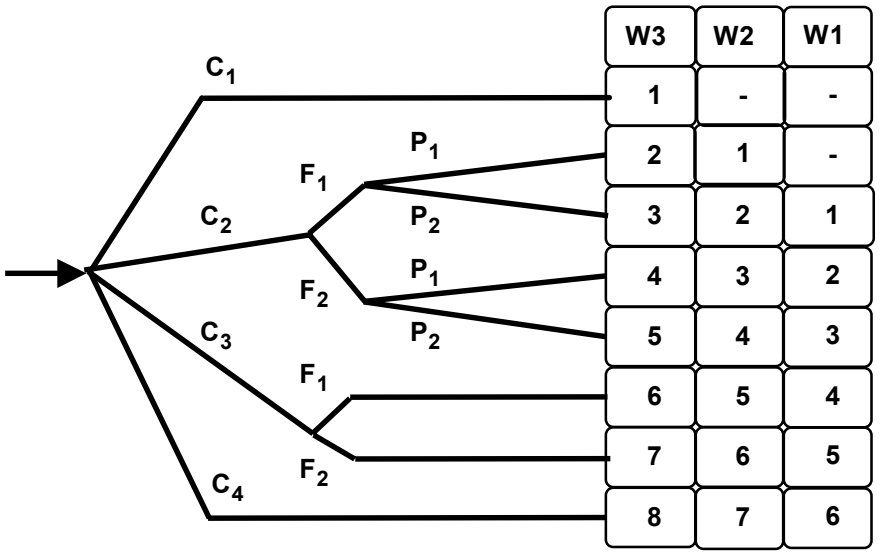


Figure E.1 – DIN V 19250 Risk graph – personnel protection (see Table E.1)

Table E.1 – Data relating to risk graph (see Figure E.1)

Risk parameter		Classification	Comments
Consequence (C)	C_1	Light injury to persons	1 This classification system has been developed to deal with injury and death of people. Other classification schemes would need to be developed for environmental or asset damage.
	C_2	Serious permanent injury to one or more persons; death of one person	
	C_3	Death of several persons	
	C_4	Catastrophic effect, very many people killed	
Frequency of presence in the hazardous zone multiplied with the exposure time (F)	F_1	Rare to more frequent exposure in the hazardous zone	2 See comment 1 above.
	F_2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the consequences of the hazardous event (P)	P_1	Possible under certain conditions	3 This parameter takes into account the: – operation of a process (supervised (that is, operated by skilled or unskilled persons) or unsupervised); – rate of development of the hazardous event (for example suddenly, quickly or slowly);
	P_2	Almost impossible	– ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); – avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical process or a similar process or may not exist).

--`,,`,,,,`,`,,`,,,,,,,,,,,,-`-`,,`,,`,`,,`---

AA
COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003
07:19:03 MDT Questions or comments about this message: please call the Document
Policy Management Group at 1-800-451-1584.

Risk parameter		Classification	Comments
Probability of the unwanted occurrence (W)	W_1	A very slight probability that the unwanted occurrences occur and only a few unwanted occurrences are likely	4 The purpose of the W factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety instrumented systems (E/E/PE or other technology) but including any external risk reduction facilities.
	W_2	A slight probability that the unwanted occurrences occur and few unwanted occurrences are likely	
	W_3	A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely	

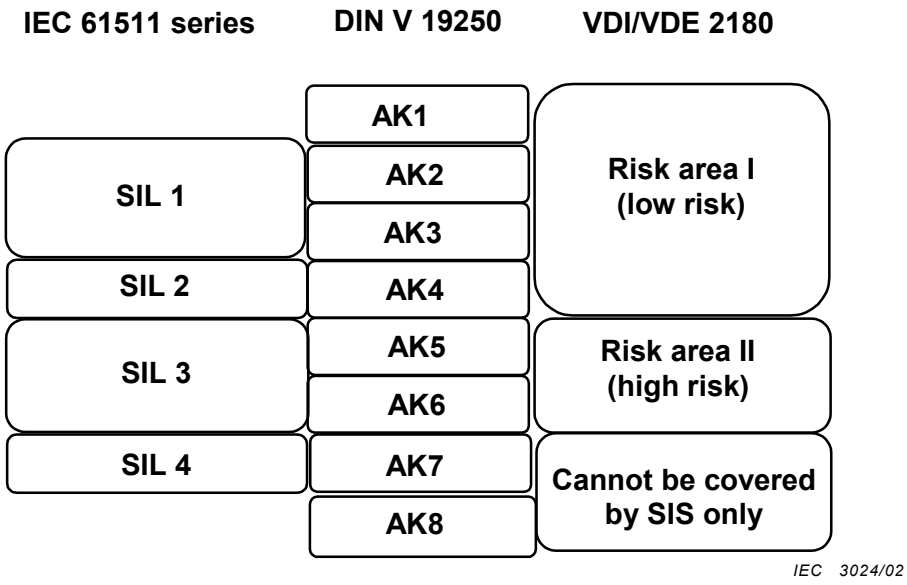


Figure E.2 – Relationship between IEC 61511 series, DIN 19250 and VDI/VDE 2180

E.5 Relevant issues to be considered during application of risk graphs

When applying the risk graph method, it is important to consider risk requirements from the owner and any applicable regulatory authority.

The interpretation and evaluation of each risk graph branch should be described and documented in a clear and understandable terms to ensure consistency in the method application.

It is important that the risk graph is agreed to at a senior level within the organisation taking responsibility for safety.

--`,,,`,,,,``,,```,,,````````-`-`,,`,,`,`,,`---

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Annex F
(informative)

Layer of protection analysis (LOPA)

F.1 Introduction

This annex describes a process hazard analysis tool called Layer of Protection Analysis (LOPA). The method starts with data developed in the Hazard and Operability analysis (HAZOP study) and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction can then be determined and the need for more risk reduction analyzed. If additional risk reduction is required and if it is to be provided in the form of a Safety Instrumented Function (SIF), the LOPA methodology allows the determination of the appropriate Safety Integrity Level (SIL) for the SIF.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is based on a method described in more detail in the following reference:

Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1.

F.2 Layer of protection analysis

The safety lifecycle defined in IEC 61511-1 requires the determination of a safety integrity level for the design of a safety-instrumented function. The LOPA described here is a method that can be applied to an existing plant by a multi-disciplinary team to determine a safety instrumented function SIL. The team should consist of the:

– operator with experience operating the process under consideration;
– engineer with expertise in the process;
– manufacturing management;
– process control engineer;
– instrument/electrical maintenance person with experience in the process under consideration;
– risk analysis specialist.

One person on the team should be trained in the LOPA methodology.

The information required for the LOPA is contained in the data collected and developed in the Hazard and Operability analysis (HAZOP study). Table F.1 shows the relationship between the data required for the Layer of Protection Analysis (LOPA) and the data developed during the HAZOP study. Figure F.1 shows a typical spreadsheet that can be used for the LOPA.

LOPA analyzes hazards to determine if SIFs are required and if so, the required safety integrity level (SIL) of each SIF.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Table F.1 – HAZOP developed data for LOPA

LOPA required information	HAZOP developed information
Impact event	Consequence
Severity level	Consequence severity
Initiating cause	Cause
Initiating likelihood	Cause frequency
Protection layers	Existing safeguards
Required additional mitigation	Recommended new safeguards

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS								
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access,F.8 F.14.7	IPL additional mitigation dikes, pressure relief F.9 F.14.8	Inter-mediate event likelihood F.10 F.14.9	SIF integrity level F.11 F.14.10	Mitigated event likelihood F.12 F.14.10	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1		0,1	01	PRV 01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC 3025/02

NOTE Severity Level E = Extensive; S = Serious; M = Minor.

Likelihood values are events per year, other numerical values are probabilities of failure on demand average.

Figure F.1 – Layer of Protection Analysis (LOPA) report

F.3 Impact event

Using Figure F.1, each impact event description (consequence) determined from the HAZOP study is entered in column 1.

F.4 Severity Level

Severity levels of Minor (M), Serious (S), or Extensive (E) are next selected for the impact event according to Table F.2 and entered into column 2 of Figure F.1.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Table F.2 – Impact event severity levels

Severity level	Consequence
Minor (M)	Impact initially limited to local area of event with potential for broader consequence, if corrective action not taken.
Serious (S)	Impact event could cause serious injury or fatality on site or off site.
Extensive (E)	Impact event that is five or more times severe than a serious event.

F.5 Initiating cause

All of the initiating causes of the impact event are listed in column 3 of Figure F.1. Impact events may have many Initiating causes, and it is important to list all of them.

F.6 Initiation likelihood

Likelihood values of the initiating causes occurring, in events per year, are entered into column 4 of Figure F.1. Table F.4 shows typical initiating cause likelihood. The experience of the team is very important in determining the initiating cause likelihood.

Table F.4 – Initiation Likelihood

Low	A failure or series of failures with a very low probability of occurrence within the expected lifetime of the plant. EXAMPLES – Three or more simultaneous Instrument, or human failures. – Spontaneous failure of single tanks or process vessels.	$f < 10^{-4}$, $/_{yr}$
Medium	A failure or series of failures with a low probability of occurrence within the expected lifetime of the plant. EXAMPLES – Dual instrument or valve failures. – Combination of instrument failures and operator errors. – Single failures of small process lines or fittings	$10^{-4} < f < 10^{-2}$, $/_{yr}$
High	A failure can reasonably be expected to occur within the expected lifetime of the plant. EXAMPLES – Process Leaks – Single instrument or valve failures. – Human errors that could result in material releases.	$10^{-2} < f$, $/_{yr}$

F.7 Protection layers

Figure 2 shows the multiple Protection Layers (PLs) that are normally provided in the process industry. Each protection layer consists of a grouping of equipment and/or administrative controls that function in concert with the other layers. Protection layers that perform their function with a high degree of reliability may qualify as Independent Protection Layers (IPL) (see Clause F.9).

Process design to reduce the likelihood of an impact event from occurring, when an Initiating cause occurs, are listed first in column 5 of Figure F.1. An example of this would be a jacketed pipe or vessel. The jacket would prevent the release of process material if the integrity of the primary pipe or vessel is compromised.

The next item in column 5 of Figure F.1 is the Basic Process Control System (BPCS). If a control loop in the BPCS prevents the impacted event from occurring when the initiating

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

cause occurs, credit based on its PFD_{avg} (average probability of failure on demand) is claimed.

The last item in column 5 of Figure F.1 takes credit for alarms that alert the operator and utilize operator intervention. Typical protection layer PFD_{avg} values are listed in Table F.3.

Table F.3 – Typical protection layer (prevention and mitigation) PFDs

Protection layer	PFD
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	$1,0 \times 10^{-2}$ to $1,0 \times 10^{-4}$
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1,0 \times 10^{-1}$
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

F.8 Additional mitigation

Mitigation layers are normally mechanical, structural, or procedural. Examples would be:

– pressure relief devices;
– dikes (bunds); and
– restricted access.

Mitigation layers may reduce the severity of the impact event but not prevent it from occurring. Examples would be:

– deluge systems for fire or fume release;
– fume alarms; and
– evacuation procedures.

The LOPA team should determine the appropriate PFDs for all mitigation layers and list them in column 6 of Figure F.1.

F.9 Independent Protection Layers (IPL)

Protection layers that meet the criteria for IPL are listed in column 7 of Figure F.1.

The criteria to qualify a Protection Layer (PL) as an IPL are:

– The protection provided reduces the identified risk by a large amount, that is, a minimum of a 100-fold reduction;
– The protective function is provided with a high degree of availability (0,9 or greater);
– It has the following important characteristics:
  a) Specificity: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL;
  b) Independence: An IPL is independent of the other protection layers associated with the identified danger.
  c) Dependability: It can be counted on to do what it was designed to do. Both random and systematic failures modes are addressed in the design.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards
Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

d) Auditability: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

Only those protection layers that meet the tests of availability, specificity, independence, dependability, and auditability are classified as independent protection layers.

F.10 Intermediate event likelihood

The Intermediate event likelihood is calculated by multiplying the initiating likelihood (column 4 of Figure F.1) by the PFDs of the protection layers and mitigating layers (columns 5, 6 and 7 of Figure F.1). The calculated number is in units of events per year and is entered into column 8 of Figure F.1.

If the intermediate event likelihood is less than your corporate criteria for events of this severity level, additional PLs are not required. Further risk reduction should, however, be applied if economically appropriate.

If the intermediate event likelihood is greater than your corporate criteria for events of this severity level, additional mitigation is required. Inherently safer methods and solutions should be considered before additional protection layers in the form of Safety Instrumented Systems (SIS) are applied. If inherently safe design changes can be made, Figure 1 is updated and the intermediate event likelihood recalculated to determine if it is below corporate criteria. If the above attempts to reduce the intermediate likelihood below corporate risk criteria fail, a SIS is required.

F.11 SIF integrity level

If a new SIF is needed, the required integrity level can be calculated by dividing the corporate criteria for this severity level of event by the intermediate event likelihood. A PFD_{avg} for the SIF below this number is selected as a maximum for the SIS and entered into column 9.

F.12 Mitigated event likelihood

The mitigated event likelihood is now calculated by multiplying columns 8 and 9 and entering the result in column 10. This is continued until the team has calculated a mitigated event likelihood for each impact event that can be identified.

F.13 Total risk

The last step is to add up all the mitigated event likelihood for serious and extensive impact events that present the same hazard. For example, the mitigated event likelihood for all serious and extensive events that cause fire would be added and used in formulas like the following:

– risk of fatality due to fire = (mitigated event likelihood of all flammable material release) X (probability of ignition) X (probability of a person in the area) X (probability of fatal injury in the fire).

Serious and extensive impact events that would cause a toxic release would be added and used in formulas like the following:

– risk of fatality due to toxic release = (mitigated event likelihood of all toxic releases) X (probability of a person in the area) X (probability of fatal injury in the release).

The expertise of the risk analyst specialist and the knowledge of the team are important in adjusting the factors in the formulas to conditions and work practices of the plant and affected community.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

The total risk to the corporation from this process can now be determined by totalling the results obtained from applying the formulas.

If this meets or is less than the corporate criteria for the population affected, the LOPA is complete. However, since the affected population may be subject to risks from other existing units or new projects, it is wise to provide additional mitigation and risk reduction if it can be accomplished economically.

F.14 Example

The following is an example of the LOPA methodology that addresses one impact event identified in the HAZOP STUDY.

F.14.1 Impact event and severity level

The HAZOP STUDY identified high pressure in a batch polymerization reactor as a deviation. The stainless steel reactor is connected in series to a packed steel fibre reinforced plastic column and a stainless steel condenser. Rupture of the fibre reinforced plastic column would release flammable vapour that would present the possibility for fire if an ignition source is present. Using Table F.2, severity level serious is selected by the LOPA team since the impact event could cause a serious injury or fatality on site. The Impact Event and its severity are entered into columns 1 and 2, Figure F.1, respectively.

F.14.2 Initiating causes

The HAZOP STUDY listed two initiating causes for high pressure. Loss of cooling water to the condenser and failure of the reactor steam control loop. The two initiating causes are entered into column 3, Figure F.1.

F.14.3 Initiating likelihood

Plant operations have experienced loss in cooling water once in 15 years in this area. The team selects once every 10 years as a conservative estimate of cooling water loss. 0,1 events per year is entered into column 4, Figure F.1. It is wise to carry this initiating cause all the way through to conclusion before addressing the other initiating cause (failure of the reactor steam control loop).

F.14.4 Protection layers design

The process area was designed with an explosion proof electrical classification and the area has a process safety management plan in effect. One element of the plan is a management of change procedure for replacement of electrical equipment in the area. The LOPA team estimates that the risk of an ignition source being present is reduced by a factor of 10 due to the management of change procedures. Therefore a value of 0,1 so it is entered into column 5, Figure F.1 under process design.

F.14.5 BPCS

High pressure in the reactor is accompanied by high temperature in the reactor. The BPCS has a control loop that adjusts steam input to the reactor jacket based on temperature in the reactor. The BPCS would shut off steam to the reactor jacket if the reactor temperature is above set-point. Since shutting off steam is sufficient to prevent high pressure, the BPCS is a protection layer. The BPCS is a very reliable DCS and the production personnel have never experienced a failure that would disable the temperature control loop. The LOPA team decides that a PFD_{avg} of 0,1 is appropriate and enters 0,1 in column 5, Figure F.1 under BPCS (0,1 is the minimum allowable for the BPCS).

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

F.14.6 Alarms

There is a transmitter on cooling water flow to the condenser, and it is wired to a different BPCS input and controller than the temperature control loop. Low cooling water flow to the condenser is alarmed and utilizes operator intervention to shut off the steam. The alarm can be counted as a protection layer since it is located in a different BPCS controller than the temperature control loop. The LOPA team agrees that 0,1 PFD_{avg} is appropriate since an operator is always present in the control room and enters 0,1 in column 5, Figure F.1 under alarms.

F.14.7 Additional mitigation

Access to the operating area is restricted during process operation. Maintenance is only performed during periods of equipment shut down and lock out. The process safety management plan requires all non-operating personnel to sign into the area and notify the process operator. Because of the enforced restricted access procedures, the LOPA teams estimate that the risk of personnel in the area is reduced by a factor of 10. Therefore 0,1 is entered into column 6, Figure F.1 under additional mitigation and risk reduction.

F.14.8 Independent Protection Level(s) (IPL)

The reactor is equipped with a relief valve that has been properly sized to handle the volume of gas that would be generated during over temperature and pressure caused by cooling water loss. After consideration of the material inventory and composition, the contribution of the relief valve in terms of risk reduction was assessed. Since the relief valve is set below the design pressure of the fibre glass column and there is no possible human failure that could isolate the column from the relief valve during periods of operation, the relief valve is considered a protection layer. The relief valve is removed and tested once a year and never in 15 years of operation has any pluggage been observed in the relief valve or connecting piping. Since the relief valve meets the criteria for a IPL, it is listed in column 7, Figure F.1 and assigned a PFD_{avg} of 0,01.

F.14.9 Intermediate event likelihood

The columns in row 1, Figure 1 are now multiplied together and the product is entered in column 8, Figure F.1 under intermediate event likelihood. The product obtained for this example is 10^{-7}.

F.14.10 SIS

The mitigation and risk reduction obtained by the protection layers are sufficient to meet corporate criteria, but additional mitigation can be obtained for a minimum cost since a pressure transmitter exists on the vessel and is alarmed in the BPCS. The LOPA team decides to add a SIF that consists of a current switch and a relay to de-energize a solenoid valve connected to a block valve in the reactor jacket steam supply line. The SIF is designed to the lower range of SIL 1, with a PFD_{avg} of 0,01. 0,01 is entered into column 9, Figure F.1 under SIF Integrity Level.

The mitigated event likelihood is now calculated by multiplying column 8 by column 9 and putting the result (1×10^{-9}) in column 10, Figure 1.

F.14.11 Next SIF

The LOPA team now considers the second initiating cause (failure of reactor steam control loop). Table F.3 is used to determine the likelihood of control valve failure and 0,1 is entered into column 4, Figure 1 under initiation likelihood.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

The protection layers obtained from process design, alarms, additional mitigation and the SIS still exist if a failure of the steam control loop occurs. The only protection layer lost is the BPCS. The LOPA team calculates the intermediate likelihood (1×10^{-6}) and the mitigated event likelihood (1×10^{-8}). The values are entered into columns 8 and 10, Figure F.1 respectively.

The LOPA team would continue this analysis until all the deviations identified in the HAZOP study have been addressed.

The last step would be to add the mitigated event likelihood for the serious and extensive events that present the same hazard.

In this example, if only the one impact event was identified for the total process, the number would be $1{,}1 \times 10^{-8}$. Since the probability of ignition was accounted for under process design (0,1) and the probability of a person in the area under additional mitigation (0,1) the equation for risk of fatality due to fire reduces to:

Risk of fatality due to fire = (Mitigated event likelihood of all flammable material releases) X (Probability of fatal injury due to fire)

or

Risk of fatality due to fire = $(1{,}1 \times 10^{-8}) \times (0{,}5) = 5{,}5 \times 10^{-9}$

This number is below the corporate criteria for this hazard and further risk reduction is not considered economically justified, so the work of the LOPA team is complete.

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained.

Details and advice can be obtained from the Copyright & Licensing Manager. Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553. Email: copyright@bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL

COPYRIGHT 2003; British Standards Institution on ERC Specs and Standards

Document provided by IHS Licensee=Agip KOC/5950653001, User=, 06/18/2003 07:19:03 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.