IEC 61511-3

Edition 2.0 2016-07
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

Functional safety – Safety instrumented systems for the process industry sector –
Part 3: Guidance for the determination of the required safety integrity levels

IEC 61511-3:2016-07 RLV(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC 61511-3

Edition 2.0 2016-07
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

Functional safety – Safety instrumented systems for the process industry sector –
Part 3: Guidance for the determination of the required safety integrity levels

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.01

ISBN 978-2-8322-3545-4

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

International Standard IEC 61511-3: has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

Additional H&RA example(s) and quantitative analysis consideration annexes are provided.

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

FDIS	Report on voting
65A/779/FDIS	65A786/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.

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. ~~It also requires~~ A process hazard and risk assessment ~~to be~~ is carried out to enable the specification for SIS 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 SIS. The SIS includes all ~~components~~ devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application; SIS safety life-cycle and safety integrity levels (SIL).

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010 ~~(see Annex A of IEC 61511-1)~~.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

– ~~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 SIS is carried out;
– works within a framework which is applicable to all instrumented ~~methods~~ means 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 standard on safety instrumented systems for the process industry:~~

– addresses~~es~~ing all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
– enabl~~es~~ing existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example national, federal, state, province, county, city) have established process safety design, process safety management, or other ~~requirements~~ regulations, these take precedence over the requirements defined in ~~this standard~~ the IEC 61511-1.

~~This standard~~ The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk ~~analysis~~ assessment ~~(H & RA)~~. The information herein is intended to provide a broad overview of the wide range of global methods used to implement ~~H & RA~~ hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016 should be reviewed. The informative annexes in ~~this standard~~ the IEC 61511-3 address the following:

Annex A provides ~~an overview of the concepts of tolerable risk and ALARP~~ information that is common to each of the hazard and risk assessment methods shown herein.

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.

Annex G provides a layer of protection analysis using a risk matrix.

Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.

Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.

Annex J provides an overview of the impact of multiple safety systems on determining the required SIL.

Annex K provides an overview of the concepts of tolerable risk and ALARP.

Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that the IEC 61511 series plays in the achievement of functional safety for SIS.

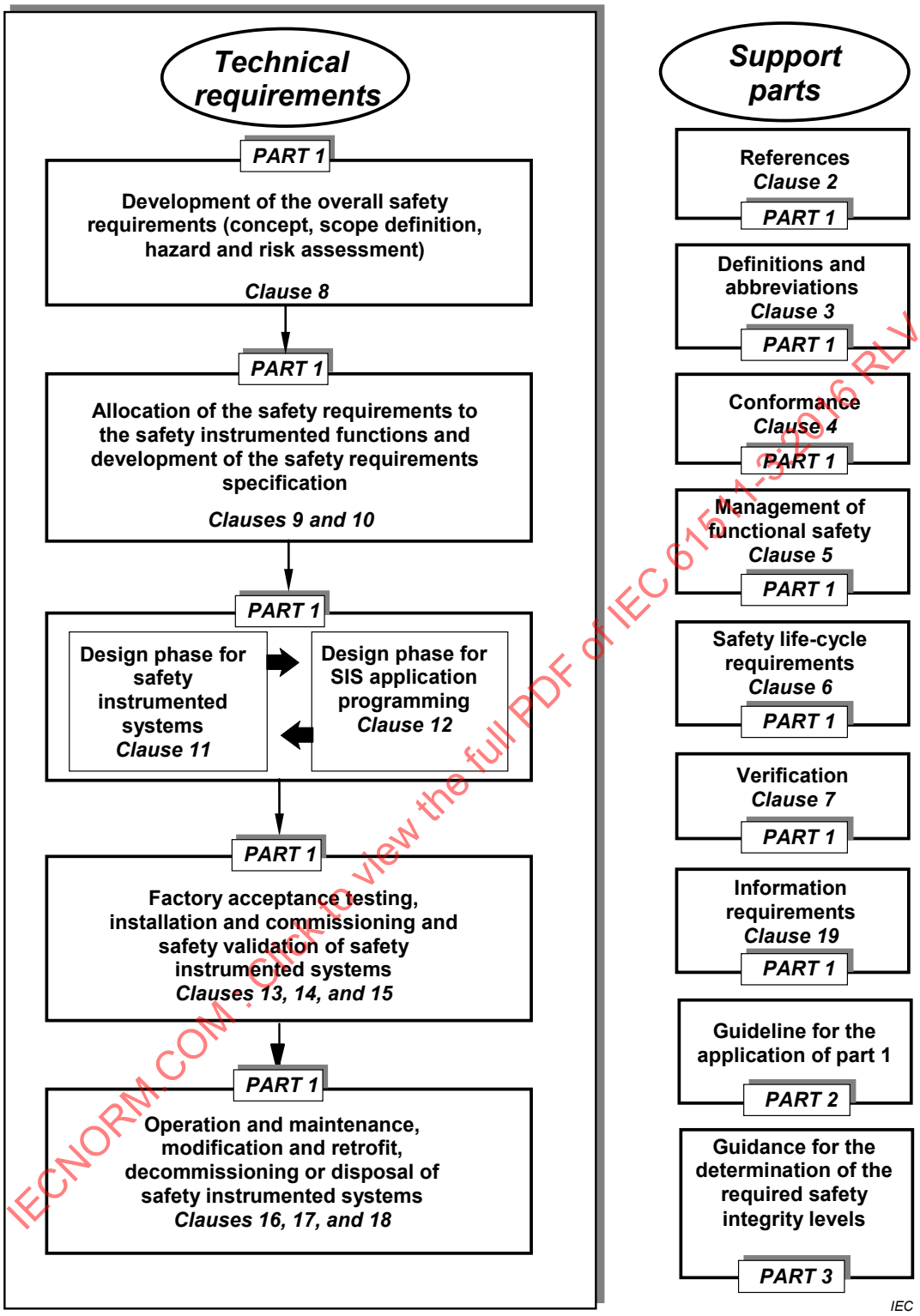


Figure 1 – Overall framework of the IEC 61511 series

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

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

1 Scope

This part of IEC 61511 provides information on:

– the underlying concepts of risk and the relationship of risk to safety integrity (see Clause A.4);

– the determination of tolerable risk (see Annex K);

– a number of different methods that enable the safety integrity level~~s~~ (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);

– the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;

d) illustrates techniques/measures available for determining the required SIL;

e) provides a framework for establishing SIL but does not specify the SIL required for specific applications;

f) does not give examples of determining the requirements for other methods of risk reduction.

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes ~~should~~ can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction ~~methods~~ means.

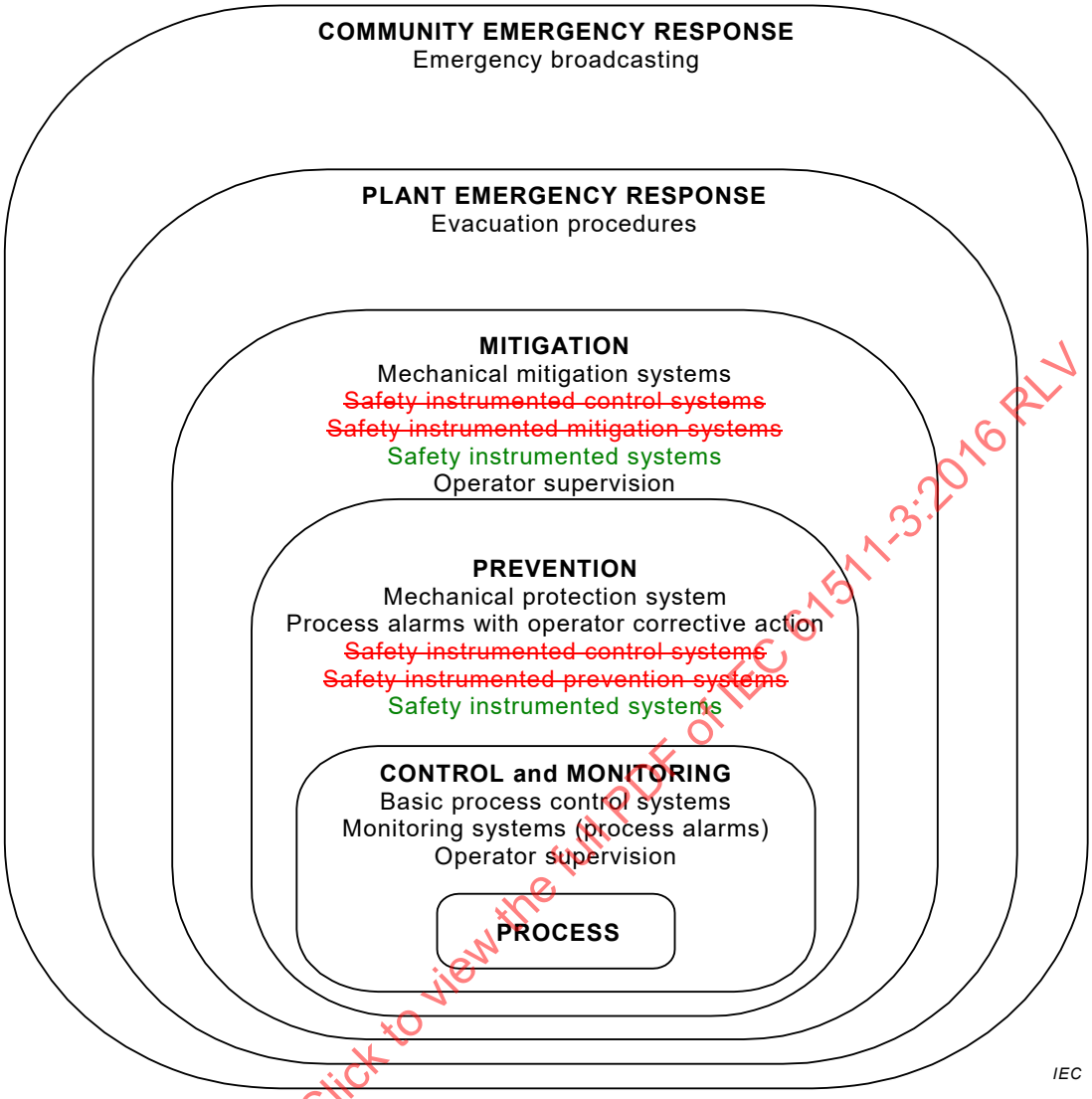


Figure 2 – Typical protection layers and risk reduction ~~methods~~ means ~~found in process plants (for example, protection layer model)~~

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61511-1:2016 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements*

3 Terms, definitions and abbreviations

For the purposes of this document the terms, definitions, and abbreviations given in IEC 61511-1:2016 apply.

The annexes in this Part 3 are informative and not normative. Also, the application of any particular method described in Part 3 annexes does not guarantee compliance with the requirements of IEC 61511-1:2016.

Annex A
(informative)

Risk and safety integrity – general guidance

A.1 General

Annex A 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~~ assessment ~~(H & RA)~~ methods shown herein.

A.2 Necessary risk reduction

The necessary risk reduction (which may be stated either qualitatively (see Note 1) or quantitatively (see Note 2) is the reduction in risk that has to be achieved to meet the tolerable risk (for example, the 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 (SRS) for the SIF (in particular, the safety integrity requirement~~s part of the safety requirements specification~~). The purpose of determining the tolerable risk (for example, the 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 A.2) 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.

NOTE 1 In determining the necessary risk reduction, the tolerable risk ~~needs to be~~ is established. Annexes D and E of IEC 61508-5:2010 outline qualitative methods and semi-quantitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly rather than stated explicitly.

NOTE 2 For example, that a hazardous event, leading to a specific consequence, would typically be expressed as a maximum frequency of occurrence per year.

A.3 Role of safety instrumented systems

A safety instrumented system (SIS) implements the SIF(s) 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~~ SRS 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 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.

A SIF 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.

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 SIF together with any other protection layer has to be such as to ensure that:

– the ~~failure~~ accident frequency due to the failure 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 A.1 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:

  - mechanical protection system;
  - safety instrumented systems;
  - non-SIS instrumented systems;
  - mechanical mitigation system.

NOTE 1 Figure A.1 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 SIS or other protection layers. The resulting risk model may therefore differ from that shown in Figure A.1.

The various risks indicated in Figures A.1 and A.2 are as follows:

– Process risk – The risk existing for the specified hazardous events for the process, the basic process control system (BPCS) and associated human factor issues – no designated safety protective features are considered in the determination of this risk;

– Tolerable risk (for example, the 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 BPCS, the IEC 61511 series 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 A.1.

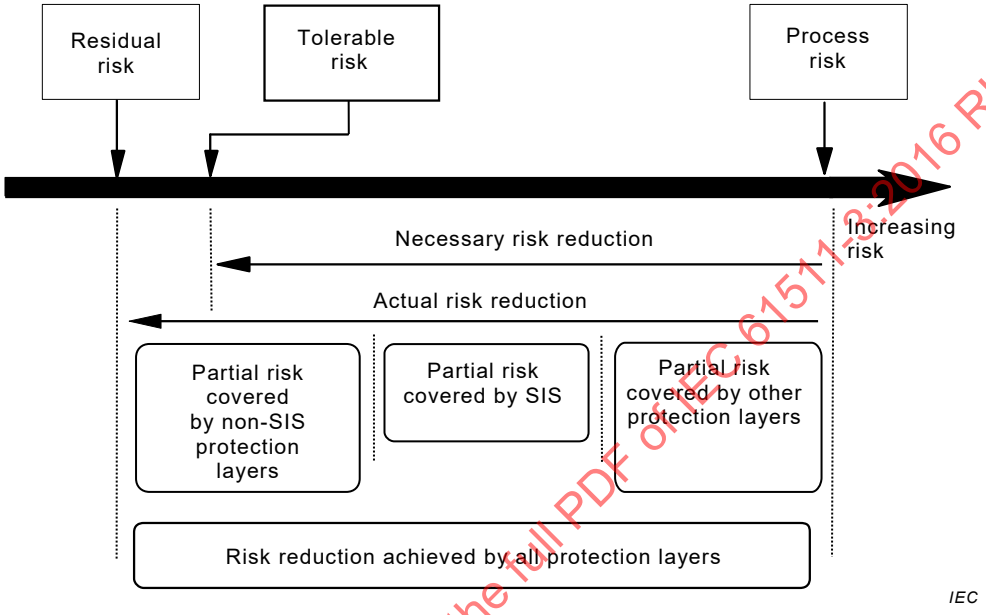


Figure A.1 – Risk reduction: general concepts

NOTE 2 In some applications, risk parameters (e.g., frequency and probability of failure on demand) cannot be combined simply to achieve the risk target as depicted in Figure A.1 without considering the factors noted in Annex J. This may be due to overlapping, common cause failure, and holistic dependencies between the various protection layers.

A.4 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 A.1). 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~~ risk reduction. Once the tolerable risk has been set, and the necessary reduction estimated, the safety integrity requirements for the SIS can be allocated.

NOTE The allocation ~~may~~ can 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 A.1 and A.2.

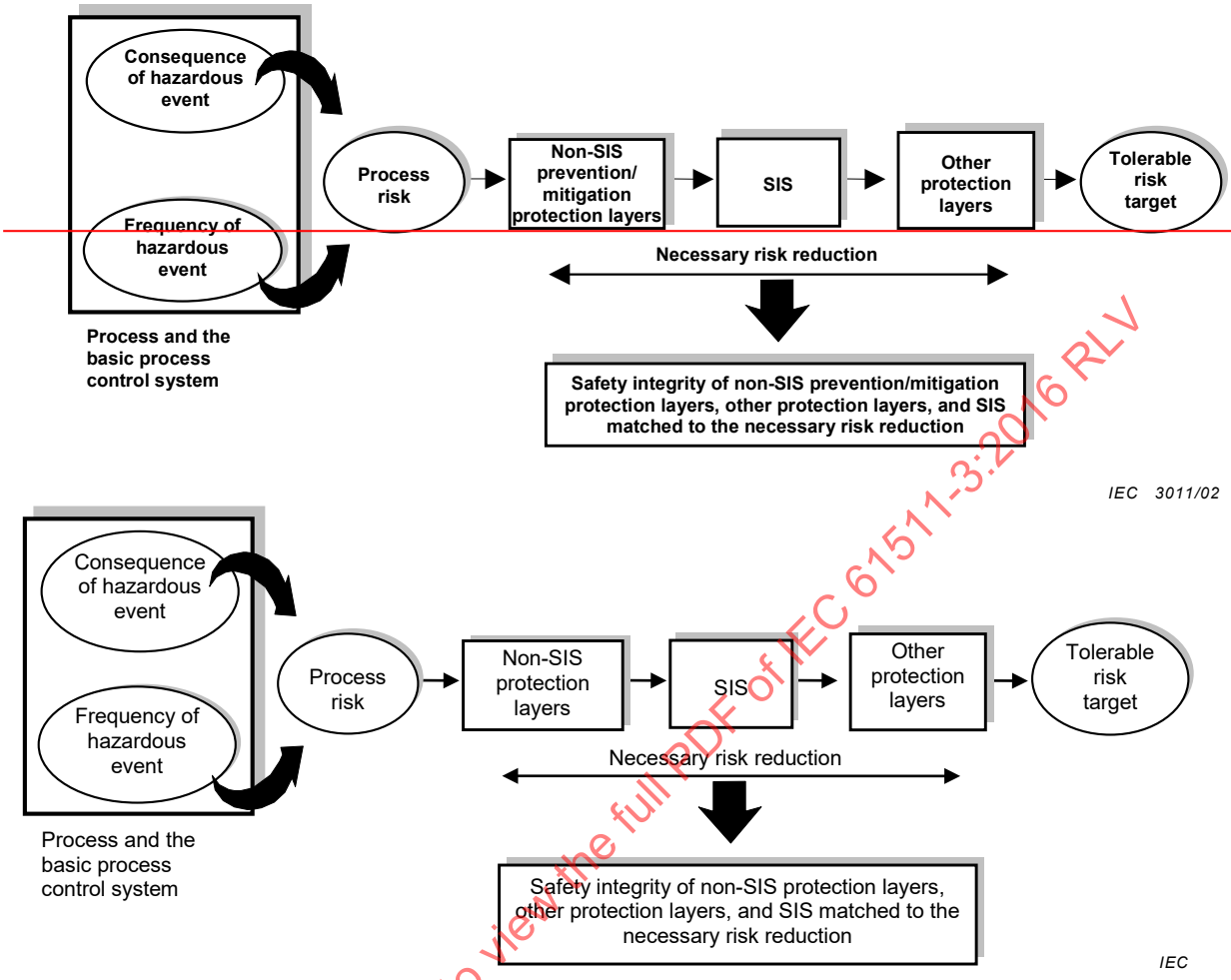


Figure A.2 – Risk and safety integrity concepts

A.5 Allocation of safety requirements

The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the SIS and other protection layers is shown in Figure A.4. The requirements ~~for~~ of the ~~safety requirements~~ allocation ~~phase~~ process are given in Clause 9 of IEC 61511-1:-.

The methods used to allocate the safety integrity requirements to the SIS, 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 through I inclusive).

A.6 Hazardous event, hazardous situation and harmful event

The terms “hazardous event” and “hazardous situation” are used often in the subsequent annexes illustrated herein. Figure A.3 is intended to illustrate the difference between the terms by showing the progression from hazardous event to hazardous situation through loss of control to the occurrence of a harmful event.

Figure A.3 uses harm to people but can equally apply to the outcome of harm to the environment, or damage to property.

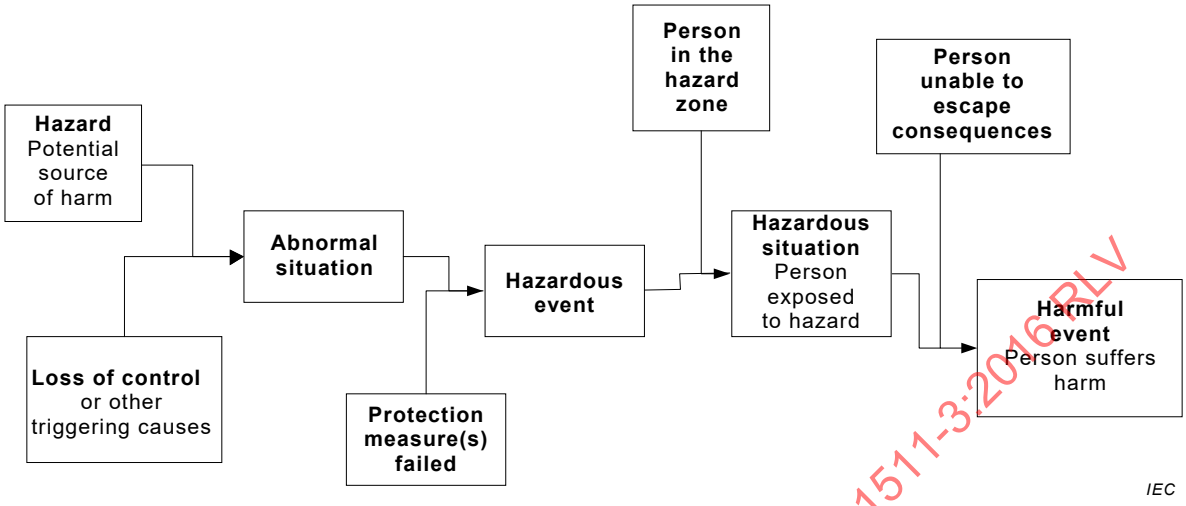


Figure A.3 – Harmful event progression

Figure A.3 shows how loss of control, or any other initiating cause result in an abnormal situation and place a demand on protective measures, such as safety alarms, SIS, relief valves etc. A hazardous event results when a demand occurs and the relevant protective measures are in a failed state, and do not function as intended. A hazardous event in and of itself does not necessarily cause harm, but should a person(s) be in the impact zone (or effect area), thus exposed to the hazardous event, this results in a hazardous situation. If the person is unable to escape the harmful consequences of exposure, this is characterized as a harmful impact due to the personnel injury.

A.7 Safety integrity levels

In the IEC 61511-1:2016, four SILs are specified, with SIL 4 being the highest level and SIL 1 being the lowest.

The ~~safety integrity level~~ target failure measures for the four SIL are specified in Tables 4 and 5 of IEC 61511–1:. Two parameters are specified, one for SIS operating in a low demand mode of operation and one for SIS operating in a continuous/high demand mode of operation.

NOTE For a SIS operating in a low demand mode of operation, the ~~safety integrity~~ target failure measure of interest is the average probability of failure to perform its designed function on demand. For a SIS operating in a continuous/high demand mode of operation, the ~~safety integrity~~ target failure measure of interest is the average frequency of a dangerous failure ~~per hour~~, see 3.2.83 and Table 5 of IEC 61511-1:2016.

A.8 Selection of the method for determining the required safety integrity level

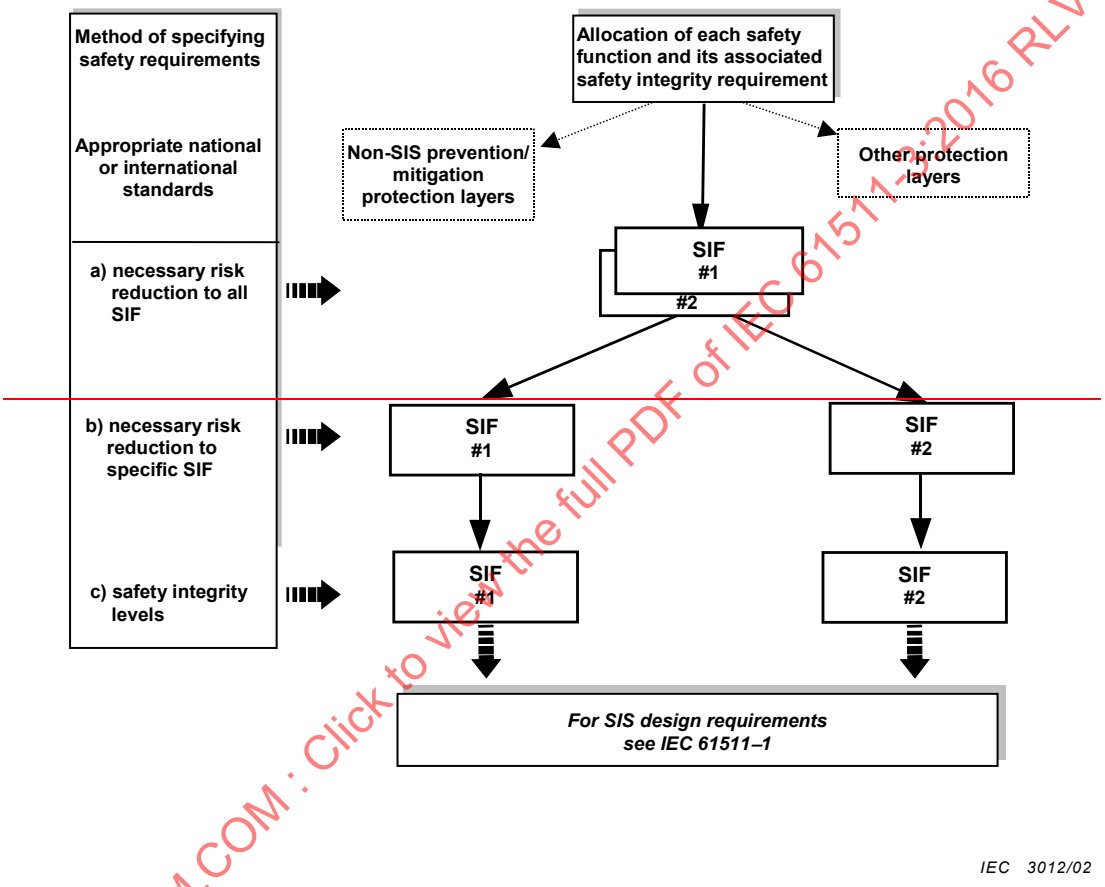
There are a number of ways of establishing the required SIL for a specific application. Annexes B to I present information on a number of methods that have been used. The method selected for a specific application will depend on many factors, including:

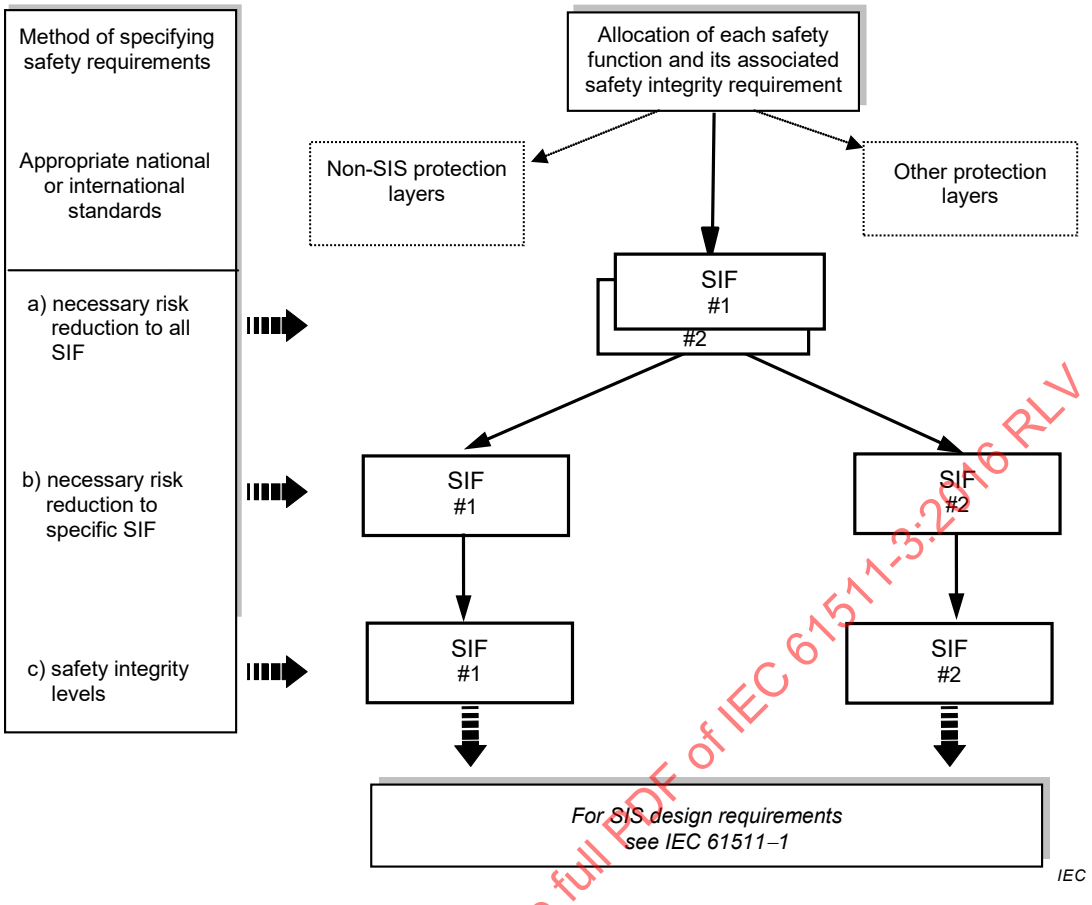
– the complexity of the application;
– the guidelines from regulatory authorities;
– the nature of the risk and the required risk reduction;
– the experience and skills of the persons available to undertake the work;
– the information available on the parameters relevant to the risk (see Figure A.4);

– the information available on SIS currently in use in the particular applications, such as those described in industry standards and practices.

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.

It is important that whichever method(s) are selected for application, that the site risk criteria should be used for the assessment.





NOTE Safety integrity requirements are associated with each SIF before allocation (see IEC 61511-1:2016, Clause 9).

Figure A.4 – Allocation of safety requirements to the ~~safety instrumented systems,~~ non-SIS ~~prevention/mitigation~~ protection layers and other protection layers

Annex B
(informative)

Semi-quantitative method – event tree analysis

B.1 ~~General~~ Overview

Annex B outlines how the target safety integrity levels (SIL) can be determined if a semi-quantitative approach is adopted. A semi-quantitative approach utilizes both qualitative and quantitative techniques and 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).

Annex B is not intended to be a definitive account of the method but is intended to be an overview 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.~~

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008).

B.2 Compliance with IEC 61511-1:2016

The overall objective of Annex B is to outline a procedure to identify the required safety instrumented functions (SIF) and establish their SIL. The basic steps required to comply are the following:

a) Establish the safety target (tolerable risk) ~~of~~ for the process;

b) Perform a hazard and risk ~~analysis~~ assessment to evaluate existing risk for each specific hazardous event;

c) Identify safety function (s) needed for each specific hazardous event;

d) Allocate safety function (s) to protection layers;

NOTE Protection layers are assumed to be independent from each other. The allocation process can ensure that the common cause, common mode, and systematic failures are sufficiently low compared to the overall risk reduction requirements.

e) Determine if a SIF is required;

f) Determine required SIL of the SIF.

Step a) establishes the process safety target. Step b) focuses on the risk ~~analysis~~ assessment of the process, and Step c) derives from the risk ~~analysis~~ assessment what safety functions are required and what risk reduction they need to meet the process safety target. After allocating these safety functions to protection layers in Step d); it will become clear whether a SIF is required (Step e)) and what SIL it will need to meet (Step f)).

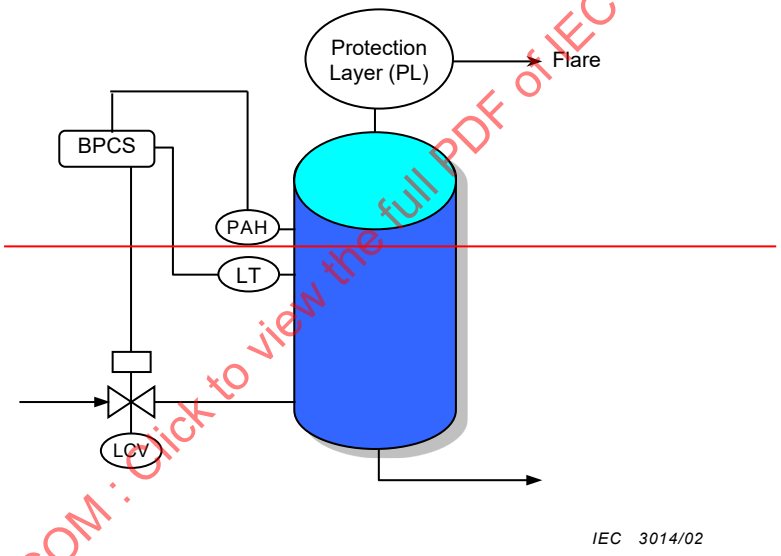
Annex B proposes the use of a semi-quantitative risk assessment technique to meet the objectives of the IEC 61511-1:2016, Clause 8. A technique is illustrated through a simple example.

B.3 Example

B.3.1 General

Consider a process comprised of a pressurized vessel with a pumped in feed and two exits (liquid and gas) containing a mixture of gas and 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~~ flow 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, which is a pressure relief valve, to address the hazards associated with high vessel pressure. Releases from the ~~protection layer~~ pressure relief valve 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~~ instrumented protection ~~layers~~ systems and associated operator~~(s)~~ action(s).



IEC 3014/02

~~Key~~

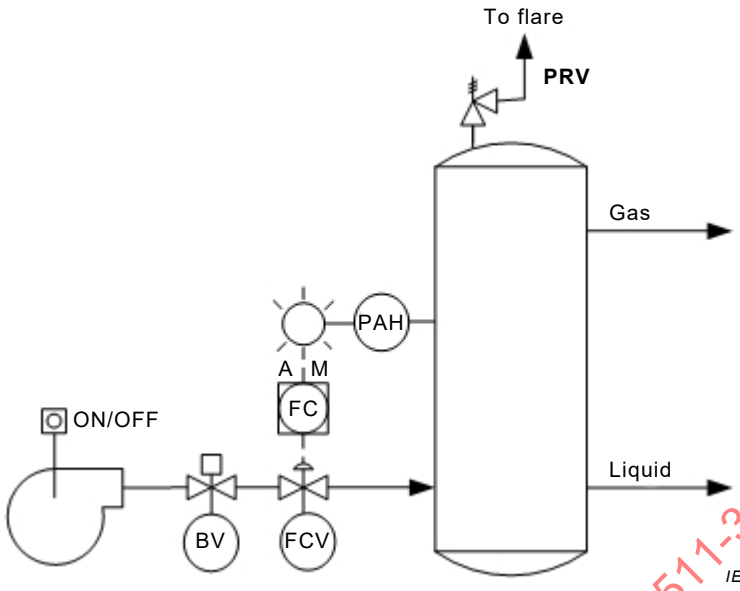
~~PL Protection Layer for additional mitigation (that is, dikes, pressure relief, restricted areas, holding tank)~~

~~PAH Pressure Alarm High~~

~~LT Level Transmitter~~

~~LCV Level Control Valve~~

~~BPCS Basic Process Control System~~



Key

FC	Flow controller
FCV	Flow control valve
PAH	Pressure alarm high
BV	Block valve
PRV	Pressure relief valve

Figure B.1 – Pressurized vessel with existing safety systems

B.3.2 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~~ (or 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.

B.3.3 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~~ High pressure is a process deviation that could propagate into a hazardous event that causes various scenarios 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	Deviations	Causes	Consequences	Safeguards	Action
	~~High level~~	~~Failure of BPCS~~	~~High pressure~~	~~Operator~~	
Vessel	High flow	Flow control loop fails	High flow leads to high pressure (see Note below)		
	High pressure	~~1) High level~~ 1) Flow control loop fails 2) External fire	Vessel damage and release to environment	~~1) Alarm, operator, protection layer~~ 1) High pressure alarm 2) Deluge system 3) Pressure relief valve	Evaluate design conditions for pressure relief valve release to environment
	Low/no flow	~~Failure of BPCS~~ Flow control ~~loop~~ fails	No consequence of interest		
	Reverse flow		No consequence of interest		

NOTE For this example, assume the vessel can experience high pressure due to the inability of the downstream equipment to handle full gas flow from the vessel when the feed flow is too high.

B.3.4 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.

a) Identify process hazards;

b) Identify initiating events;

c) Develop hazardous event scenarios for every initiating event;

d) Identify ~~safety~~ protection 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.~~ Safety functions are allocated to protection layers to safeguard a process and includes SIS and other risk reduction means (see Figure B.2).

NOTE 2 This step ~~2~~ applies to the above example since ~~this is~~ it involves an existing process ~~as given in the example~~ with existing protection layers.

e) Ascertain the frequency of occurrence of the initiating events and the reliability of existing safety ~~systems~~ functions using historical data or modelling techniques (for example, event tree analysis, failure modes and effects analysis, or fault tree analysis~~, Markov Modelling~~).

f) Quantify the frequency of occurrence of significant hazardous events;

g) Evaluate the consequences of all significant hazardous events;

h) Integrate the results (consequences and frequency of an accident) into risk assessment 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~~ function 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 led to the stated outcome and provides a system for life-cycle management.

For the illustrative example, one ~~initiating~~ hazardous event – over-pressurization – 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 B.3.4 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 SIF.

B.3.5 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 over-pressurization, is caused due to the failure of the ~~basic process control system (~~ BPCS~~)~~ (e.g., flow control loop), 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, and the frequency of external fire is considered to be negligible in comparison. 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~~ per year. Note that each cause shown in Figure B.2 is assumed to be independent (i.e., no overlapping) of other causes, with failure rate expressed as events per year.

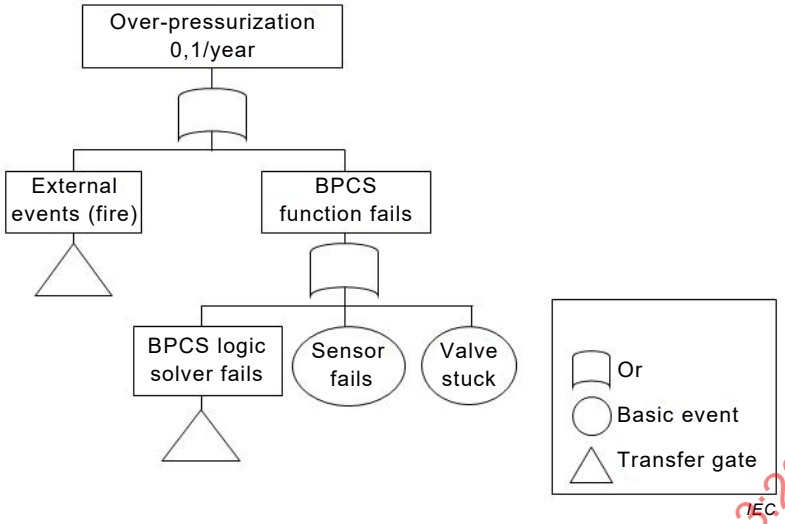


Figure B.2 – Fault tree for overpressure of the vessel

NOTE 1 Figure B.2 illustrates the fault tree without consideration of protective measures.

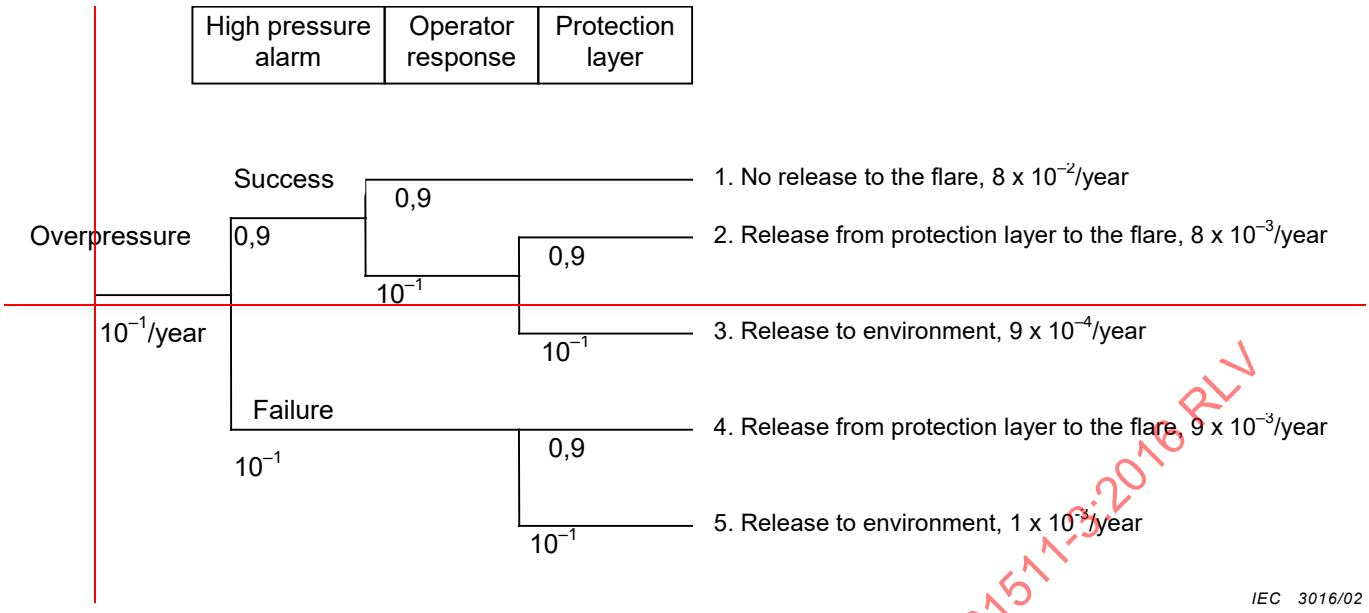
Once the frequency of occurrence of the initiating event has been established, the success or failure of the safety systems to respond to the abnormal condition is modelled using event tree analysis. The reliability data for the performance of the safety systems can be taken from field data, published 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.3 shows the potential ~~release~~ outcome scenarios that could ~~be developed~~ occur given an overpressure condition. The results of the ~~accident~~ event modelling are: a) the frequency of occurrence of each ~~accident~~ event sequence; and b) the qualitative consequences ~~in terms of release of flammable material~~ of the event outcome.

In Figure B.3, five ~~hazardous events~~ outcome scenarios are identified, each with a frequency of occurrence and a qualitative 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.~~ Outcome scenario 1 involves operator response to the high pressure alarm, occurs at a frequency of 8×10^{-2} per year and results in reduced production with no release. This is an acceptable design condition of the process and the operator is trained and tested on the appropriate response to achieve the risk reduction.

Furthermore, outcome scenarios 2 and 4 involve release of material to the flare, occurs at a combined frequency of $1{,}9 \times 10^{-2}$ per year ($9 \times 10^{-3} + 1 \times 10^{-2}$) and are also considered as a design condition of the process. The remaining outcome scenarios 3 and 5 have a combined frequency of occurrence of $1{,}9 \times 10^{-4}$ per year ($9 \times 10^{-5} + 1 \times 10^{-4}$) and result in vessel damage and release material to the environment (see Note 2).

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~~ flow sensor. Such common cause failure could lead to a significant increase in the ~~probability of failure on demand of the alarm system~~ frequency of occurrence for outcome 3 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.~~



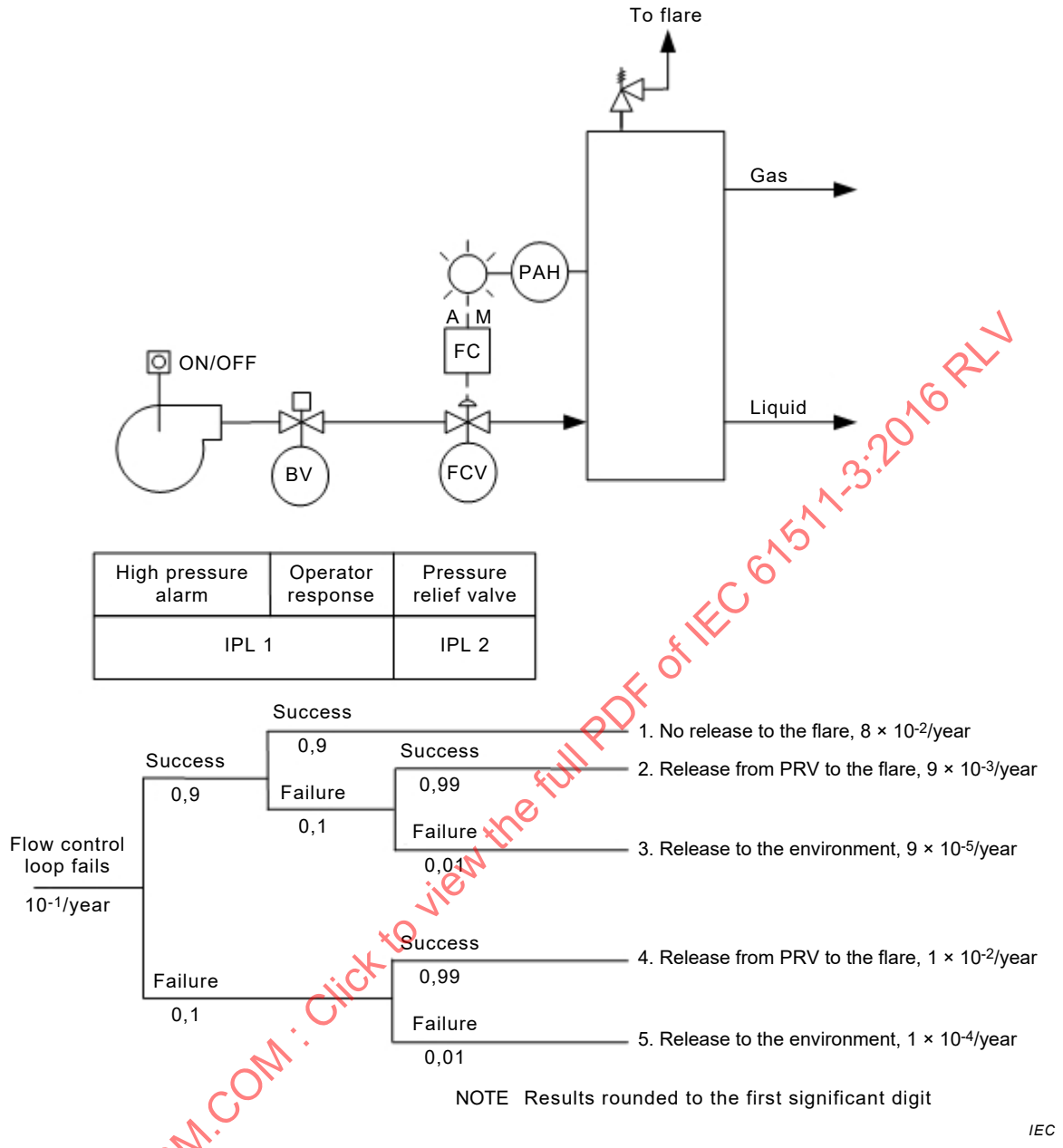


Figure B.3 –Hazardous events with existing safety systems

NOTE 2 In some applications the frequency and probability of failure on demand cannot be multiplied as shown in Figure B.3. This may be due to overlapping, common cause failure, and holistic dependencies between the various protection layers. See Annex J.

NOTE 3 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).

B.3.6 Events that do not meet the process safety target ~~level~~

As was stated earlier, plant specific guidelines establish the process safety target ~~level~~ as: no release of material to the environment with a frequency of occurrence greater than 10^{-4} in one year. The overall frequency of environmental releases is 9×10^{-5} (scenario 3) + $1{,}0 \times 10^{-4}$ (scenario 5) = $1{,}9 \times 10^{-4}$ per year, which is greater than the process safety target. Given the frequency of occurrence of the hazardous events and consequence data in Figure B.3,

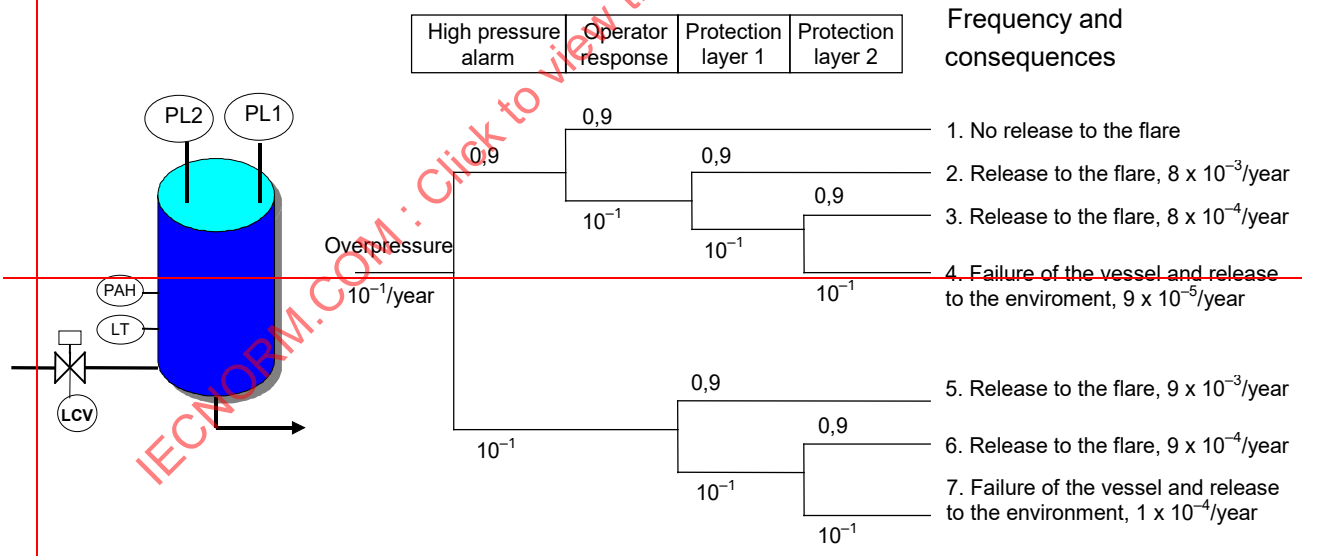
additional risk reduction is necessary in order for ~~accidents~~ outcome scenarios 3 and 5 to be below the process safety target ~~level~~.

B.3.7 Risk reduction using other protection layers

Protection layers of other technologies should be considered prior to establishing the need for a SIF 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.~~ A deluge system is listed as a safeguard in Table B.1, but it does not prevent the vessel damage or release to the environment.

~~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 $1{,}9 \times 10^{-4}$ 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.~~

Given that the intent of the analysis is to minimise the risk due to a release of material to the environment, it can be assumed that the deluge system is not an acceptable risk reduction scheme for vessel damage or release to the environment. The deluge system does reduce the risk to personnel and for event escalation, which is not being assessed in this example.



~~Figure B.4 – Hazardous events with redundant protection layer~~

B.3.8 Risk reduction using a safety instrumented function

The process 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 SIF ~~implemented in a SIS~~ is required to meet the process safety target ~~level~~. The new SIF is shown in Figure B.4.

It is not necessary at this point to perform a detail design on the SIF. A general SIF design concept is sufficient. The goal in this step is to determine if a new SIL 2 SIF will provide the required risk reduction and allow the achievement of the process safety target ~~level~~. Detail design of the SIF will occur after the process safety target ~~level~~ has been ~~achieved~~ defined for the SIF. For this example, the new SIF ~~can~~ uses dual, safety dedicated, pressure sensors in a 1oo2 configuration (not shown in Figure B.4) sending signals to a logic solver. The output of the logic solver controls ~~one additional~~ the shutdown valve and the pump.

NOTE 1oo2 means that either one of the pressure sensors can ~~send a signal to~~ initiate shutdown of the process.

The new SIL 2 SIF is used to minimize the frequency of a release from the pressurized vessel due to an overpressure. Figure B.4 presents the new ~~safety~~ protection 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 process safety target ~~level~~ can be met provided the SIF 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 ×10^{-5} per year, below the safety target of 10^{-4} per year.~~

In Figure B.4, seven outcome scenarios are identified, each with a frequency of occurrence and a qualitative statement of consequence. The frequency of outcome scenario 1 is the same as previously discussed. Operator response results in reduced production at a frequency of 8×10^{-2} per year.

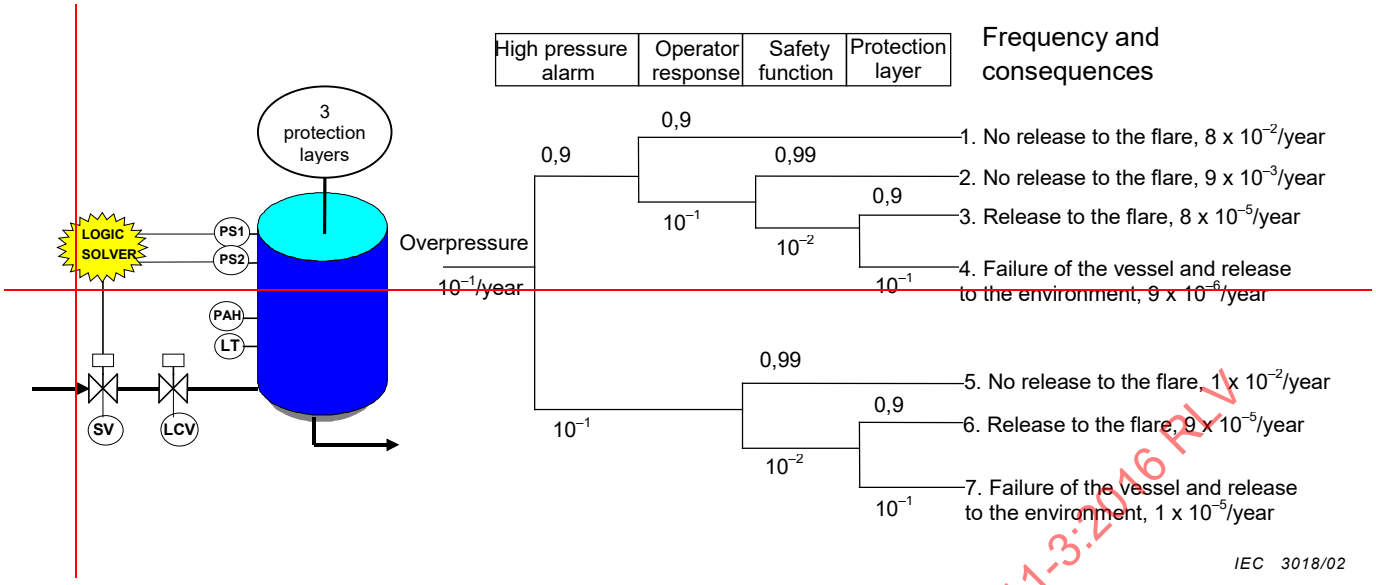
In this design case, successful operation of the SIS results in a shutdown of the process and occurs at a frequency of $1{,}9 \times 10^{-2}$ per year. The SIS reduces the process demand rate on the pressure relief valve. The frequency of scenario outcome 3 involving release from the PRV to the flare is reduced two orders of magnitude from the previous case to 9×10^{-5} per year. Scenario outcome 4, the hazardous event with release of material to the environment has a frequency of occurrence of 9×10^{-7} per year.

Scenario outcome 5 results in no release due to shutdown of the process by the SIS and occurs at a frequency of 1×10^{-2} per year. If the SIS fails to operate, the PRV provides the next safety function as shown in scenario outcome 6 and opens to the flare. The PRV opening occurs at a frequency of 1×10^{-4} per year. The total frequency of releases to the flare is determined by scenarios 3 and 6, which occur at an overall frequency of $9 \times 10^{-5} + 1 \times 10^{-4}$ or $1{,}9 \times 10^{-4}$. Releases from the flare are an acceptable design condition for the process. Scenario outcome 7 addresses the failure of all of the safety functions and occurs at 1×10^{-6} per year.

The total frequency of vessel failure with release to the environment (sum of frequencies of scenarios 4 and 7) has been reduced to 1,9 ×10^{-6} per year, below the process 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~~ and holistic dependencies between the high pressure alarm and the SIL 2 SIF. There may also be potential for common cause failure and holistic dependencies between ~~both of these protective arrangements and the failure of the BPCS level sensor~~ the safety functions and the failure of the BPCS flow sensor.

Such common cause failures may lead to a ~~highly~~ significant increase in the probability of failure on demand of the protective functions and hence ~~to~~ a 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.~~



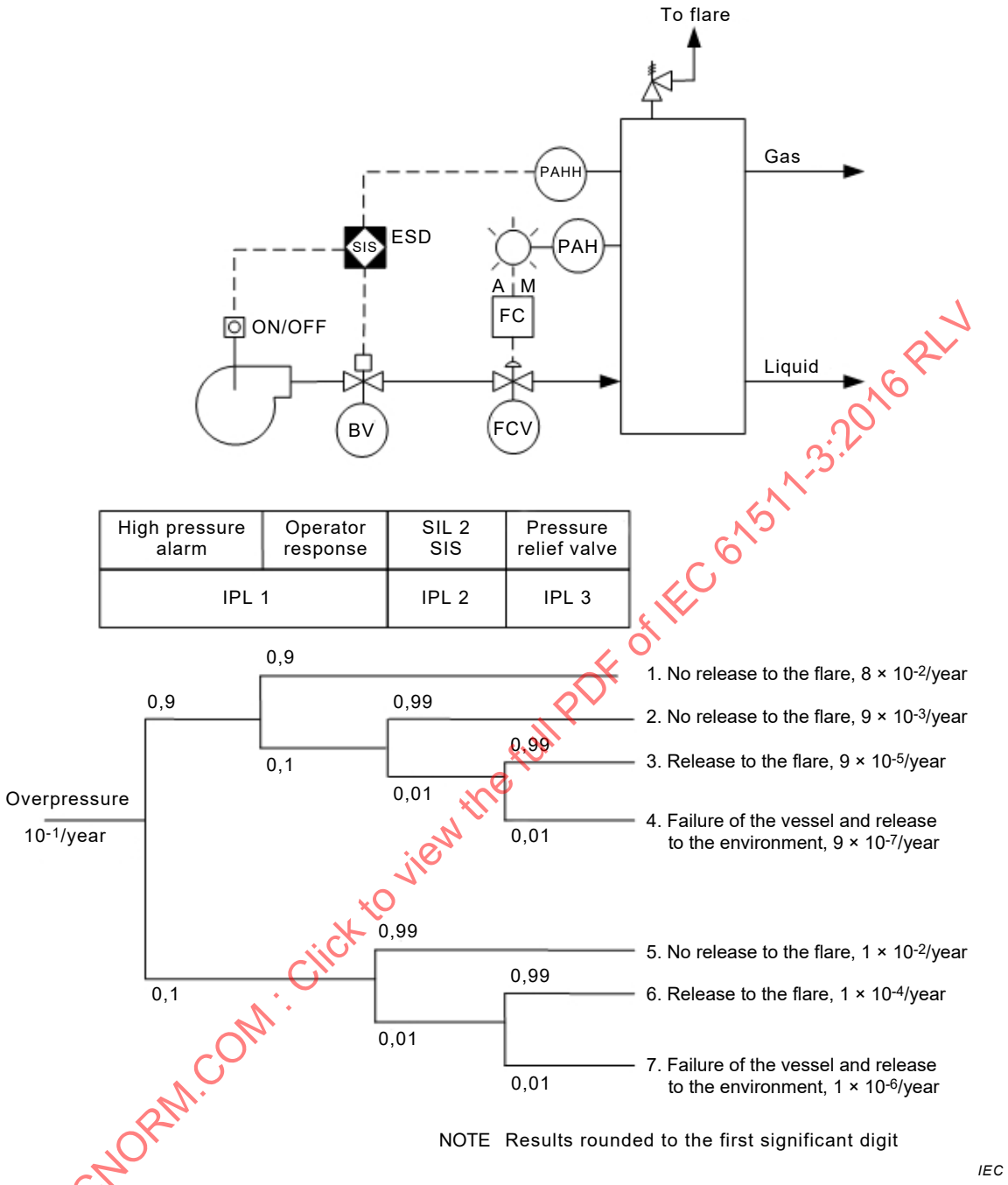


Figure B.4 –Hazardous events with SIL 2 ~~SIS~~ safety instrumented function

Annex C
(informative)

The safety layer matrix method

C.1 ~~Introduction~~ Overview

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 Figure C.1 below, 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.

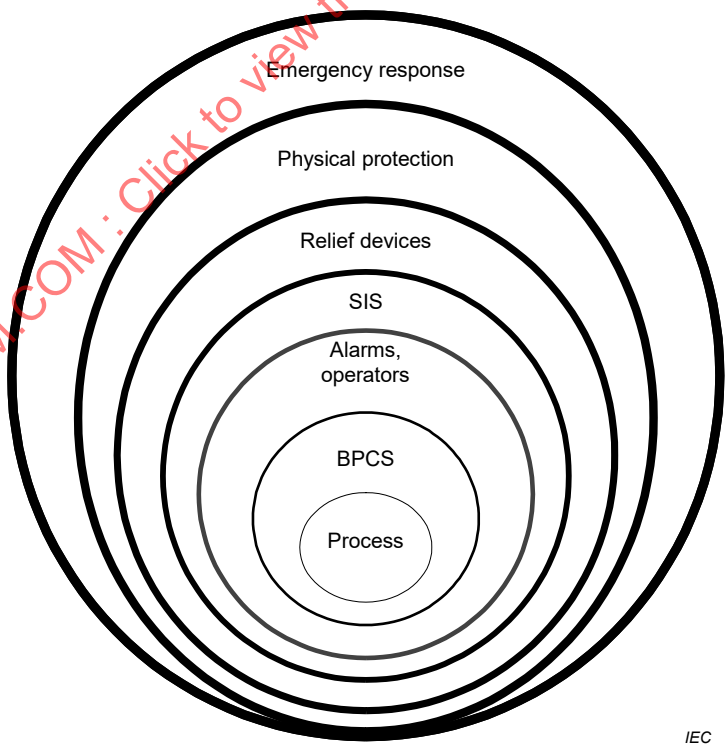


Figure C.1 – Protection layers

The concept of protection layers relies on three basic concepts:

a) 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.

b) 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 virtue of addressing both random failures and systematic failures in its design.

   • Auditability – a PL is designed to facilitate regular validation of the protective functions.

c) A safety instrumented ~~function~~ system (SIS) protection layer is a protection layer that meets the definition of a SIS in IEC 61511-1:2016 Clause 3.2.69 ("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

– *Layer of Protection Analysis-Simplified – Process risk assessment,* American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

– CCPS/AIChE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, Wiley-Interscience, New York (2007)

~~– 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~~

– ISA 84.91.01: *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industries*, The Instrumentation, Society of Automation, 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 (or tolerable risk) 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;
– 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.~~ HAZOP is detailed in such standards as IEC 61882:2001. 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. Guidewords 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 measures or ~~a~~ follow-up actions for management consideration.

Frequently, process experience and the HAZOP study results for a particular process can be generalized so as 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~~ assessment 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.

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

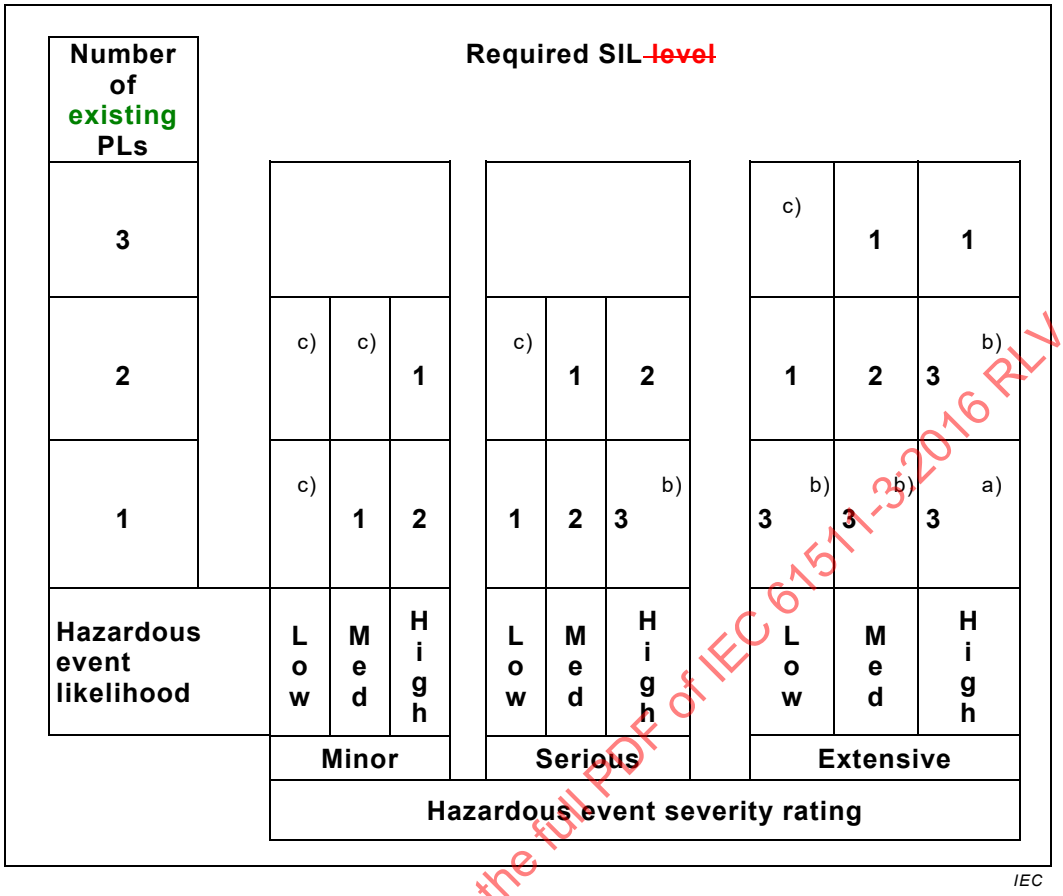
Type of events	Likelihood
	Qualitative ranking
Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels.	Low
Events such as dual instrument, valve failures, or major releases in loading/unloading areas.	Medium
Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	High
NOTE The system ~~should~~ can be in accordance with the IEC 61511-1:2016 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 process 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 process safety target ~~level~~.



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

b) One level SIL 3 SIF 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.

NOTE 1 Total number of PLs – includes all the PLs protecting the process including the SIS SIF being classified (i.e., number of PLs after the analysis is completed, including the new SIF (if required)).

NOTE 2 Hazardous event likelihood – refers to the likelihood that the hazardous event occurs without any of the PLs in service. See Table C.1 for guidance.

NOTE 3 Hazardous event severities – the impact associated with the hazardous event. See Table C.2 for guidance.

NOTE 4 This approach is not considered suitable for SIL 4.

Figure C.2 – Example of safety layer matrix

C.6 General procedure

a) Establish the process safety target level.

b) Perform a hazard identification (for example, HAZOP studies) to identify all hazardous events of interest.

c) Establish the hazardous event scenarios and estimate the hazardous event likelihood using company specific guidelines and data.

d) Establish the severity rating of the hazardous events using company specific guidelines.

e) Identify existing PLs (Figure C.2). The estimated likelihood of hazardous events should be reduced by a factor of 10 for every PL.

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

g) Identify the SIL from Figure C.2.

h) The user should adhere to Clause C.1 b).

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

Annex D
(informative)

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

D.1 ~~Introduction~~ Overview

Annex D is based on the general scheme of risk graph implementation described in Clause E.1 of IEC 61508-5:2010. Annex D has been adapted to be more suited to the needs of the process industry.

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

The approach uses a number of parameters, which together describe the nature of the hazardous situation when a SIS fails or is not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the SIL allocated to the SIF. 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 Annex D is to provide guidance on the above issues.

Annex D starts with protection against personnel hazards. It presents one possibility of applying the general risk graph of Figure E.1 of IEC 61508-5:2010 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 61511-1:2016). Typically, in the process sector, risk is a function of the following four parameters:

– the consequence of the hazardous ~~situation~~ event (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 SIF being considered) (W).

When a risk graph is used to determine the SIL 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 (see Table D.1) should represent the risk factors that relate best to the application characteristics involved. Consideration will also need to be given to the mapping of the SIL 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 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~~ can 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	Probability that exposed persons are able to avoid the hazardous situation which exists if the SIF 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 SIF 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:

a) 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.

b) To ensure the SIL selected for an application is in accordance with corporate risk criteria and takes into account risks from other sources.

c) 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 SIF under consideration. Each of the parameters is assigned a range of values such that when applied in combination, a graded assessment of the risk that 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 SIL. The relationship between the combinations of risk parameters and SIL is established by considering the tolerable risk associated with specific hazards. See Annex I as a description of the calibration process (Subclause I.2 and I.4.7).

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.

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~~ criterion for societal risk is based on the likelihood, *F*, of *N* or more 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. Guidance on developing criteria for risks giving rise to societal concerns is included in the UK HSE publication "Reducing Risks, Protecting People" ISBN 0 7176 2151 0.

The four risk parameters referred to in Clause D.2 are included in a decision tree of the form represented in Figure D.1. 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~~ SILs 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 SIL. 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.

The team normally considers each SIF in turn. The team will need comprehensive information on the process and the likely number of persons exposed to the risk. The team should include a person with previous experience of using the risk graph method and understands the basic concepts that the method is based on. The chairman should ensure that everyone feels free to ask questions and express views.

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~~ and relates to the probability of a fatality should the hazardous event occur, The P parameter is a measure that relates to preventing the ~~hazard~~ hazardous event. 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.

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.

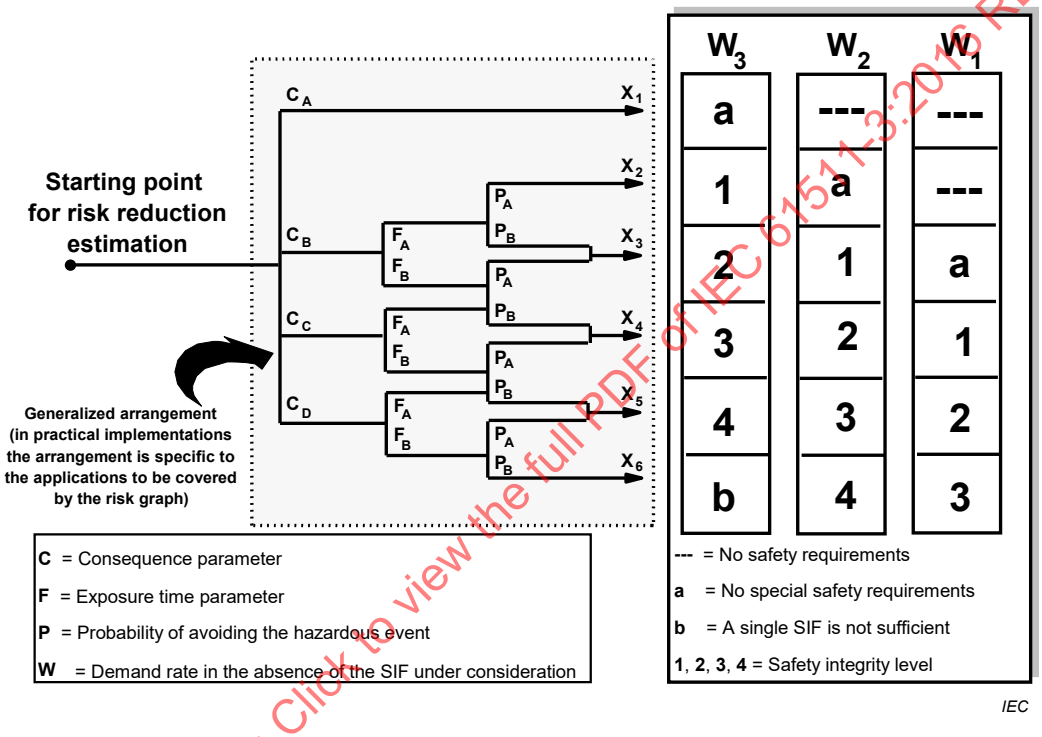


Figure D.1 – Risk graph: general scheme

Figure D.1 should not be used without re-calibration to align with site risk criteria. Any site without appropriate risk criteria should not attempt to use this method. The way in which calibration is carried out will depend on how the tolerable risk criteria are expressed. Parameter descriptions should be adjusted so that they fit with the range of intended applications and the risk tolerability. Values of C, F, P or W may be modified. Table D.2 shows an example calibration where the value of W is adjusted by a calibration factor D so as to align with specified risk criteria.

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

Risk parameter		Classification	Comments
Consequence (C) Number of fatalities 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. The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: 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	CA CB CC CD	Minor injury Range 0,01 to 0,1 Range >0,1 to 1,0 Range >1,0	a) The classification system has been developed to deal with injury and death to people. b) For the interpretation of CA, CB, CC and CD, the consequences of the accident and normal healing should be taken into account.
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 FA 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.	FA FB	Rare to more frequent exposure in the hazardous zone. Occupancy less than 0,1 Frequent to permanent exposure in the hazardous zone	c) See comment a) above.
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	PA PB	Adopted if all conditions in column 4 are satisfied Adopted if ~~all~~ any one of the conditions are not satisfied	d) PA 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 h 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.	W1	Demand rate less than 0,1 D per year	e) The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS.

Risk parameter		Classification	Comments
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. Demand rate (W) is equal to the demand rate on the SIF under consideration.	W2 W3	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	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 3.2.39.2 of IEC 61511-1:2016. f) D is a calibration factor, the value of which should be determined so that the risk graph results in a level of residual risk which is tolerable taking into consideration other risks to exposed persons and corporate criteria. The numeric values to be used against each value of W in the table should be derived by undertaking risk graph calibration as described in Clause D.3 or Annex I.
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~~ can be agreed with those involved, taking into account tolerable risk, see Clauses 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. Table D.3 shows consequences in environmental terms. 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.

Table D.3 – General environmental consequences

Risk parameter		Classification	Comments
Consequence (C)	CA	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
	CB	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
	CC	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
	CD	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. 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 although the value of the calibration factor D may need to be modified to align with environmental risk criteria.

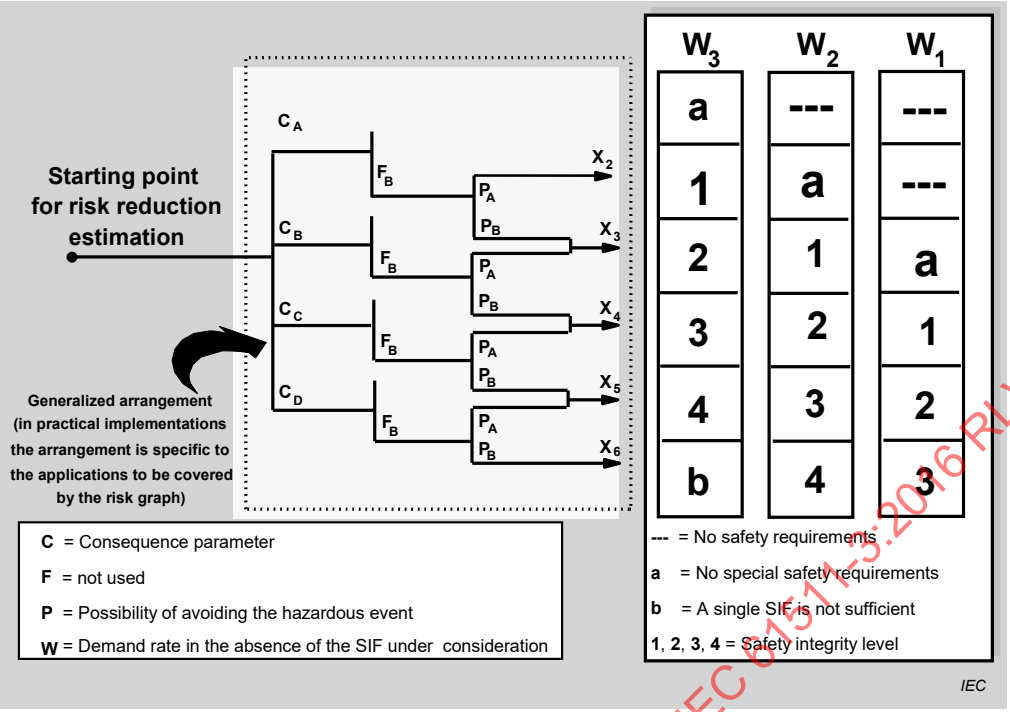


Figure D.2 – Risk graph: environmental loss

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 although the value of the calibration factor D may need to be modified to align with asset risk criteria.

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.

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*~~

Annex E describes the risk graph method for determining the safety integrity levels (SIL) of the safety instrumented functions (SIF). This is a qualitative method that enables the SIL of a SIF to be determined from knowledge of the risk factors associated with the process and basic process control system (BPCS).

The approach uses a number of parameters which together describe the nature of the hazardous situation when SISs fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the SIL allocated to the SIF. 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.~~

The method presented in Annex E is shown in more detail in VDI/VDE 2180 (2015).

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:

– BPCS;

– process monitoring systems;

– SIS.

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.

BPCS 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. BPCS are in continuous operation or frequently requested to act and intervene before the reaction of a SIS is necessary (BPCS systems do not normally need to be implemented according to the requirements of the IEC 61511-1:2016).

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 the IEC 61511-1:2016).

SIS either prevents a dangerous fault state of the process plant ("protection system") or reduces the consequences of a hazardous event.

If there is no SIS, a hazardous event leading to personnel injury is possible.

In contrast to the functions of a BPCS, the functions of SIS 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 SIS 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 SIS exists, although typical non-SIS 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 SIS in place (but all other ~~external~~ risk reduction ~~facilities~~ means are operating) – this is termed the probability of the unwanted occurrence.

This produces the following four risk parameters:

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

When a risk graph is used to determine the SIL of a SIF 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 SIL 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 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 ($S_1 < S_2 < S_3 < S_4$; $A_1 < A_2$; $G_1 < G_2$; $W_1 < W_2 < W_3$). 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 SIL required for it.

When determining the risk to be prevented by SIS, the risk has to be assumed without the existence of the SIS 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~~ VDI/VDE 2180, 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 SIS and therefore generally the more stringent the requirements and resulting measures.

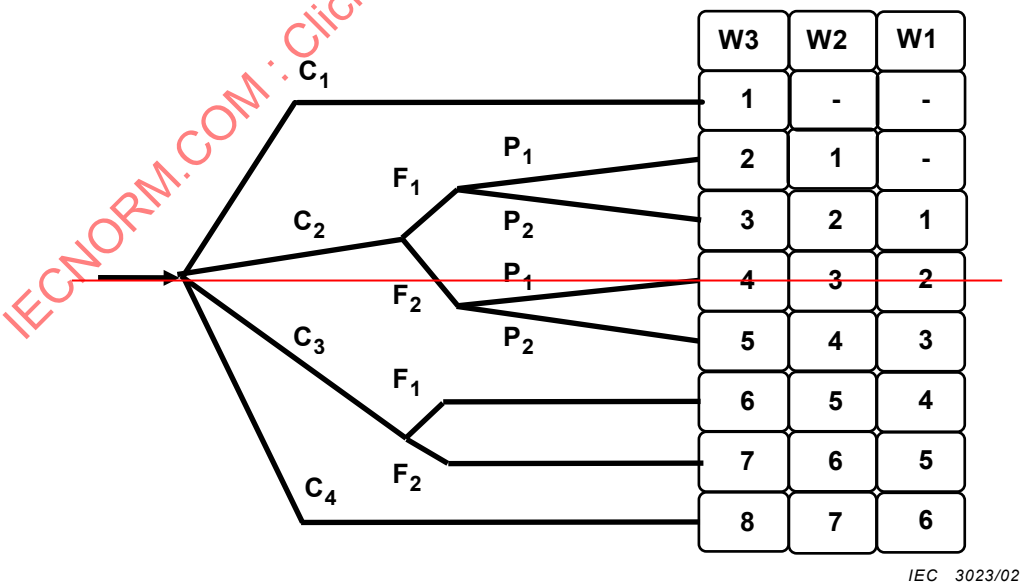
For the process industry, ~~requirement classes AK 7 and 8 are~~ SIL 4 is not covered by SIS alone. Non-process control measures are needed to reduce the risk to at least ~~requirement class AK 6~~ SIL 3.

~~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.~~

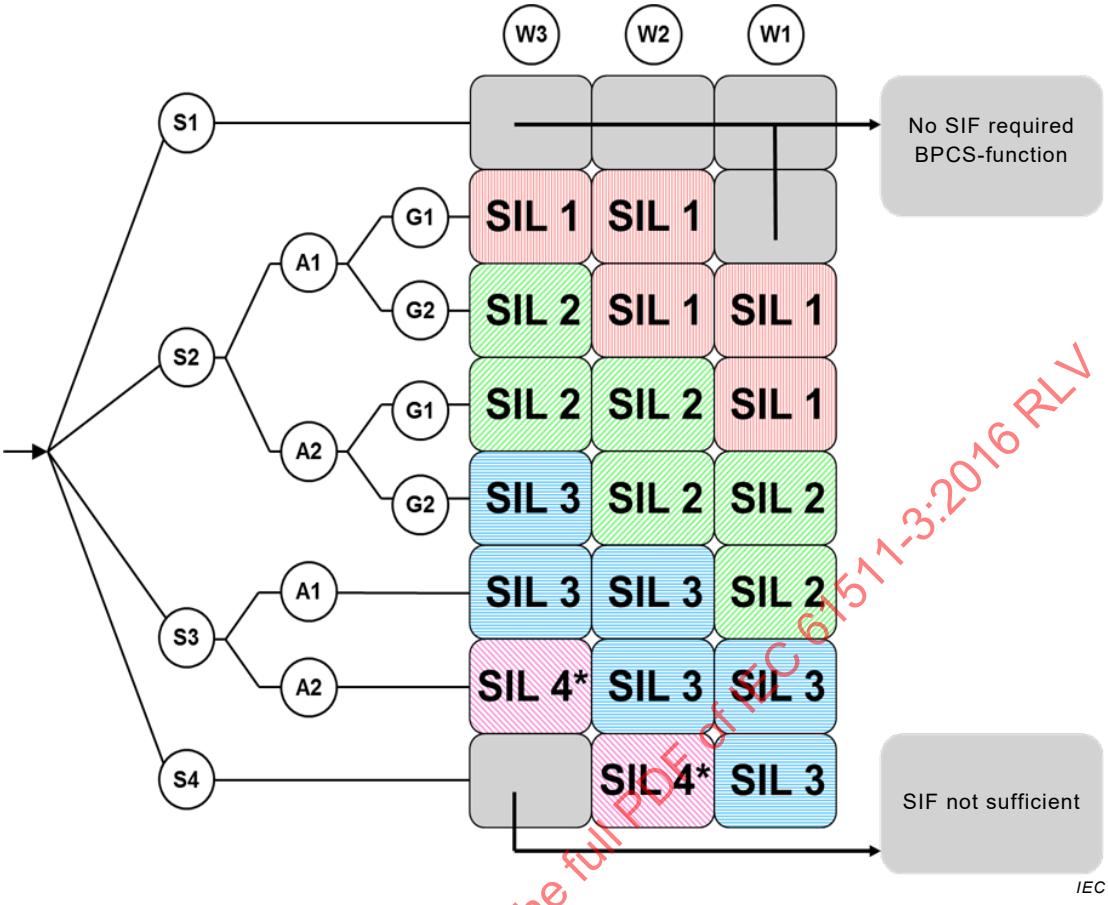
~~Risk area I: Lower risk to be covered (SIL 1 and 2)~~

~~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.~~



~~**Figure E.1 – DIN V 19250 risk graph – personnel protection (see Table E.1)**~~



Key: * = SIF not recommended

NOTE Different colours are used to facilitate identification of different SIL values.

Figure E.1 – VDI/VDE 2180 Risk graph – personnel protection and relationship to SILs

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

Risk parameter		Classification	Comments
Consequence of the hazardous event. Severity (S)	S1	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.
	S2	Serious permanent injury to one or more persons; death of one person	
	S3	Death of several persons	
	S4	Catastrophic effect, very many people killed	
Frequency of presence in the hazardous zone multiplied with the exposure time (A)	A1	Rare to more frequent exposure in the hazardous zone	2) See comment 1 above.
	A2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the consequences of the hazardous event (G)	G1	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); – 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).
	G2	Almost impossible	
Probability of the unwanted occurrence (W)	W1	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 SIS (E/E/PE or other technology) but including any external risk reduction facilities.
	W2	A slight probability that the unwanted occurrences occur and few unwanted occurrences are likely	
	W3	A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely	

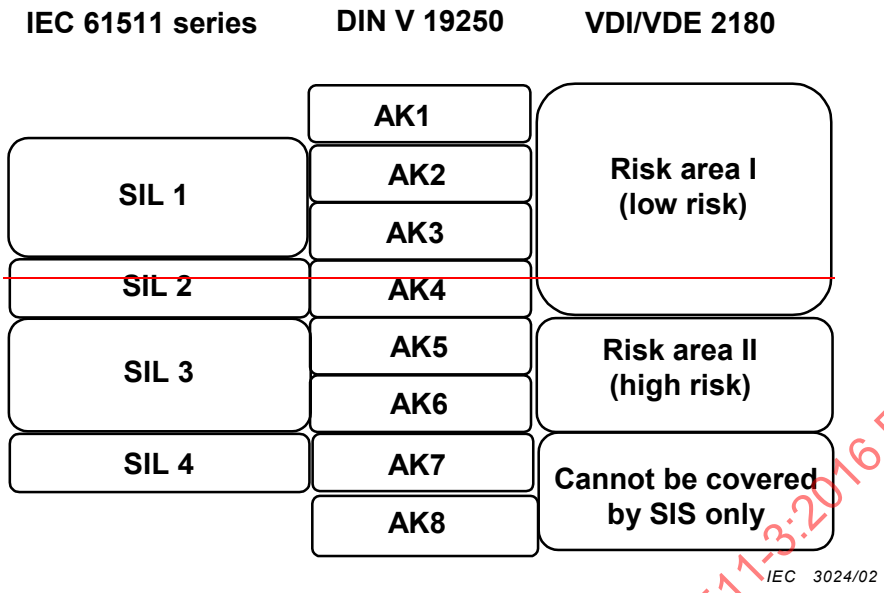


Figure E.2 – Relationship between IEC 61511 series, DIN 19250 and VDI/VDE 2180

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 clear and understandable terms to ensure consistency in the method application.

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

Annex F
(informative)

Layer of protection analysis (LOPA)

F.1 ~~Introduction~~ Overview

Annex F 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)~~ during hazard identification 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 SIF, the LOPA methodology allows the determination of the appropriate SIL for the SIF.

Annex F 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:

Guideline~~s~~ 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.

See also IEC 61511-2: -, Clause F.11 for example applications of LOPA.

The values illustrated in Annex F should not be taken as generic and used in specific layer of protection analysis applications.

~~F.2 Layer of protection analysis~~

The SIS safety life-cycle defined in IEC 61511-1:2016 requires the determination of a SIL 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 the SIL of the SIF. 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)~~ identification process. Table F.1 shows the relationship between the data required for the Layer of Protection Analysis (LOPA) and the data developed during the hazard identification process (HAZOP study for this example). Figure F.1 shows a typical spreadsheet that can be used for the LOPA.

LOPA analyses hazards to determine if SIFs are required and if so, the required SIL of each SIF.

F.2 Impact event

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

F.3 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.

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.2 F.13.2	Severity level F.3 F.13.2	Initiating cause F.4 F.13.3	Initiation likelihood per year F.5 F.13.4	General process design F.13.5	BPCS F.13.6	Alarms, etc. F.13.7	Additional mitigation, restricted access,F.7 F.13.8	IPL additional mitigation dikes, pressure relief F.7 F.13.9	Inter-mediate event likelihood per year F.9 F.13.10	SIF integrity level F.10 F.13.11	Mitigated event likelihood per year F.11 F.13.11	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV ~~01~~ 0,01	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	0,1	PRV ~~01~~ 0,01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC

Key

~~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

NOTE If independent protection layers have not been properly selected frequency and probability of failure on demand cannot be multiplied as shown in Figure F.1. See Annex J.

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.4 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.5 Initiation likelihood

Likelihood values of the initiating causes occurring, in events per year, are entered into column 4 of Figure F.1. Table F.3 shows typical initiating cause likelihoods. The experience of the team is very important in determining the initiating cause likelihood.

Values in Table F.3 are not to be used for specific assessments (see Note 1).

Table F.3 – 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	$f < 10^{-4}$, /year
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	$10^{-4} < f < 10^{-2}$, /year
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	$10^{-2} < f < 100$, /year
NOTE 1 This table is illustrative. These values cannot be taken as generic frequencies and cannot be used in specific assessments. NOTE 2 "*f*" = Initiating event frequency (initiating event likelihood).		

F.6 Protection layers

Figure 2 in Clause 1 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.8).

Process design to reduce the likelihood of an impact event from occurring, when an initiating cause occurs, is 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 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.4.

Values in Table F.4 are not to be used for specific assessments (see Note).

Table F.4 – Typical protection layers (prevention and mitigation) PFD~~s~~$_{avg}$

Protection layer	PFD_{avg}
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	~~$1,0 \times 10^{-2}$ to $1,0 \times 10^{-4}$~~ $1,0 \times 10^{-1}$ to $1,0 \times 10^{-2}$
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)

NOTE The figures in Table F.4 are illustrative of the range of values that could appear in assessments. These values cannot be taken as generic probabilities and used in specific assessments. Human error probabilities can be appropriately assessed on a case by case basis.

F.7 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 PFD~~s~~$_{avg}$ for all mitigation layers and list them in column 6 of Figure F.1.

F.8 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~~ 10-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;
  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 (IPL).

F.9 Intermediate event likelihood

The intermediate event likelihood is calculated by multiplying the initiating likelihood (column 4 of Figure F.1) by the PFD~~s~~$_{avg}$ 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~~ process safety target level 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 SIS are applied. If inherently safe design changes can be made, Figure F.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.10 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.11 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.12 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) × (probability of ignition) × (probability of a person in the area) × (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) × (probability of a person in the area) × (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.

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.13 Example

F.13.1 General

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

F.13.2 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 of Figure F.1, respectively.

F.13.3 Initiating cause

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 of Figure F.1.

F.13.4 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 of 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.13.5 ~~Protection layers~~ General process 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 of Figure F.1 under process design.

F.13.6 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 of Figure F.1 under BPCS (0,1 is the minimum allowable for the BPCS).

F.13.7 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 of Figure F.1 under alarms.

F.13.8 Additional mitigation

Access to the operating area is restricted during process operation. Maintenance is only performed during periods of equipment shutdown and lockout. 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 of Figure F.1 under additional mitigation and risk reduction.

F.13.9 Independent protection ~~level~~ layer(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~~ plugging 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 of Figure F.1 and assigned a PFD_{avg} of 0,01 based on previously discussed operating experience and published industry data.

F.13.10 Intermediate event likelihood

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

F.13.11 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 of 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 of Figure F.1.

F.13.12 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 of Figure F.1 under initiation likelihood.

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 of 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) × (Probability of fatal injury due to fire) = 0,5.

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.

Annex G
(informative)

Layer of protection analysis using a risk matrix

G.1 Overview

Annex G describes a hazard and risk assessment method that uses layer of protection analysis (LOPA) to identify the safety functions that reduce the frequency of loss of primary containment (LOPC) events to a tolerable level. The method encourages the implementation of proactive safeguards that prevent the LOPC, but allows the consideration of consequence mitigation systems as necessary. When consequence mitigation systems are implemented, the method requires the explicit examination of the outcome resulting from the mitigation system deployment. Since the method does not determine the frequency of harm posed by the LOPC, this method does not consider post-release conditions, such as the probability of ignition or occupancy. This simplifies the method and focuses the assessment team on reducing LOPC events through inherently safer design and proactive layers of protection.

This method uses a risk matrix to communicate the risk criteria to the assessment team. The risk matrix has been calibrated to account for the consequence severity potentially posed by the LOPC event. The criteria include consideration for safety, environmental, and economic loss potential.

The method examines hazardous events identified using any hazard identification technique appropriate for the process lifecycle step. At a minimum, the hazard identification should describe the hazardous events that were assessed and should identify the initiating cause(s) and the safeguard(s) that prevent or mitigate the event(s).

The risk assessment is performed using LOPA where the process risk is determined and compared to a tolerable risk as defined by a semi-quantitative risk matrix. When the process risk is above tolerable, safety functions are identified and allocated to independent protection layers (IPLs) as shown in Figure G.1 (adapted from CCPS, 2007). Some IPLs are proactive and act to prevent the hazardous event from occurring. Others are reactive and act to reduce the harm caused by the hazardous event.

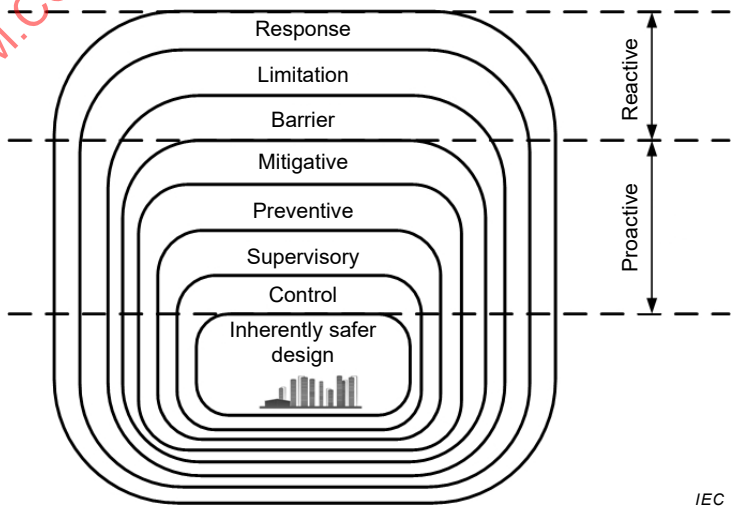


Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL

This method encourages the selection of proactive IPL, which reduce the frequency of the hazardous event (e.g., loss of containment or equipment damage). The use of any protection layer requires the additional consideration of the secondary consequence that results from their successful operation. This is particularly true of mitigative layer IPLs – see step 7 below.

When the study is completed, the identified safety functions have been allocated risk reduction in accordance with guidelines that are established for each type of IPL and associated function. When risk reduction is allocated to a SIS, this risk reduction yields a SIL in accordance with IEC 61511-1:2016 Table 4.

This method does not consider the duration of the operating mode when analysing sequenced, batch, start-up or maintenance risk. In this method, the risk of each operating mode should be reduced to the tolerable frequency regardless of the amount of time the process is in a particular operating mode.

The tolerable frequency for a hazardous event is determined by assessing the worse credible scenario consequence in terms of the health and safety impact to plant personnel and the public, environmental impact, and economic impact (property and business losses). The team is expected to qualitatively estimate the worst credible consequence regardless of likelihood and identify IPLs to reduce the event risk. Again, since this method seeks to reduce the hazardous event frequency (e.g., loss of primary containment or equipment damage), this method does not consider the use of conditional modifiers for occupancy, ignition or fatality, which are typically used to assess the frequency of specific types of harm caused by the event.

NOTE 1 This method leverages the availability of the team and information to assess economic impact of loss of containment events. The implementation of any recommendations for economic-related events is determined by business approval processes.

NOTE 2 The frequency, probability and risk reduction values used are for illustration only and are not to be used as generic values for specific assessments.

Annex G 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 references:

Layer of Protection Analysis Simplified – Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7.

Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design, Welding Research Council, PO Box 1942, New York, NY 10156, 2005, ISBN 1-58145-505-4.

Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system, American Petroleum Institute, 1220 L Street, NW, Washington, D.C. 20005, 2007.

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2007, ISBN 0-4719-7940-6.

Guidelines for Initiating Events and Independent Protection Layers in LOPA, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2015, ISBN: 978-0-470-34385-2.

G.2 Procedure

G.2.1 General

This LOPA procedure results in the identification of the IPLs that can reduce the process risk in accordance with the risk criteria. The following is a step-by-step description of the work process, which is shown graphically in Figure G.2.

G.2.2 Step 1: General Information and node definition

The team members, attendance date, study date, and document revision number are recorded in the Worksheet. The facilitator reviews the node boundary to ensure that each team member is familiar with the process operation and flow sheet (Figure G.3). The P&IDs under review are recorded along with any other documentation reviewed by the team during the study.

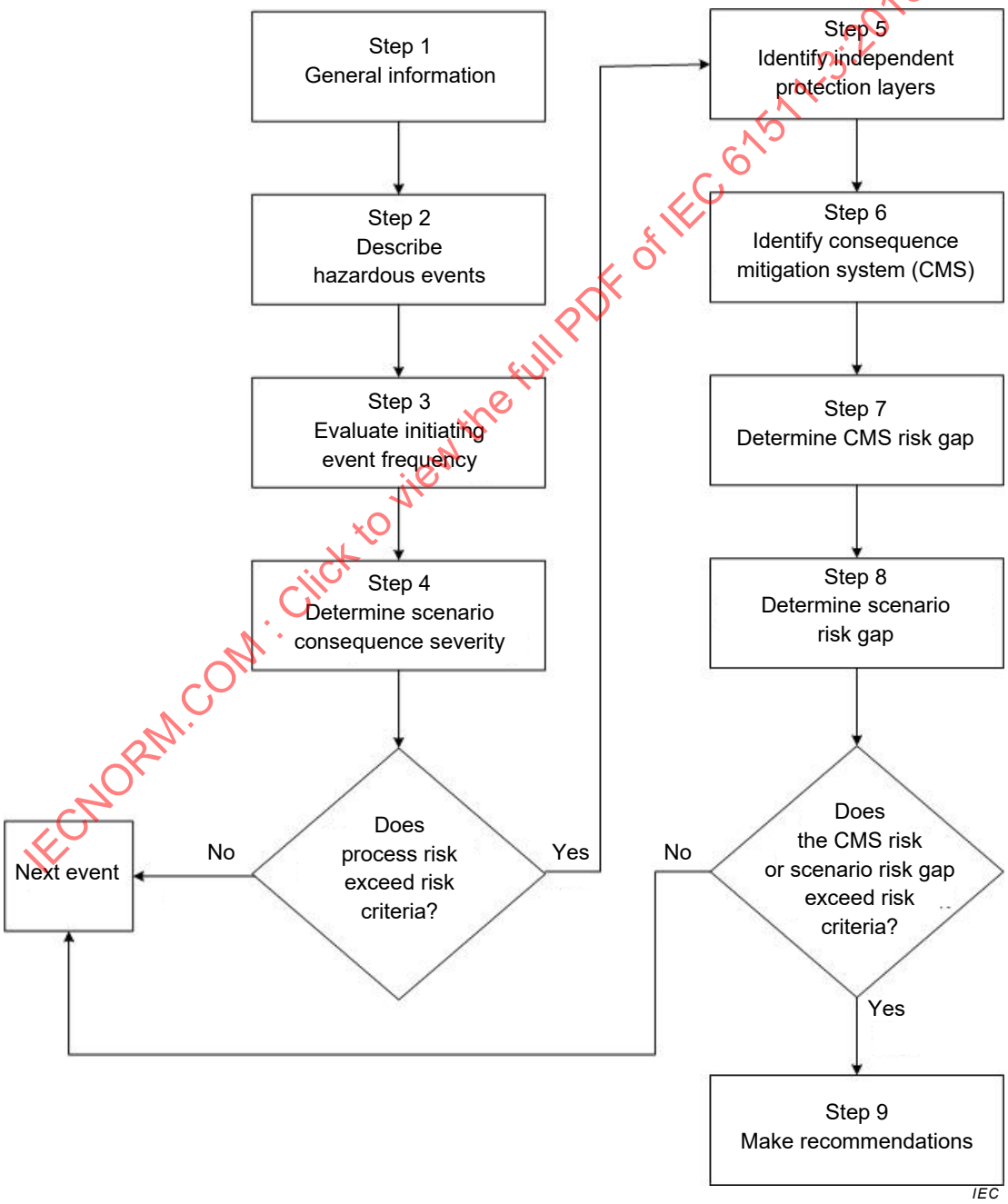
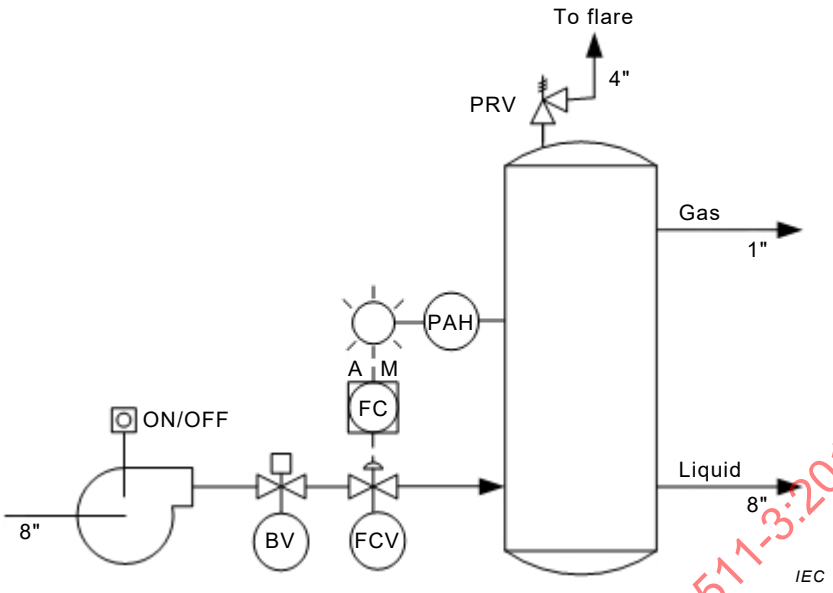


Figure G.2 – Work process used for Annex G



Key

FC	Flow controller
FCV	Flow control valve
PAH	Pressure alarm high
BV	Block valve
PRV	Pressure relief valve

Figure G.3 – Example process node boundary for selected scenario

G.2.3 Step 2: Describe hazardous event

Deviation or What-if? or FMEA: The team should describe the hazardous event selected for review including the deviation, what-if question, or failure mode that was analysed during the hazard identification and how the event propagates to the loss of containment or equipment damage.

Table G.1 is an excerpt from a HAZOP performed on the node illustrated by Figure G.3. This is one of what may be many scenarios that result in overpressure in this process unit. This scenario was selected for illustration purposes.

Hazardous event description: The event propagation should be clearly, yet concisely, described from the process hazard to the worst credible consequence assuming no safeguards. It is important to thoroughly describe the hazardous event, so that each team member understands what is being analysed. It should also be recognized that this documentation assists in the management of change process and in future revalidations, so it is important that the description be clear and easily understood.

As an example, Table G.2 lists a high-pressure deviation that is caused by a flow control loop failure and results in pressure that exceeds the Maximum Allowable Working Pressure (MAWP) of the vessel. The consequence is stated as “High flow leads to pressures above 1,5 × MAWP. Potential vessel damage and release to environment within 5 minutes.” (Note that this 1,5 MAWP is only allowed by certain vessel design codes). This description provides later teams with an understanding of the degree of overpressure and the speed with which pressure propagates to an unacceptable level.

Table G.1 – Selected scenario from HAZOP worksheet

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Causes	Consequence	Rank Consequence		Safeguards	Risk Ranking		PHA Recommendation
			Cat	S		L	RR	
1. High pressure	1. Flow control loop fails	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes.	S	4	1. High pressure alarm	B	2	
			E	4		B	2	
			A	3	2. High pressure shutdown of inlet block valve	B	1	
					3. Pressure relief valve			
					4. Operator response to high pressure alarm			

NOTE See Table G.4 for consequence categories and severity ranking.

Table G.2 – Selected scenario from LOPA worksheet

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity(S) and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes.	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1.Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	10
		E	4	1 000								
		A	3	100								

NOTE See Table G.4 for consequence categories and severity ranking.

Table G.2 continued at step 6

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+ CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. None, Vents to flare	100	S	1	TR	10	TR	1 000	1000	TR		
			E	1	TR		TR	1 000		TR		
			A	1	TR		TR	100		TR		

G.2.4 Step 3: Evaluate initiating event frequency

Once the hazardous event is described, the initiating cause(s) that lead to the hazardous event are documented. An event may be initiated by a single initiating cause or multiple causes. The team should consider various types of causes, such as human error, equipment failures, procedural errors, etc.

There may be instances where the team deems there is no credible cause or combination of causes. This may be due to inherently safe process design or because the occurrence of the scenario would violate the laws of chemistry or physics. In these cases “No credible initiating cause” should be listed in the initiating cause portion of the worksheet along with an explanation of the reasoning, and the team should continue to the next scenario.

Frequency: The frequency of the initiating event is evaluated without the consideration of any IPLs (safeguards). Guidance is provided in Table G.3 based on industry published data and good engineering practice. The team should determine whether the data is appropriate based on plant historical performance or experience with the initiating cause(s) under similar plant conditions. If the team determines that a higher frequency is warranted (e.g., 1/year rather than 1/10 years), the reasoning is documented and the revised number is entered into the worksheet. In this example, the frequency of flow control loop failure is 1/10 years.

Enabling conditions: Some process deviations can lead to hazardous events only in the presence of a co-incident condition, called an enabling condition. This procedure allows the consideration of an enabling condition, when the condition is independent of the initiating cause and is necessary for propagation of the hazardous event. The combination of the enabling condition and the initiating cause results in the propagation of the hazardous event.

The frequency of the initiating event can be estimated based on the average probability of the enabling condition being present and the frequency of the initiating cause. As an example, if the operator leaves a valve open incorrectly and a process upset downstream occurs, there could be backflow through the open valve. The process upset is assumed to happen 1/year. An operator opens and closes the valve 3 times per day. Failure is assumed 1/100 opportunities. Valve position is verified every 8 hours (by the next shift operator). So the average probability of the valve being open is:

P_{avg}(open) = (3/24 hours) × (1/100) × 8 hours = 0,01

The initiating event frequency is 0,01 × 1/year = 1/100 years.

Overall frequency. The overall event frequency is the highest frequency of the listed initiating causes. If a hazardous event has more than 3 initiating causes of similar frequency, consideration is given to assigning a higher overall event frequency based on an analysis of the common cause aspects of the causes. In the example (Table G.2), there is only one cause listed, so the initiating event frequency is 1/10 year.

Table G.3 – Example initiating causes and associated frequency

Initiating cause	Conditions	MTBF[a] in years
Basic Process Control Loop (BPCS)	Complete instrumented loop, including the sensor, controller, and final element.	10
Operator Action (SOP)	Action is performed daily or weekly per procedure. The operator is trained on the required action. {This value can be reduced by a factor of 10 (value=1 in 10 years) based on experience. The team should document job aids, procedures, and/or training used to achieve 1 in 10 years.}	1
	Action is performed monthly to quarterly per procedure. The operator is trained on the required action.	10
	Action is performed yearly, after turnaround or temporary shutdown per procedure. The operator is trained on the required action.	100
Instrumented Safety Device (OTHER)	Instrumented safety device spuriously operates, e.g., closure of block valve, pump shutdown, and opening of vent valve.	10

[a] The initiating causes listed can be assumed to occur more frequently (e.g., changed from 1/100 year to 1/10 year based on process experience. The values cannot be made less frequent without additional justification and approval by process safety. Additional analysis should be submitted as part of the justification. This would include human factors analysis, failure modes and effects analysis (FMEA), event tree analysis or fault tree analysis.

G.2.5 Step 4: Determine hazardous event consequence severity and risk reduction factor

The hazardous event is assessed to determine the worst credible consequence in terms of the health and safety impact to plant personnel and the public, environmental impact, and economic impact (property and business losses).

Severity: The consequence severity is assessed according to standardized definitions in Table G.4 "Consequence severity decision table". In the example (see Table G.2), the team determined that there was the potential for a significant flammable hydrocarbon release. Since an operator made frequent rounds through the unit, a fatality was possible. The consequence severity for safety was ranked as “4.” The environmental severity ranking was also determined to be consequence level 4, while the asset severity ranking was consequence level 3.

Risk assessment: The process risk is determined by the overall initiating event frequency (Step 3) and consequence severity (Step 4). These ranking are used as input to Table G.8 Risk reduction factor matrix. The matrix shows the risk reduction factor (RRF) required to reduce the process risk to a tolerable level. If the RRF yields a result of TR (tolerable risk), the risk falls within the risk criteria without additional IPLs. Those hazardous events that indicate other than TR should be assessed further.

In the example (see Table G.2), a consequence severity of 4 and a frequency of 1/10 years results in a required risk reduction of 1 000 (see Table G.5).

In some instances, IPLs may not be required from a risk standpoint, but may be required by code, practice, or regulation. The requirements of codes, practices, or regulations supersede this procedure.

Table G.4 – Consequence severity decision table

RANK	SAFETY (S)	ENVIRONMENTAL (E)	ASSET (A)
5	Multiple fatalities across a facility and/or Injuries or fatalities to the public	Catastrophic off-site environmental damage with long-term containment and clean-up	Expected loss greater than $10,000,000 and/or substantial damage to buildings located off-site
4	Hospitalization of three or more personnel (e.g., serious burns, broken bones) and/or one or more fatalities within a unit or local area and/or Injuries to the public	Significant off-site environmental damage (e.g., substantial harm to wildlife) with prolonged containment and clean-up	Expected loss between $1,000,000 and $10,000,000 and/or extended downtime with significant impact to the facility operation and/or minor damage (e.g., broken windows) to buildings located off-site
3	Hospitalization injury (e.g., serious burns, broken bones) and/or multiple lost work day injuries and/or Injury to the public	On-site release requiring containment and clean-up and/or off-site release causing environmental damage with quick clean-up	Expected loss between $100,000 And $1,000,000 and/or downtime of several days severely impacting the facility operation
2	Lost work day injury and/or recordable injuries (e.g., skin rashes, cuts, burns) and/or minor impact to public	On-site release requiring containment and clean-up by emergency personnel and/or off-site release (e.g., odour) but no environmental damage	Expected loss between $10,000 and $100,000 and/or downtime of more than day causing impact to facility operation and/or reportable quantity event
1	Recordable injury and/or no impact to the public	On-site release requiring containment and clean-up by on-site personnel	Expected loss of less than $10,000 and/or downtime of less than a day with minor impact to the facility operation

Table G.5 – Risk reduction factor matrix

		REQUIRED RISK REDUCTION FACTOR				
CONSEQUENCE SEVERITY	5	100 000	10 000	1 000	100	10
	4	10 000	1 000	100	10	TR
	3	1 000	100	10	TR	TR
	2	100	10	TR	TR	TR
	1	10	TR	TR	TR	TR
		1	10	100	1 000	10 000
		FREQUENCY (1 in x years)				

G.2.6 Step 5: Identify independent protection layers and risk reduction factor

Safeguards are identified during the H&RA, which provide some measure of protection against the hazardous event under review. Each identified safeguard is evaluated against the IPL criteria.

Not all safeguards meet the design and management criteria necessary to be classified as IPLs. It is also important to ensure adequate independence of the selected safeguards so that the potential for common cause, common mode, and systematic issues is sufficiently low compared to the overall risk reduction requirement.

Table G.6 provides guidance on the RRF for example safety functions that may be classified as IPLs. The risk reduction factor is based on specific IPL design and management criteria,

which is briefly described in Table G.6. The restrictions provided in the table shall be met for the IPL to be allocated the listed risk reduction.

A safeguard that does not meet the criteria may be listed in the worksheet with RRF=1, if desired. A safeguard may only be allocated a RRF>1, when the process safety information demonstrates that the safeguard meets the criteria.

In the example (see Table G.2), the team determined that there was not sufficient time for the operator to respond to the alarm. A previous analysis of the SIS showed that it achieved SIL 1, so the team allocated an RRF of 10 to it (see Table G.2).

G.2.7 Step 6: Identify consequence mitigation systems and risk reduction factor

The successful action of any IPL results in a new operating or shutdown state. This new state is referred to as the secondary consequence of the IPL. The risk associated with the secondary consequence shall be acceptable or additional/alternate IPL shall be applied. Since successful action of most mitigative proactive IPL and reactive IPL result in the reduction of the consequence severity, these IPL are collectively referred to as Consequence Mitigation Systems (CMSs).

CMS IPL, which act to reduce the harm resulting from the hazardous event, may be credited if a review (Note 1) verifies that the CMS IPL is designed and managed to address the particular hazardous event and (Note 2) determines that the secondary consequence risk is acceptably managed.

NOTE 1 If there are no documents to support the claim that the CMS IPL is properly designed, located, and maintained to reduce the consequence of the particular release scenario, no RRF may be taken.

NOTE 2 The successful action of a CMS IPL reduces the consequence of the hazardous event under review. The reduced consequence resulting from the proper functioning of the CMS IPL can still be unacceptable. The risk associated with the IPL's operation is determined by evaluating this secondary consequence severity and release frequency. This value is compared to the risk criteria to determine if additional risk reduction is required.

Table G.7 lists the CMSs considered during study and RRF for specific safety functions that may be classified as IPLs. It is important for the team to review the CMS to verify that the CMS is designed and managed to address the hazard scenario. Only CMS that proactively reduce the frequency of the primary consequence event (LOPC) are considered in this method.

In this example (see Table G.2), the team determined that the pressure relief valve was designed for overpressure caused by flow control loop failure. The team allocated an RRF of 100 to it.

Table G.6 – Examples of independent protection layers (IPL) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)

IPL	Conditions	RRF	PFD
Basic Process Control System (BPCS)	The BPCS IPL should be designed and managed to achieve the RRF. It is a typically a control loop whose normal action prevent the scenario. The BPCS IPL shall run in automatic mode during all operating phases where the hazard scenario could occur.	10	0,1
Operator response to alarm with ≥10 minutes response time (ALARM)	Operator response does not have to perform troubleshooting or diagnostics to take the action. Alarm may be implemented in the BPCS or independent of the BPCS.	10	0,1
Operator response to alarm with ≥40 minutes response time (ALARM)	Operator response requires minor troubleshooting or diagnostics prior to taking action. Alarm may be implemented in the BPCS or independent of the BPCS.	10	0,1
SIL 1 (SIS)	Safety Integrity Level 1	10	0,1
SIL 2 (SIS)	Safety Integrity Level 2	100	0,01
SIL 3 (SIS)	Safety Integrity Level 3	1 000	0,001

Table G.7 – Examples of consequence mitigation system (CMS) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)

CMS	Conditions	RRF	PFD
Pressure Relief Valve	Clean Service. Designed for the hazardous event	100	0,01
Vessel Rupture Disk	Designed for the hazardous event	100	0,01
Vacuum Breaker	Designed for the hazardous event	100	0,01
Overflow Line	Overflow line is designed to discharge to containment area which is sized to address the hazardous event. Any valves in line shall be administratively controlled to ensure the CMS is available when needed.	100	0,01

G.2.8 Step 7: Determine CMS risk gap

As with any IPL, there are two potential states when a process demand occurs: 1) success where the CMS works as designed and 2) failure where the CMS does not work as designed. In Step 7, the CMS risk is addressed by assessing the consequence when the CMS works as designed. In Step 8, the risk associated with the CMS not working as designed is assessed.

To determine the CMS risk (i.e., works as designed), it is necessary to first evaluate the severity of the secondary consequence. The consequence severity is assessed according to standardized definitions in Table G.4 "Consequence severity decision table". The CMS risk is determined by CMS consequence severity and the frequency of the CMS use. This frequency is determined by multiplying the overall initiating event frequency (Step 3) by the RRF of each IPL that prevents the initiating event from placing a demand on the CMS. These IPL were identified in Step 5.

The CMS risk is evaluated using Table G.5 RRF matrix. If the CMS risk gap is reduced to "TR," no further risk reduction is required. The team may identify functions that improve the risk reduction, if desired. If the CMS risk gap is 10, 100, 1 000, or 10 000, the team shall identify more IPLs, as appropriate. If these safeguards do not exist in the current design, recommendations are made.

In this example (Table G.2 and Figure G.4), the team determined that the flare availability was good at the site and the material released to the flare did not pose any unacceptable

consequence. When the PRV operates as designed, the scenario releases material to the flare and was determined to be at the tolerable risk level.

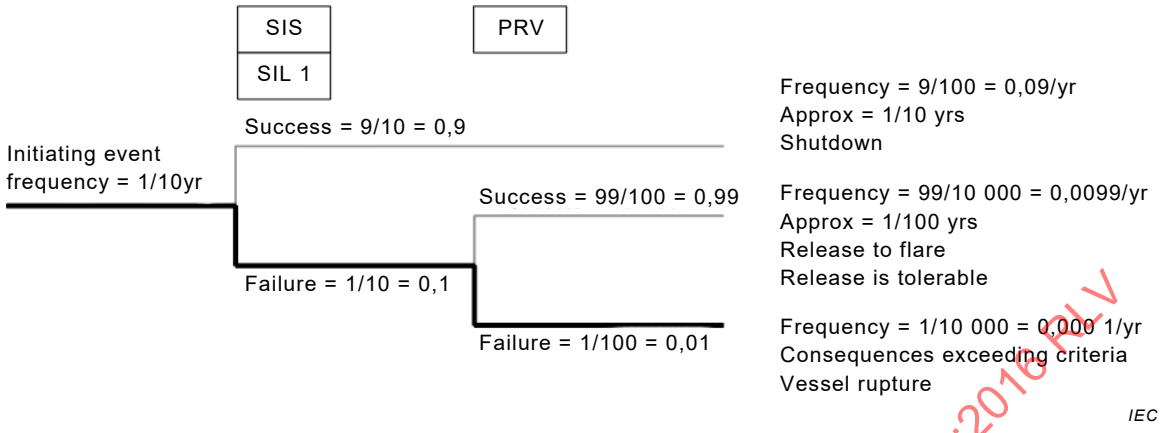


Figure G.4 – Acceptable secondary consequence risk

After the study was completed, a flare study determined that the release from the pressure relief valve could overload the flare and cause excessive backpressure in the relief system. Figure G.5 updates the event tree to show the revised secondary consequence – an overpressure event with significant consequence that occurs 1/100 years.

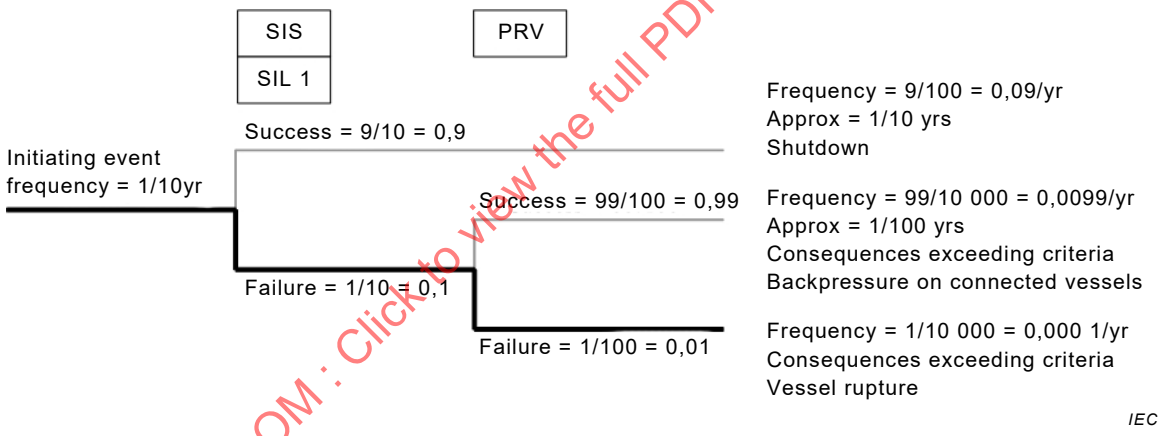


Figure G.5 – Unacceptable secondary consequence risk

Table G.8 updates Table G.2 with the revised assessment of the release from the PRV to the flare, showing the consequence created by the lifting of the pressure relief valve. The team determined that it was possible for the back-pressure generated by this relief scenario to cause overpressure in other units during a simultaneous relief event. The consequence of opening the relief valve was determined to be as high as the scenario considering failure of the PRV (see failure path for PRV). While the risk associated with the primary scenario (rupturing the vessel) is reduced to the tolerable risk (TR) level, the risk associated with the secondary consequence (overloading the relief system) is higher than the risk tolerance. The CMS risk gap is RRF = 100 for the safety and environmental consequence rankings, while the asset CMS is RRF = 10.

The CMS risk gap is determined by first evaluating the consequence of successful operation of the CMS using Table G.4. Then the challenge frequency for the CMS is determined by the scenario initiating event frequency (including enabling conditions) as reduced by the proactive IPLs operating prior to the CMS challenge (see the event trees Figures G.4 and G.5). The CMS risk gap is then taken from Table G.5.

Table G.8 – Step 7 LOPA worksheet *(1 of 2)*

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes. What If Consequence 1.1.1.1	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1. Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	10
		E	4	1 000								
		A	3	100								

Table G.8 *(2 of 2)*

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. Overloads relief system causing excessive backpressure	100	S	4	1 000	10	100	1 000	1000	TR		
			E	4	1 000		100	1 000		TR		
			A	3	100		100	100		TR		

Applying this new risk reduction requirement, it was determined that the SIS should be upgraded to SIL 3 in accordance with recommendations from API 521 *Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system* and ASME *Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design*. A SIL3 SIS reduced the demand frequency on the PRV and achieved an acceptable level of risk as shown in Figures G.5 and G.6.

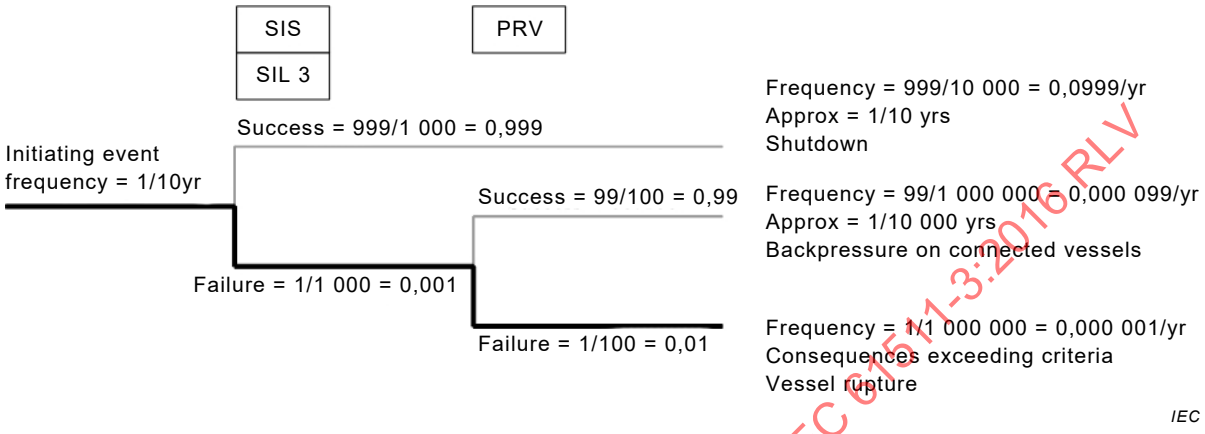


Figure G.6 – Managed secondary consequence risk

G.2.9 Step 8: Determine scenario risk gap

The scenario risk gap is determined from its consequence severity (Step 4) and its frequency given the presence of identified IPLs (Step 5) and CMSs (Step 6). Each frequency is determined by multiplying the overall initiating event frequency by the RRF of each IPL preventing the scenario and each CMS mitigating the scenario. IPLs were identified in Step 5 and CMSs were identified in Step 6.

The scenario risk is compared to the risk criteria as shown in Table G.9 using Table G.5. If the scenario risk gap is reduced to "TR," no further risk reduction is required. The team may identify functions that improve the risk reduction, if desired. If the scenario risk gap is 10, 100, 1 000, or 10 000, the team shall identify more IPLs or CMSs, as appropriate. If these do not exist in the current design, recommendations are made.

In this example (Table G.9), the scenario needed a total risk reduction of 1 000 to achieve the tolerable risk. With a SIL 3 SIS providing an RRF of 1 000 and a pressure relief valve providing an RRF of 100, an overall risk reduction of 100 000 is provided by the IPL design against overpressure of the vessel. Table G.9 shows the scenario risk gap meets tolerable risk.

G.2.10 Step 9: Make recommendations when needed

Recommendations shall be listed when the CMS or scenario risk gap is not reduced to "TR." Any listed recommendation should describe the safety function, classify it as a specific IPL type, and provide the required risk reduction. Other recommendations shall be listed by the team, if desired.

Table G.9 – Step 8 LOPA worksheet *(1 of 2)*

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity (S) and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes. What If Consequence 1.1.1.1	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1. Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	1 000
		E	4	1 000								
		A	3	100								

Table G.9 *(2 of 2)*

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. Overloads relief system causing excessive backpressure	100	S	4	1 000	1000	TR	1 000	100 000	TR		
			E	4	1 000		TR	1 000		TR		
			A	3	100		TR	1 000		TR		

Annex H
(informative)

A qualitative approach for risk estimation & safety integrity level (SIL) assignment

H.1 Overview

Informative Annex H provides one example of a qualitative approach for risk estimation and SIL assignment that can be applied to SIFs in the process industry.

NOTE 1 The methodology described in Annex H uses qualitative estimation of risk and is intended to be generally applied for the assignment of a SIL(s) to safety instrumented function (SIF(s)) in the process industry. The risk parameters (see Figure H.2) used whilst applying this methodology to particular processes and their specific hazards can be subject to agreement with those involved to ensure that the SIS can provide adequate risk reduction.

NOTE 2 The process industry risk graph parameters used in Annex H are from Table D.1.

NOTE 3 Annex H is not intended to be a definitive account of the method but is intended to illustrate the general principles.

For each hazardous event, the safety integrity requirements should be determined separately for the SIFs to be performed by the SIS (see IEC 61511-1:2016, Subclause 6.3.1, Tables 3 and 4).

Figure H.1 is an example of a practical way of carrying out a risk assessment at a specific hazardous event leading to estimation of a SIL for a SIF. This methodology should be performed for each hazardous event where the risk has to be reduced. Figure H.1 should be used in conjunction with the guidance information in Annex H.

It is important that the risk graph and its calibration is agreed to at a senior level within the organization taking responsibility for safety.

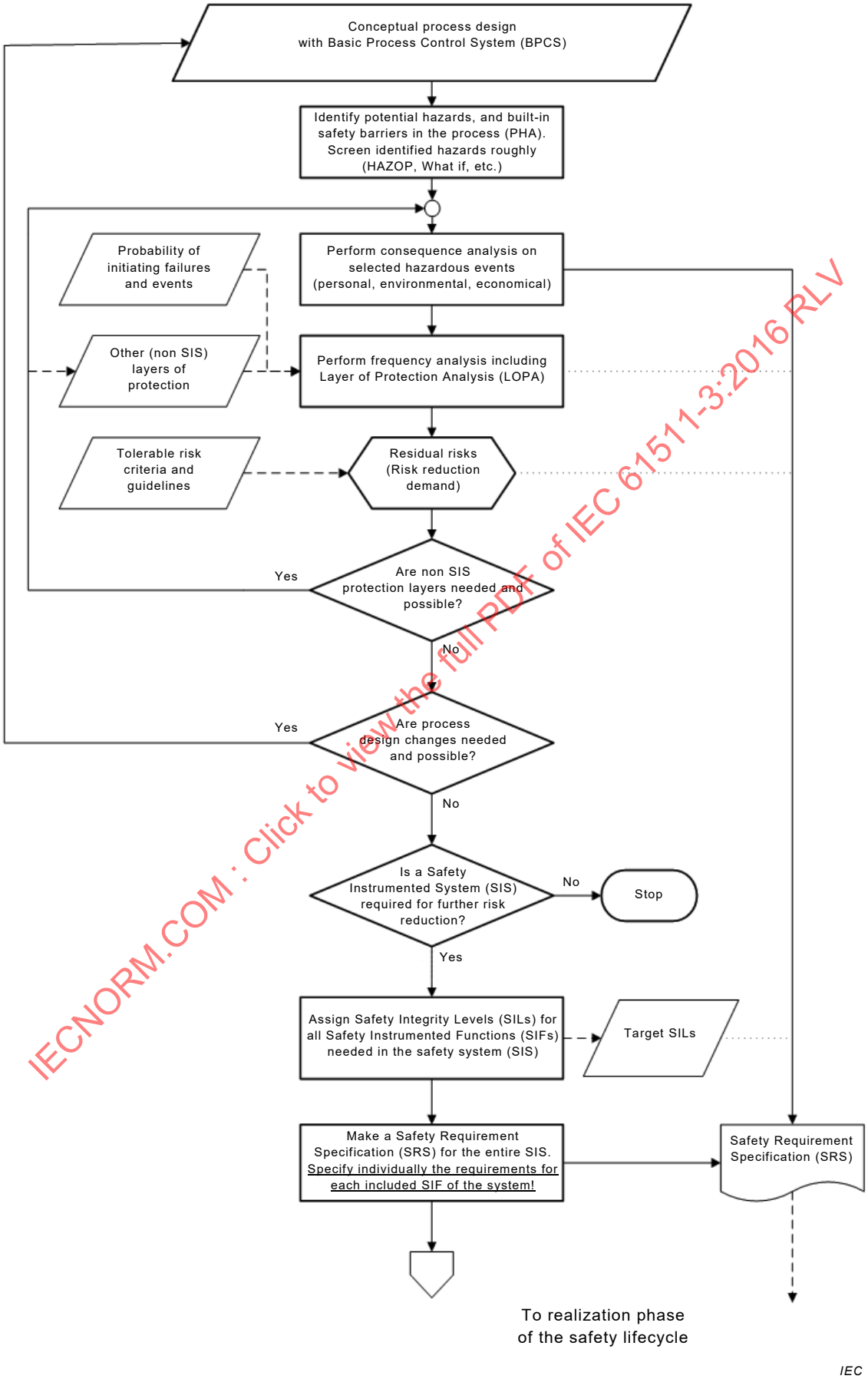


Figure H.1 – Workflow of SIL assignment process

Risk estimation is an iterative process; this means that the process may need to be carried out more than once.

H.2 Risk estimation and SIL assignment

H.2.1 General

Clause H.2 provides guidance on what and how to achieve risk guidance and SIL assignment.

H.2.2 Hazard identification/indication

Indicate the hazardous event, including those from reasonable foreseeable misuse, whose risks are to be reduced by implementing a SIF. List them in the hazardous event column in Table H.1.

Table H.1 – List of SIFs and hazardous events to be assessed

SIF No.	Hazardous event description	Safety Instrumented Function (SIF) description
01		
02		
03		
04		

H.2.3 Risk estimation

The risk graph matrix is used for SIL assignment for SIF. SILs are established by combining the risk graph consequence parameter C and the likelihood summarized as the risk graph parameters F, P and W. For each hazardous event SIL could be determined individually for health, environment and financial aspects. The overall target SIL of the considered SIF will be decided by the maximum determined SIL among these three aspects (health, environment and asset).

Risk estimation should be carried out for each hazardous event by determining the risk parameters shown in Figure H.2 and should be derived from the following:

– consequence of harm (C), and

– probability of occurrence of that harm, which is a function of:

- occupancy parameter (F) which is the probability that the exposed area is occupied at the time of the hazardous event;
- avoidance parameter (P) the probability that exposed persons are able to avoid the hazardous situation, which exists if the SIF fails on demand;
- demand rate parameter (W) is the residual demand rate or frequency of the hazardous event if considering SIF is not implemented.

Risk related to the identified hazardous event	=	H.2.4 Consequence of the possible harm, C	&	H.2.5.2 Probability that the exposed area is occupied at the time of the hazardous event, F H.2.5.3 Probability that exposed persons are able to avoid the hazardous situation, P H.2.5.4 Residual demand rate or frequency of the hazardous event, W	H.2.6 Probability of occurrence of that harm

IEC

Figure H.2 – Parameters used in risk estimation

For each hazardous event many different sequences of events could exist that lead to this hazardous event. All these sequences should be handled separately because the probability of occurrence could differ (F, P and W).

H.2.4 Consequence parameter selection (C) (Table H.2)

This is the 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.

Severity level (C) is the estimated consequence of the hazardous event. Select proper level for health, hnvironmental and financial hazards. Fill in the chosen severity letter (A-F) for each individual hazard in the C column.

Determining proper severity levels presupposes consequence categories calibrated to meet the tolerable risk levels established by company risk management and authorities.

Table H.7 provides examples of consequence categories.

Table H.2 – Consequence parameter/severity level

Consequence parameter		
Severity Level		C
CF	Catastrophic	F
CE	Extensive	E
CD	Serious	D
CC	Considerable	C
CB	Marginal	B
CA	Negligible	A

H.2.5 Probability of occurrence of that harm

H.2.5.1 General

Clause H.2.5 provides guidance on key parameters related to probability of harm occurrence.

Each of the three parameters of probability of occurrence of harm (i.e., F, P and W) should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that under specification of a SIL does not occur.

H.2.5.2 Occupancy parameter section (Table H.3)

Assess 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).

Exposure probability (F) is the probability that the exposed area is occupied at the time of the hazardous event. The exposure probability is only valid for health risks (H). If occupancy is permanent or if credit already has been given for reduced occupancy likelihood when the health severity level was chosen, the "Permanent" alternative (F_D) shall be chosen. Exposure probability (F_C) shall be chosen if occupancy is frequent or if the occupancy is dependent on the hazardous situation. Exposure probability (F_B) should be chosen if the area is occupied just occasionally and human presence is obviously independent of the hazardous situation. Exposure probability (F_A) should only be chosen if the hazardous area is confined and human presence rare and independent of the hazardous situation. Fill in the selected correlating number (0-2) in the (F) column. A value of 1 for the occupancy parameter is predefined for the environmental and financial hazards.

Table H.3 – Occupancy parameter/Exposure probability (F)

Occupancy parameter			
Frequency of human presence in the hazardous zone. Credit for limited occupancy shall not have been taken choosing the consequence categories.			
Exposure probability			F
FD	Permanent	=1	2
FC	Frequent	0,1-1	2
FB	Occasionally	0,01-0,1	1
FA	Rare	<0,01	0

H.2.5.3 Avoidance parameter selection (Table H.4)

This parameter describes the probability for exposed persons to be able to avoid the hazardous situation which exists even when the SIF has failed 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.

Avoidance probability (P) is the probability of avoiding the hazardous event even if the considered safety function fails to prevent the event. Normal choice is P_B "Avoidance conditions not fulfilled".

P_A could be chosen individually for the health hazard (H) if all persons in the hazardous area are likely to be evacuated to a safe area in time if the SIF fails on demand. This requires that:

- persons have sufficient time to evacuate, and
- independent facilities for alerting and evacuating all people in the hazardous area are existing.

P_A could also be claimed if the hazardous event is likely to be avoided in time by manual operator actions. In this case, P_A is also relevant for environmental and financial hazards. This requires that:

- independent facilities for alerting the operator of the functional failure and for manually bringing the process to a safe state are available,
- at least 1 hour (minimum) is available between operator alert and the hazardous event.

Fill in the correlating number (0 or 1) of the selected avoidance parameter in the P column.

NOTE In Annex H, choosing P_A implies at least 90% probability that the hazard will be avoided.

Table H.4 – Avoidance parameter/avoidance probability

Avoidance parameter		
Probability of avoiding the hazardous event if the SIF fails on demand. Implies independent facilities provided to "shut-down" so hazard can be avoided or enable all persons to escape to a safe area. Conditions to be fulfilled for P_A: Facilities to alert operator that the SIS has failed Independent facilities to bring process to safe state Time between operator alert and hazardous event >1h		
Avoidance probability		P
P_B	Avoidance conditions not fulfilled	1
P_A	All avoidance conditions are fulfilled	0

H.2.5.4 Demand rate parameter selection (Table H.5)

The number of times per year that the hazardous event would occur in the absence of the SIF under consideration 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.

The demand rate parameter (W) is selected by estimating or calculating the residual demand rate or frequency of the hazardous event if the considered SIF is not implemented. This frequency can be determined by combining frequencies of failures and other initialising events leading to the hazardous event. Credit should be given for non SIS implemented safety barriers. The total risk reduction credit for barriers implemented in the normal control system (BPCS), including alarms and operator response, cannot be more than a risk reduction factor of 10 by definition in IEC 61511:- (risk reduction factor >0.1). Fill in the chosen number correlating to the estimated or calculated residual demand rate in column W.

Table H.5 – Demand rate parameter (W)

Demand rate parameter			
Demand rate			W
W9	Often	> 1/ y	9
W8	Frequent	1/1-3 y	8
W7	Likely	/3-10 y	7
W6	Probable	1/10-30 y	6
W5	Occasional	1/30-100 y	5
W4	Remote	1/100-300 y	4
W3	Improbable	1/300-1 000 y	3
W2	Incredible	1/1 000-10 000 y	2
W1	Inconceivable	1/10 000-100 000 y	1

H.2.6 Estimating probability of harm

For each hazardous event, and as applicable, for each aspect (health, environment; financial) add the points from the F, P and W columns and enter the sum into the column SIL in Table H.6.

H.2.7 SIL assignment

Use the risk graph matrix (Table H.6) to read out the SIL for each one of the aspects (health, environment and financial) by combining its severity letter (A-F) with its likelihood sum (1-12). The overall target SIL equals the maximum determined SIL.

Using Table H.6, the intersection point where the severity (C) row crosses the relevant column for likelihood (F+P+W), indicates what kind of action is required.

Example: For a specific hazard when looking at human health with a C assigned as catastrophic, an F as 1, and a P as 1 and a W as 3 then:

F+P+W = 1 + 1 + 3 = 5. Using Table H.6, this would lead to a SIL 2 being assigned to the SIF that is intended to mitigate the specific hazardous event.

Table H.6 may be used to record the results of a SIL assignment exercise when using the methodology described in Annex H.

In Table H.6, 'NR' corresponds to an 'Unclassified' safeguard since PFD>0,1.

Table H.6 – Risk graph matrix (SIL assignment form for safety instrumented functions)

Project: Process:
Issued by: Plant:
Date: System:
Revision: Chart Nr:

Consequence parameter			Risk graph matrix						Occupancy parameter				Avoidence parameter			Demande rate parameter			
			Likelihood sum (F+P+W)						*Frequency of human presence in the hazardous zone. Credit for limited occupancy must not have been taken choosing consequence categories!*				*Probability of avoiding the hazardous event **if the SIF fails on demand**. Implies **independent** facilities provided to "shut-down" so hazard can be avoided or enable all persons to escape to a safe area. Conditions to be fulfilled:*			Estimated SIF demand rate			W
Severity level		C	1-2	3-4	5-6	7-8	9-10	11-12					• Facilities to alert operator that the SIS has failed			W_9	Often	>1/ y	9
C_F	Catastrophic	F	NR	SIL1	SIL2	SIL3	SIL4	NO					• Independent facilities to bring process to a safe state			W_8	Frequent	1/1-3 y	8
C_E	Extensive	E	NR	NR	SIL1	SIL2	SIL3	SIL4	Exposure rate			F	• Time between operator alert and hazardous event			W_7	Likely	1/3-10 y	7
C_D	Serious	D	OK	NR	NR	SIL1	SIL2	SIL3	F_D	Permanent	= 1	2				W_6	Probable	1/10-30 y	6
C_C	Considerable	C	OK	OK	NR	NR	SIL1	SIL2	F_C	Frequent	0,1-1	2	Avoidance probability		P	W_5	Occasional	1/30-100 y	5
C_B	Marginal	B	OK	OK	OK	NR	NR	SIL1	F_B	Occasionally	0,01-0,1	1	P_B	Avoidance conditions not fulfilled	1	W_4	Remote	1/100-300 y	4
C_A	Negligible	A	OK	OK	OK	OK	NR	NR	F_A	Rare	<0,01	0	P_A	All avoidance conditions are fulfilled	0	W_3	Improbable	1/300-1 000 y	3
																W_2	Incredible	1/1 000-10 000y	2
																W_1	Inconceivable	1/10 000-100 000 y	1

SIF-NO:	Hazardous Event Description	Safety instrumented Function (SIF) Description	Consequence		Influence		Demande	Likelib	Integrity		Comments
			Harm	C	F	P	W	Sum	SIL	SIL	
01			*H*	**E**	1	1	3	**5**	1	**2**	
			E	**F**	*I*	1		**5**	2		
			F	**C**				**5**	NR		
02			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		
03			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		
04			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		

Table H.7 – Example of consequence categories

C	Human harm (H)	Probability loss of life		Max. health consequences due to the hazardous event	Additional comments to the health consequence categories
CF	Catastrophic	PLL > 1		Several (3 or more) dead. Many (10 or more) critical injured.	Several fatalities likely.
CE	Extensive	PLL = 0,1 – 1,0		Some (1 to 2) dead. Several (3 or more) critical injured.	Individual fatality/fatalities likely.
CD	Serious	PLL = 0,01 – 0,1		Some (1 to 2) critical injuries. Several (3 or more) injured.	Several lost time injury/injuries. One or some lasting disablement. Fatality/fatalities not likely but possible.
CC	Considerable	PLL < 0,01		Some (1 to 2) injuries. Serious discomfort.	One or some lost time injury/injuries. Minor probability of lasting disablement. Fatality improbable.
CB	Marginal	PLL = 0		Minor injury/injuries. Lasting discomfort.	No lost time injury/injuries. Medical treatment required.
CA	Negligible	PLL = 0		Negligible injury/injuries. Temporary discomfort.	No lost time injury/injuries. No medical treatment required.
C	Environmental harm (E)	Effluent Influence	Effluent Extension	Max. environmental consequences due to the hazardous event	Additional comments to the environmental consequence categories
CF	Catastrophic	Lasting	Wide	Wide permanent or long time harm. Decontamination impossible or hard.	A liquid spill into river or sea. A wide vapour or aerosol release. The effluent causes lasting or permanent damage to plants and wildlife.

C	Human harm (H)	Probability loss of life		Max. health consequences due to the hazardous event	Additional comments to the health consequence categories
CE	Extensive	Lasting	Confined	Confined permanent or long time harm. Decontamination impossible or hard.	A liquid spill to ground water. A confined vapour or aerosol release. The effluent causes lasting or permanent damage to plants and wildlife.
CD	Serious	Lasting	Limited	Limited permanent or long time harm. Decontamination impossible or hard.	Onsite liquid spill. A limited vapour or aerosol release (within fence). The effluent causes lasting or permanent damage to plants and wildlife.
CC	Considerable	Temporary	Wide/Confined	Wide to confined temporary harm. Decontamination easy or not needed.	A liquid spill into river or sea. A limited vapour or aerosol release. The effluent causes temporary damage to plants and wildlife.
CB	Marginal	Temporary	Limited	Limited (on site) temporary harm. Decontamination easy or not needed.	Onsite liquid spill. A limited vapour or aerosol release (within fence). The effluent causes temporary damage to plants and wildlife.
CA	Negligible	Negligible		Negligible environmental harm. Decontamination not needed	Moderate leak from flange or valve. Small liquid spill or small soil pollution not effecting ground water. Negligible environmental effects.
C	Financial harm (F)	Damaged property (k€)	Production loss (k€)	Max. financial consequences due to the hazardous event	Additional comments to the financial consequence categories
CF	Catastrophic	>10 000	>50 000	Devastating loss off production, market share and image.	Devastating damage to production unit and/or plant. Event causing or requiring a production stop for more than a year.
CE	Extensive	1 000 – 10 000	5 000 – 50 000	Extensive loss of production. Large loss of market share and/or image	Extensive damage to equipment and/or property. Event causing or requiring a lasting production stop of several months.
CD	Serious	100 – 1 000	500 – 5 000	Large loss of production. Considerable loss of market share and/or image	Serious damage to equipment and/or property. Event causing or requiring a lasting production stop up to a month.
CC	Considerable	10 – 100	50 – 500	Considerable loss of production. Marginal loss of market share.	Considerable damage to equipment and/or property. Event causing or requiring a lasting production stop up to a week
CB	Marginal	1 – 10	5 – 50	Minor loss of production. No loss of market share and/or image.	Minor damage to equipment. Event causing or requiring a day of production stop.
CA	Negligible	<1	<5	Negligible loss of production. No loss of market share and/or image.	Negligible damage to equipment. Event causing or requiring a temporary (hours) production stop.

Annex I
(informative)

Designing & calibrating a risk graph

I.1 Overview

Annex I describes the basic steps involved in designing and calibrating a risk graph that enables the safety integrity level (SIL) of a safety instrumented function (SIF) to be determined from knowledge of the risk factors for the process plant.

A risk graph used to assess the required safety-integrity levels for any process plant application needs to be appropriate for the particular application and calibrated to use the tolerable event frequency values that have been determined to be relevant to the potential risk outcome.

The risk graph methods shown in IEC 61511-3 are example techniques and the user needs to be satisfied that they are appropriate to the application and ensure that the results gained have the correct value. In many cases it is necessary to adapt an example method to make it relevant to the application and calibrate the chosen risk graph to give the correct values.

Annex I is not intended to be a definitive account of the process by which a risk graph is designed and calibrated but is intended to illustrate the general principles. It is based on a method described in more detail in the following reference:

"*Using risk graphs for Safety Integrity Level (SIL) assessment – first edition*"; Clive De Salis, C; Institution of Chemical Engineers", 2011.

I.2 Steps involved in risk graph design and calibration

The steps in the design and calibration of a risk graph may include, but not be limited to, the following:

- decide the assessment parameters to be included in the risk graph;
- draw the overall shape of the risk graph;
- define each of the parameters in detail;
- assign values to each of the parameters that match the definitions;
- identify the tolerable event frequency values to be used for each consequence definition;
- identify the calibration axis line for each consequence;
- calculate all other values in the graph relative to the relevant calibration axis line;
- convert the event probability values into SIL numbers using the relevant tolerable event frequency;
- review the overall risk graph and remove any routes through the risk graph that are contrary to requirements.

I.3 Risk graph development

Clause I.3 provides an overview of how a risk graph may be developed.

The first steps in designing and calibrating a risk graph are to define the parameters that need to be assessed, deciding the overall shape of the risk graph, defining each parameter in detail and deciding the range of values that are relevant for each parameter.

I.4 The risk graph parameters

I.4.1 Choosing parameters

When choosing parameters for use in a SIL assessment for a process plant the user shall select all of the appropriate values to be assessed. Figure I.1 shows the main parameters that should be considered but others may be relevant and may need to be added.

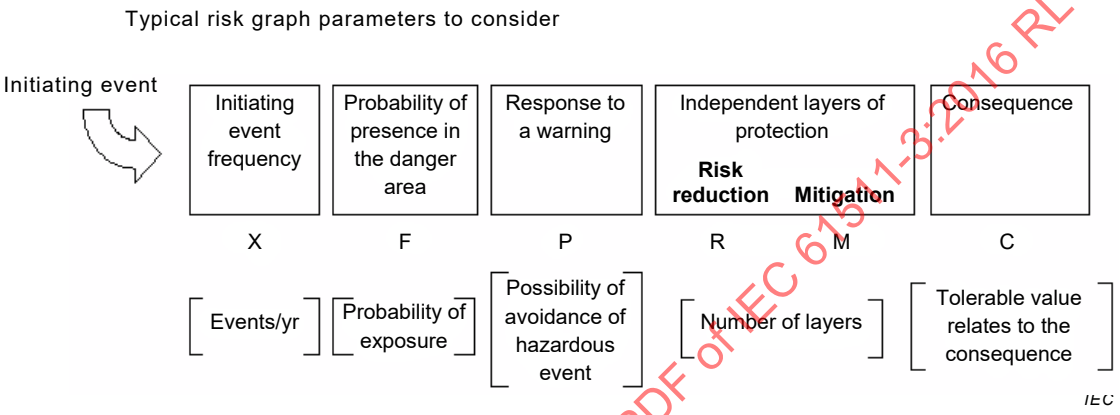


Figure I.1 – Risk graph parameters to consider

An example showing a combination of techniques from Annex D (Figure D.1) and Annex C (Figure C.2) is shown in Figure I.2 to illustrate how a risk graph can be designed to have more parameters.

I.4.2 Number of parameters

Having decided the parameters to be used, now decide the number of each parameter to be used. For example, it may be sufficient to represent the probability of exposure of a person to the risk by simply two values: F1 and F2.

I.4.3 Parameter value

Define each parameter and each value for that parameter. These definitions should be sufficiently detailed for assessment team members to understand the parameter and repeatedly select the correct value.

During this step it may be necessary to revise the decisions made in either or both of the preceding steps.

I.4.4 Parameter definition

When defining parameters to be included consider the meaning of available information.

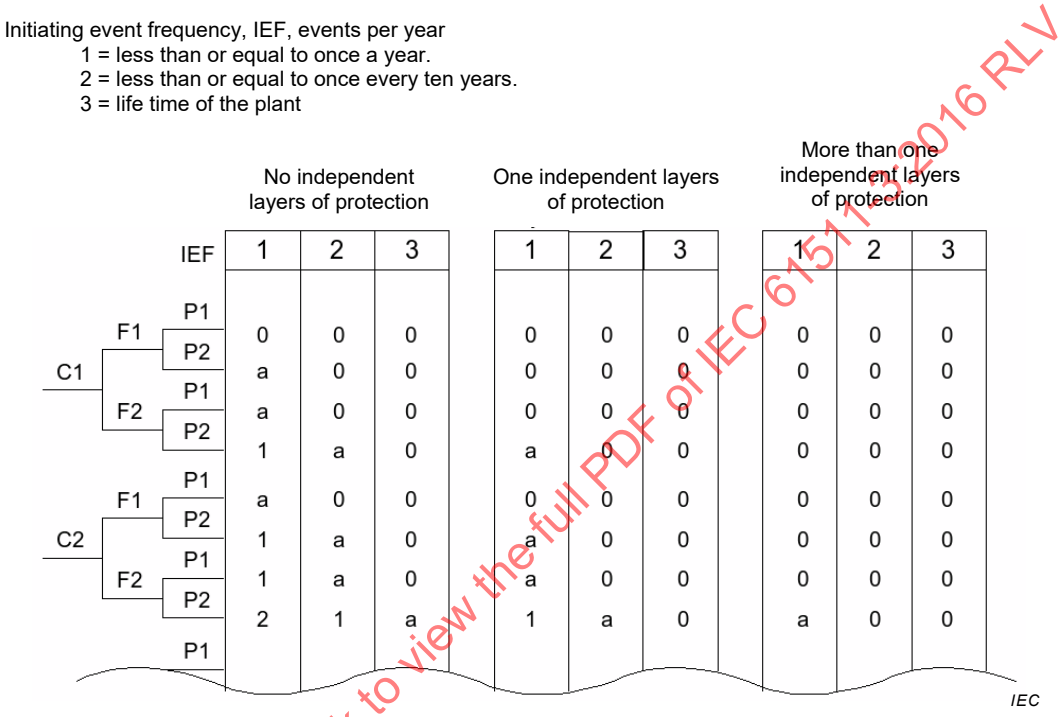
For example, you may have information on how often an event occurs for a process plant that is under the control of the BPCS in which case your data can be used for how often the event occurs and the BPCS fails to control it as a combined value. Alternatively you may have the initiating event data separately to the BPCS' capability to control that process condition.

NOTE If a risk graph is designed to use the initiating event frequency then the risk graph can include all other parameters with which to determine the demand rate on the safety function. Therefore the probability of other independent risk reducers will need to be included to properly assess the demand rate on the safety functions.

I.4.5 Risk graph

Draw the risk graph as an overall diagram.

NOTE The diagram will usually be symmetrical in form and include all combinations of possible routes including those routes through the diagram that may later be excluded. For example, your policy can be to exclude consideration of operator response to alarms where the consequence is potentially multiple fatalities. In this example case your diagram will include the operator response lines at this stage of the design but at the final stage the option of operator response will be deleted.



Key 0 = no protection layer needed; a = SIS protection layer probably not needed; 1 and 2 = SIL value needed

Figure I.2 – Illustration of a risk graph with parameters from Figure I.1

I.4.6 Tolerable event frequencies (Tef) for each consequence

I.4.6.1 Tef guidance

Provides guidance when determining tolerable event frequencies.

I.4.6.2 Tef SIL assessment

SIL assessment tolerable event frequencies are different for each consequence. Values assigned are often relative to the single fatality consequence. If the safety case for the process plant has a linear progression from Single fatality = 1, to serious injury = 0,1, minor injury = 0,01 then a full list of these values is made for each consequence defined in Clause I.4.3 and Clause I.4.4 Value progressions are not always linear. For example the values may change for multiple fatalities (N) and it is not unusual to change the values for N=10 or N=50.

I.4.6.3 Risk graph Tef

Ensure that the tolerable event frequency values are correctly used in the risk graph. If the tolerable event frequency is the number of serious injuries per year to an individual but the intended use of the risk graph is to consider a single process plant risk then these two terms

are not directly compatible. An individual will be subject to multiple risks of serious injury from his occupation and so the design shall consider how to convert from expressions of risk to the individual to risks of a single event on a process plant.

I.4.7 Calibration

I.4.7.1 General

Explains the significance of calibration in the risk graph development.

I.4.7.2 Calibration axis line

The calibration axis line for each consequence is the route through the risk graph that corresponds exactly to the consequence.

For example:

A risk graph may have the following parameters (Figure I.1):

– C3 = single fatality;
– F2 = probability of exposure is 1 (i.e., personnel likely to be present);
– P2 = difficult to avoid;
– R0 = no available independent other technology risk reducers;
– M0 = no available independent mitigation measures;
– 1 = initiating event frequency is once per year.

The sequence of this example route through the risk graph means that the outcome is potentially a single fatality, they are present, it is difficult to avoid, there are neither independent risk reducers to prevent it nor mitigation measures to change the outcome and the event happens every year = one fatality per year. This is the calibration axis line for the single fatality consequence because if the tolerable event frequency required for this event is 2×10^{-5} then the probability of failure required of the safety function to avoid this is 2×10^{-5} FD. The mathematical value for each parameter in this sequence is 1 indicating the number of people present and the probability of each parameter failing to avoid the outcome. C3 × F2 × P2 × R0 × M0 × 1 per year = 1 fatality × 1 × 1 × 1 × 1 × 1 per year = 1 fatality per year.

I.4.7.3 Calibration events per year

For each calibration axis line final destination write in the events per year represented by that route through the risk graph.

I.4.7.4 Route events per year

Using the values determined inI.4.3, I.4.4 and I.4.7.3 calculate the events per year that will occur for each route through the risk graph by adjusting one parameter at a time.

This can be illustrated by the same example from I.4.7.2 above in which we change one value, for example F2 becomes F1.

A risk graph may have the following parameters:

– C3 = single fatality;
– F1 = probability of exposure is 0,1 (i.e., less than 10% chance of personnel in the danger zone);
– P2 = difficult to avoid;

– R0 = no available independent other technology risk reducers;

– M0 = no available independent mitigation measures;

– 1 = initiating event frequency is once per year.

The sequence of this example route through the risk graph means that the outcome is potentially a single fatality, they are present for less than 10% of the time, it is difficult to avoid, there are neither independent risk reducers to prevent it nor mitigation measures to change the outcome and the event happens every year = 0,1 fatalities per year. The mathematical value for each parameter in this sequence is 1 indicating the number of people present and the probability of each parameter failing to avoid the outcome, except for the value of F2 which has been defined as a less than 10 % chance of being in the area and therefore has a value of 0,1. C3 × F2 × P2 × R0 × M0 × 1 per year = 1 fatality × 0.1 × 1 × 1 × 1 × 1 per year = 0,1 fatalities per year.

I.4.7.5 PFD_{avg} calculation

With all destination points in the risk graph calculated as the frequency of events, now divide the tolerable event frequency value for the consequence by the calculated value at the destination point. The values now written in the risk graph are the PFD_{avg} required.

I.4.7.6 PFD_{avg} conversion to SIL

Now convert each PFD_{avg} value into the SIL number. When converting a PFD_{avg} value into a SIL number for the risk graph a value should never be rounded down to a less onerous value but always rounded up.

I.4.8 Completion of the risk graph

I.4.8.1 General

Discusses items to consider when finalizing the risk graph.

I.4.8.2 Routes removal

Remove routes through the risk graph that should not be present.

For example, your policy may be to exclude consideration of operator response to alarms where the consequence is potentially multiple fatalities. For this example case the route(s) for the response to a warning being possible would be removed from the risk graph where the potential outcome is multiple fatalities.

I.4.8.3 Risk graph instructions

A detailed set of instructions describing the correct use of the risk graph should be written. The instructions should include a statement describing the limitations of use for the risk graph (i.e., the limits of applicability).

Annex J
(informative)

Multiple safety systems

J.1 Overview

The semi quantitative approaches presented in IEC 61511-3:- annexes are very useful to evaluate quickly the risk reduction which is needed to achieve a given hazardous event frequency target established from a prior risk analysis (refer to Annex A about ALARP approach). Nevertheless, the underlying hypothesis that the risk reduction achieved by a SIS is directly linked to its relevant failure measure (e.g., average unavailability – PFD_{avg}) is true only when a single SIS is implemented. When several safety systems (SIS and non-SIS) are designed to run in sequence to prevent a given hazardous event the risk reduction still increases when the failure measures decrease but the link is not so simple and the risk reduction which is actually provided by a given SIS may be lower than that which can be inferred directly from its individual failure measure. This is true especially when periodically proof tested systems are implemented.

Therefore, when several safety systems working together have been designed according to the approaches developed in IEC 61511-3 annexes it is important to check that common cause failures and dependency effects between the safety systems are negligible or properly taken into account in order to actually achieve the tolerable hazardous event frequency.

NOTE More information can be found in the documents provided in bibliography.

J.2 Notion of systemic dependencies

Figure J.1 illustrates the conventional calculations used in semi quantitative approaches. Two safety instrumented systems (SIS_1 and SIS_2) are working in sequence. When a demand occurs from the process then SIS_1 has to react first. If it fails then SIS_2 has to react in turn and, if it also fails, the hazardous event occurs.

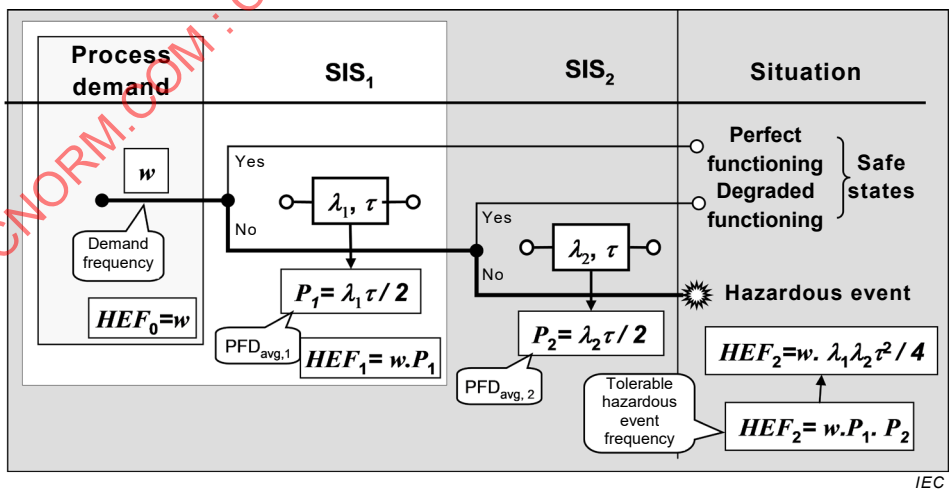


Figure J.1 – Conventional calculations

When using the semi quantitative approaches it is accepted that the risk reduction provided by a SIS is equal to the inverse of its failure measure (e.g., P_i=1/$PFD_{avg,i}$). Therefore, without any SIS, the hazardous event frequency HEF_0 is equal to the demand frequency itself (w). Then, the SIF achieved by SIS_1 provides a risk reduction $HEF_0/HEF_1=1/P_1$ and the risk drops

to $HEF_1=w.P_1$. Afterward the SIF achieved by SIS_2 provides a risk reduction $HEF_1/HEF_2=1/P_2$ and the risk drops to $HEF_2=HEF_1.P_2=w.P_1.P_2$ which is expected to comply with the tolerable hazardous event frequency requirements.

However, the times for proof testing, MTTR, MRT, common cause failure and other factors for each of the SIFs can interact to give a different risk reduction to that presumed in the simplistic view that has so far been described.

In the simple example of Figure J.1, SIS_1 comprises only one sensor (S), one logic solver (LS) and one final element (FE) organised in series and tested at the same time with a periodical proof test interval. Then the failure rate of SIS_1 is $\lambda_1 = \lambda_{1_S} + \lambda_{1_{LS}} + \lambda_{1_{FE}}$ and its average unavailability (i.e., $PFD_{avg,1}$) is $P_1 = \frac{\lambda_1.\tau}{2}$. Similarly, the average unavailability of SIS_2 (i.e., $PFD_{avg,2}$) is given by $P_2 = \frac{\lambda_2.\tau}{2}$. Therefore, with the two safety instrumented systems (SISs), the hazardous event frequency is established at $HEF_2 = w.P_1.P_2 = w.(\frac{\lambda_1.\tau}{2}).(\frac{\lambda_2.\tau}{2}) = w\frac{\lambda_1\lambda_2.\tau^2}{4}$ where the SIF achieved by SIS_1 provides a risk reduction of $HEF_0/HEF_1 = 1/PFD_{avg,1}$ and the SIF achieved by SIS_2 a risk reduction of $HEF_1/HEF_2 = 1/PFD_{avg,2}$.

The above calculation only takes into account the test interval but not the scheduling of the tests according to the time. This is shown in Figure J.2 where the two SIS are tested at the same time. This is a popular current test policy allowing to simplify the maintenance team tasks or to minimize the number of process shut-downs for performing the tests.

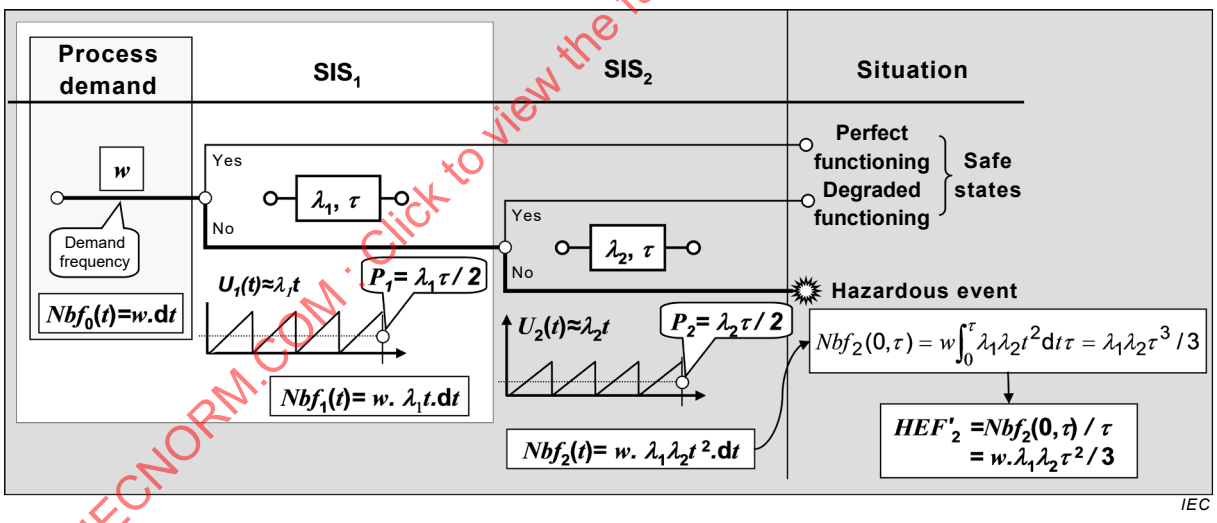


Figure J.2 – Accurate calculations

Within a proof test interval the unavailability of SIS_1 is given by $U_1(t) = 1 - e^{-\lambda_1 t}$ which is approximated by $\lambda_1 t$ when $\lambda_1 t << 1$. Just after a proof test $U_1(t)$ goes to 0 (if the repair time is negligible or if the process is stopped) then it increases until just before the next proof test. This gives the well known saw-tooth shaped curve which is represented in the Figure J.2. This is exactly the same for $U_2(t)$. Therefore $U_1(t)$ and $U_2(t)$ are *correlated* because they are low (just after a test) and high (just before a test) at the same time. This seems insignificant but, in fact, introduces a *systemic* dependency between SIS_1 and SIS_2 which, therefore, are not really completely independent. The term "*systemic dependency*" means that this dependency is a property of *SIS*$_1$ and *SIS*$_2$ considered as a whole, which cannot be described just by considering SIS_1 or SIS_2 separately. It has to be noted that this type of correlation doesn't exist for immediately revealed failures (e.g., detected by diagnostic tests) because the

unavailability related to these failures reaches asymptotic values which is not the case with proof tested failures.

When a demand occurs, $\lambda_1 \cdot t$ is the probability that SIS_1 fails, $\lambda_1.\lambda_2.t^2$ is the probability that both SIS_1 and SIS_2 fail and $w.\lambda_1.\lambda_2.t^2$ is the probability that the hazardous event occurs. If w is the demand frequency, $Nbf_0 = w.dt$ is the number of demands occurring between t and $t+dt$ (i.e., the number of hazardous events in the absence of safety systems). With the two SIS's, the number of hazardous event occurring over dt becomes $Nbf_2(t) = w.\lambda_1.\lambda_2.t^2 dt$ and a simple integral gives the number of hazardous events occurring within [0, τ]: $Nbf_2(0,\tau) = w.\lambda_1.\lambda_2.\tau^3/3$. Finally the average hazardous event frequency is equal to $HEF'_2 = Nbf_2(0,\tau)/\tau = w.\lambda_1.\lambda_2.\tau^2/3$. Note that the constant demand frequency w is factored. Then $3/\lambda_1.\lambda_2.\tau^3$ represent the risk reduction provided by the equivalent single safety system comprising both SIS_1 and SIS_2.

Finally $HEF'_2 = 1{,}33\ HEF_2$ which is obviously greater than HEF_2. We can write $HEF'_2 = w.(\frac{\lambda_1.\tau}{2}).\frac{4}{3}.(\frac{\lambda_2.\tau}{2}) = w.P_1 \text{ x } 1{,}33 \text{ x } P_2$ which shows that SIS_1 provides 100 % of the expected risk reductions P_1 and SIS_2 only 3/4 =75 % of P_2 because it acts in second position.

If a third SIS was added and tested at the same time (i.e. $P_3 = \frac{\lambda_3.\tau}{2}$), the hazardous event frequency would become $HEF'_3 = w\frac{\lambda_1\lambda_2\lambda_3.\tau^3}{4} = 2w.(\frac{\lambda_1.\tau}{2})(\frac{\lambda_2.\tau}{2})(\frac{\lambda_3.\tau}{2}) = 2w.P_1.P_2.P_3$ i.e., the risk reduction is only 1/2 = 50 % of what being expected from the semi quantitative approaches. Writing $HEF'_3 = w(\frac{\lambda_1.\tau}{2}).\frac{4}{3}(\frac{\lambda_2.\tau}{2}).\frac{3}{2}(\frac{\lambda_3.\tau}{2}) = HEF'_2 \text{ x } 1{,}5 \text{ x } P_3$ shows that the contribution of the third SIS of only 2/3 = 66 % of the expectation.

We can also write $HEF'_2 = [w.(\frac{\lambda_1.\tau}{2})].\frac{4}{3}(\frac{\lambda_2.\tau}{2}) = w'.\frac{4}{3}(\frac{\lambda_2.\tau}{2})$ where w' is the demand frequency on SIS_2. If w' is considered as a process demand, this shows that systemic dependencies may also exist between the process and the SIS. Therefore even in the case where a single SIS is considered, it may provide a reduction lower than expected.

If now we stagger the tests and perform some mathematical development we will find that an optimum is reached when SIS_2 is tested in the middle of the test interval of SIS_1. In this optimum case, the hazardous event frequency drops to $HEF''_2 = w.\frac{5}{24}\lambda_1\lambda_2.\tau^2$. This can be written $HEF''_2 = w.(\frac{\lambda_1.\tau}{2}).\frac{10}{12}.(\frac{\lambda_2.\tau}{2}) = w.P_1\frac{10 \text{ x } P_2}{12}$. The proof tests are still correlated but now SIS_2 provides a risk reduction of 12/10=120 % of what was expected. Therefore the correlation between the proof tests of the various SIS may be detrimental or beneficial depending of the implemented proof test policy.

As shown on the left hand side of Figure J.3 the multiple safety system analysed above is equivalent to a single redundant SIS. This allows the introduction of the potential common cause failures (CCF) which are likely to exist between SIS_1 and SIS_2 as shown on the right hand side of the figure. Common cause failures also constitute systemic dependencies between SIS_1 and SIS_2.

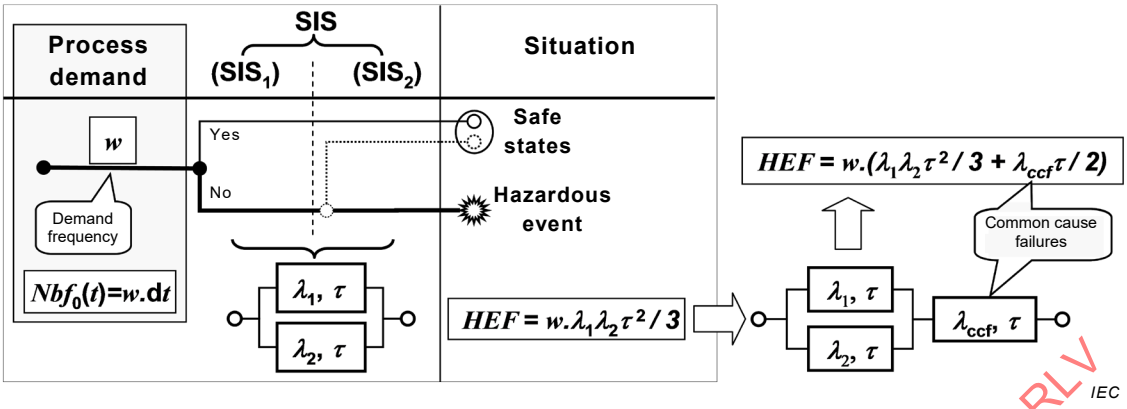


Figure J.3 – Redundant SIS

The CCF impact is generally more important than the correlation of proof tests and it is always detrimental. In the above example where the proof tests are performed at the same time this introduces an additional factor $w.\lambda_{ccf}.\tau/2$ to the hazardous event frequency. This impact can be reduced by staggering the proof tests: when SIS_1 and SIS_2 are not tested at the same time, any test is an opportunity to disclose the CCF provided that relevant procedures are implemented. The CFF proof test interval can be reduced up to $\tau/2$ thus dividing by two the CCF contribution to the hazardous event frequency. With a third SIS similar to SIS_1 and SIS_2, the CCF contribution may be divided by three, etc.

In conclusion the risk reduction provided by multiple SIS running in sequence may be lower, equal or greater than expected from semi-quantitative approaches. When the various safety systems are periodically tested at the same time the semi quantitative approaches leads to non-conservative results and the non-conservativeness increases with the level of redundancy. When complex patterns of proof tests are implemented, the result of the competition between detrimental or beneficial effects is difficult to anticipate. Therefore, when a multiple safety system has been designed according to the individual requirements established from semi quantitative approaches, it is wise to check that the targeted tolerable hazardous event frequency is actually achieved.

NOTE A single safety system with redundant components experiences the same systemic dependencies described above and can be analysed in the same way.

J.3 Semi-quantitative approaches

The semi quantitative approaches can be used to check the hazardous event frequency to take into account the effects of common cause failures and systemic dependencies.

When a proof test staggering policy is implemented (to mitigate the negative impact of proof test correlation) and no common cause failures are identified between the single SISs forming the multiple safety system the conventional calculations can be used. In the other cases some adjustments of the conventional calculations are needed.

If common cause failures are identified, they should be handled at the multiple safety system level as shown in Figure J.3. If proof tests are staggered and a relevant procedure is implemented, then the CCF proof test interval can be reduced to the interval between the successive staggered proof tests.

When no staggering proof test policy is implemented, then the systemic dependencies due to the correlation of proof test should be considered. Corrective coefficients like those presented in Figure J.4 ma

y help to estimate the corrections to be done. This table has been built with the hypothesis that all components are tested at the same time. The correction increases when the number of individual SISs increases and when the length of the scenarios leading to the hazardous event (the order of the so called minimal cut sets – MCS) increases. The table on the left hand side of Figure J.4 deals with a multiple safety system made of two individual SISs and the table on the right hand side deals with a multiple safety system made of three individual SISs. The corrective coefficients in this table are calculated as *m*/*n* where *m* is the coefficient of the integrals calculated separately and *n* the coefficient of the integral calculated as a whole. For example, for MCS of order 2 obtained from two separate SISs we compare factors like $\lambda_1\tau/2 \times \lambda_2\tau/2$ (integrals calculated separately) to factors like $\lambda_1\lambda_2\tau^2/3$ (integral calculated as a whole) and that gives a corrective factor of 2 × 2/3 = 4/3 = 1,33.

Multi SS	SIS1	SIS2	
MCS order	MCS order	MCS order	Coefficient
2	1	1	4/3=1,33
3	1	2	6/4=1,50
3	2	1	6/4=1,50
4	1	3	8/5=1,60
4	3	1	8/5=1,60
4	2	2	9/5=1,80
5	1	4	10/6=1,67
5	4	1	10/6=1,67
5	2	3	12/6=2,00
5	3	2	12/6=2,00

Multi SS	SIS1	SIS2	SIS3	
MCS order	MCS order	MCS order	MCS order	Coefficient
3	1	1	1	8/4=2,00
4	1	1	2	12/5=2,40
4	1	2	1	12/5=2,40
4	2	1	1	12/5=2,40
5	1	1	3	16/6=2,67
5	1	3	1	16/6=2,67
5	3	1	1	16/6=2,67
5	1	2	2	18/6=3,00
5	2	1	2	18/6=3,00
5	2	2	1	18/6=3,00

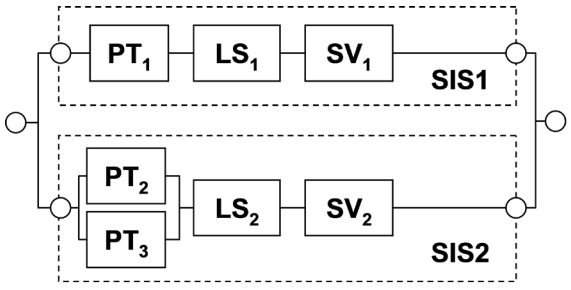
IEC

Figure J.4 – Corrective coefficients for hazardous event frequency calculations when the proof tests are performed at the same time

The tables in Figure J.4 should be applied on the minimal cut sets excluding the common cause failures at the multiple safety system level and the maximum order contributing to the hazardous event frequency should be evaluated and used to find the corrective coefficients (right columns of the tables presented in Figure J.4). For example if the maximum contributing order is 3, and if the multiple safety system comprises two SIS (left hand side of Figure J.4), the hazardous event frequency calculated from a semi quantitative approach should be multiplied by 1,5.

For a maximum contributing order of 4 it should be multiplied by a factor ranging from 1,6 to 1,8. It should be multiplied by a factor ranging from 2,7 to 3 for the minimal cut sets of order 5 of a multiple safety system made of three SIS (right hand side of Figure J.4), etc. When the multiple safety system comprises a mix of several situations, then the bigger coefficient should be used for the sake of conservativeness.

J.4 Boolean approaches



	Failure rate	Repair rate	Test interval
PT_1	4,50E-06	0,125	4380
PT_2	4,50E-06	0,125	8760
PT_3	4,50E-06	0,125	8760
PT_4	6,25E-04	0,125	Detected
PT_5	6,25E-04	0,125	Detected
PT_6	3,55E-06	0,042	8760
PT_7	3,55E-06	0,042	8760

IEC

Figure J.5 – Expansion of the simple example

In order to illustrate how multi safety systems can be handled the example which has been already analysed in Clause J.2 has been slightly modified: now SIS_1 and SIS_2 are not similar and the logic solvers have only detected dangerous failures. With two redundant sensors, the failure rate of SIS_2 is no longer constant. This new example is detailed and modelled with a reliability block diagram in Figure J.5 where PT stands for "pressure transmitter", LS for "logic solver" and SV for "safety valve". Each SIS comprises sensors (one or two), one logic solver and one safety valve organised in series. The nine failure scenarios (i.e., the so-called minimal cut sets, MCS) derived from this model are the following: {PT_1, PT_2, PT_3}, {PT_1, LS_2}, {PT_1, SV_2}, {LS_1, PT_2, PT_3}, {LS_1, LS_2}, {LS_1, SV_2}, {SV_1, PT_2, PT_3}, {SV_1, LS_2}, {SV_1, SV_2}. The MCS which are related to similar components are candidates for common cause failures. Then three minimal cut sets should be added to the nine previous ones: CCF_P, CCF_{LS} and CCF_{SV}. At the end we have twelve minimal cut sets (3 single failures, 6 double failures and 3 triple failures). Then, the first idea may be to use for each of them some simplified formulae like those proposed in IEC 61508-6:2010, Annex B. This is possible, provided that specific formulae are developed to deal with non-similar components (e.g., different failure modes and/or different proof test interval).

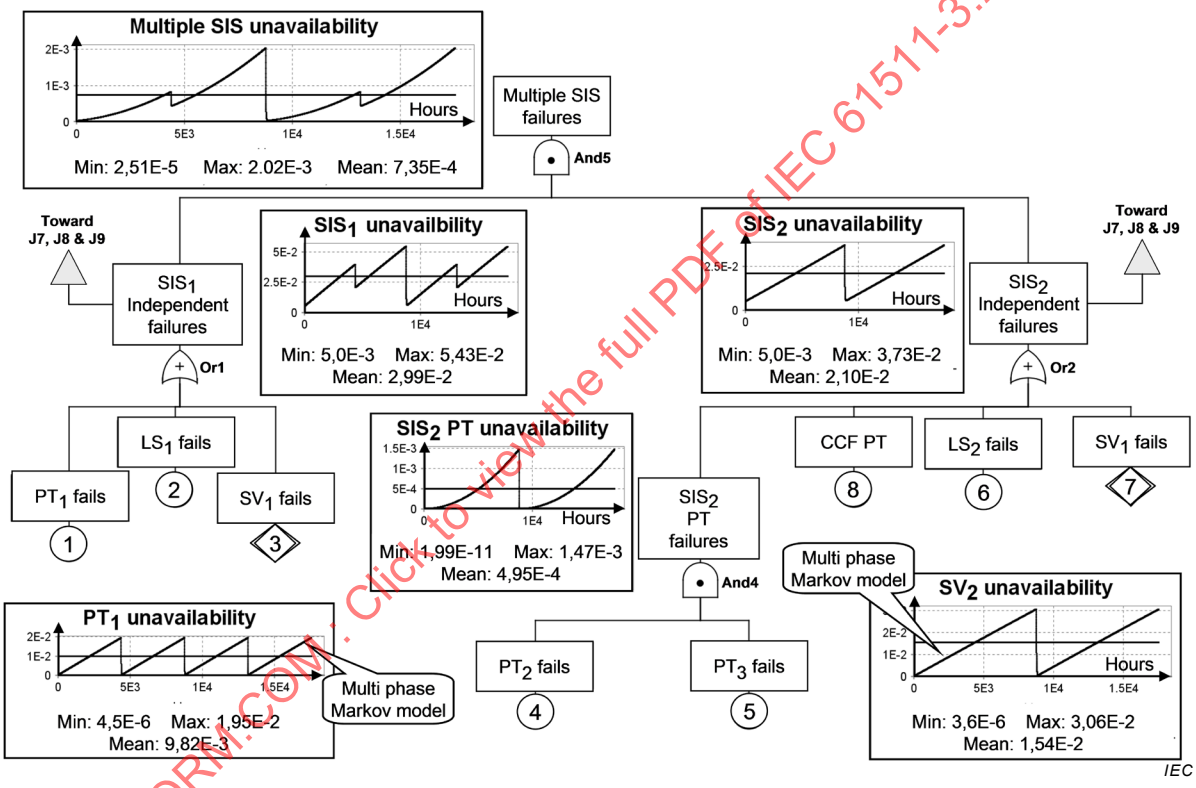


Figure J.6 – Fault tree modelling of the multi SIS presented in Figure J.5

The second idea is to use the fault tree approach which proves to be very effective when the components are reasonably independent (e.g., the probability to have 2 failures at the same time is low) and provided the calculations are handled in a correct way. The fault tree related to the above multiple SIS is presented in Figure J.6.

A fault tree gives directly the instantaneous unavailability of the top event from the instantaneous unavailability of the basic events. As said above and as shown in Figure J.6, the unavailability of a periodically tested event is a saw-tooth curve (see Note). Calculating the fault tree for a relevant number of instants t_i over a given period (e.g., 2 years), gives the unavailability at the logic gate output levels (including the top event). They are more or less complicated saw-tooth curves according to the proof test policy. Calculating the averages of the previous curves over the given period gives the average unavailability (e.g., PFD_{avg}). This averaging operation deals with the systemic dependencies due to the proof tests correlations.

Note that a beta factor of 1 % has been considered to model the CCF between PT_2 and PT_3 of SIS_2.

NOTE The input saw-tooth curves can be obtained through a multi-phase Markovian model (see IEC 61508-6:2010 Annex B). Then the fault trees are used to link small Markovian models. This is effective when those small Markovian models are independent from each other. With the data used for this example and for the independent failures we obtain an average availability P_1=2,99. 10^{-2} for SIS_1 and P_2=2,10. 10^{-2} for SIS_2. With a semi quantitative approach this would lead to a risk reduction of $1/P_1P_2$=1 588 when it is of only 1/7,35. 10^{-4}=1 360 (i.e., a difference of about 15 %).

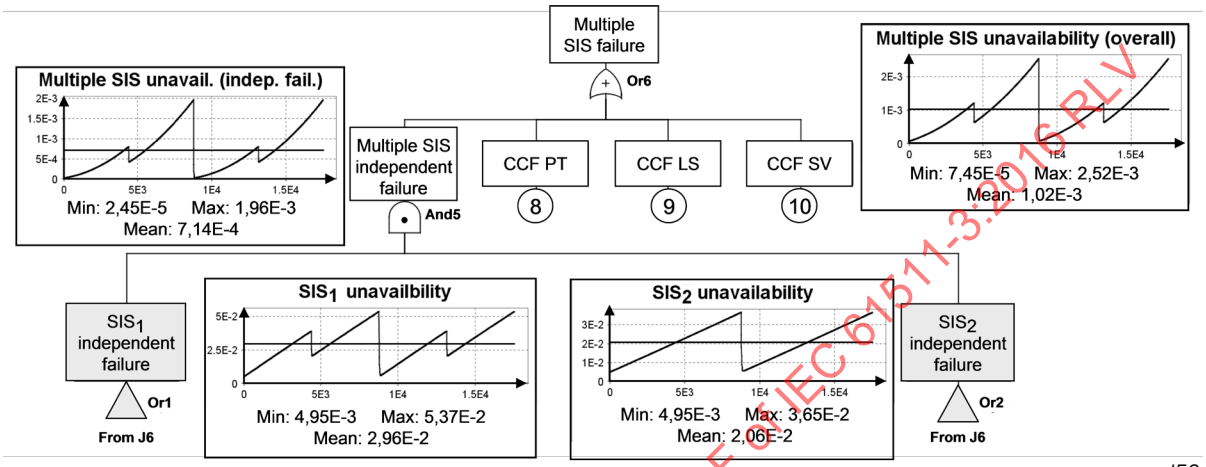


Figure J.7 – Modelling CCF between SIS_1 and SIS_2

The potential CCFs between SIS_1 and SIS_2 are not modelled in Figure J.6. This is done in Figure J.7 where the common cause failures between PTs, LSs and SVs have been considered with a beta factor of 1 %. Now, the average unavailability of the multiple safety system is 1,018 x 10^{-3} and the overall risk reduction has dropped to 982. This is about 62 % of the risk reduction expected from a semi-quantitative approach on the hypothesis that SIS_1 and SIS_2 are fully independent.

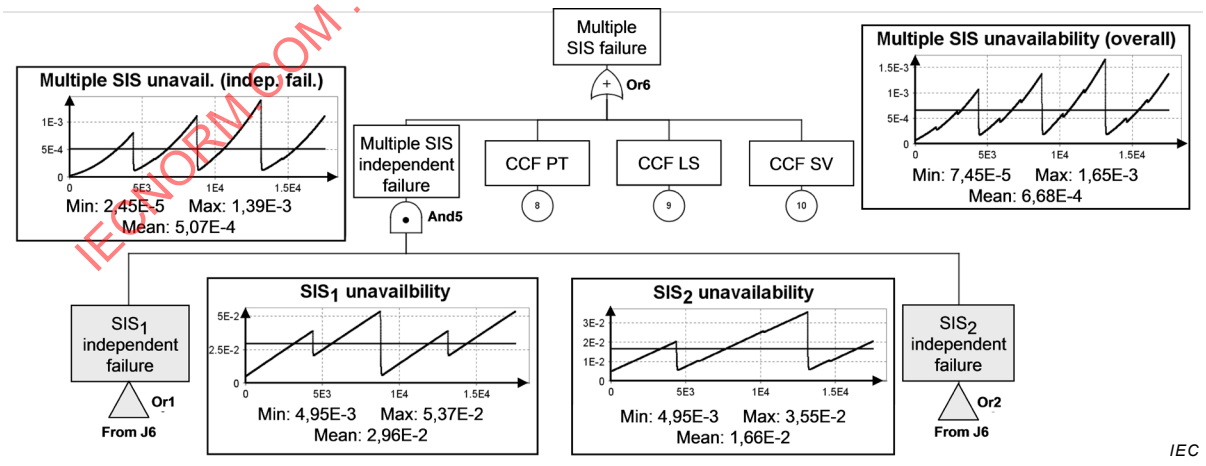


Figure J.8 – Effect of tests staggering

In Figure J.8 the tests of the three PTs have been staggered as well as those of the two SVs. The average unavailability of the two SIS considered as a whole is 6,68 x 10^{-4} and the overall risk reduction has increased to 1 497. This is just a bit lower than expected from a semi-quantitative approach.

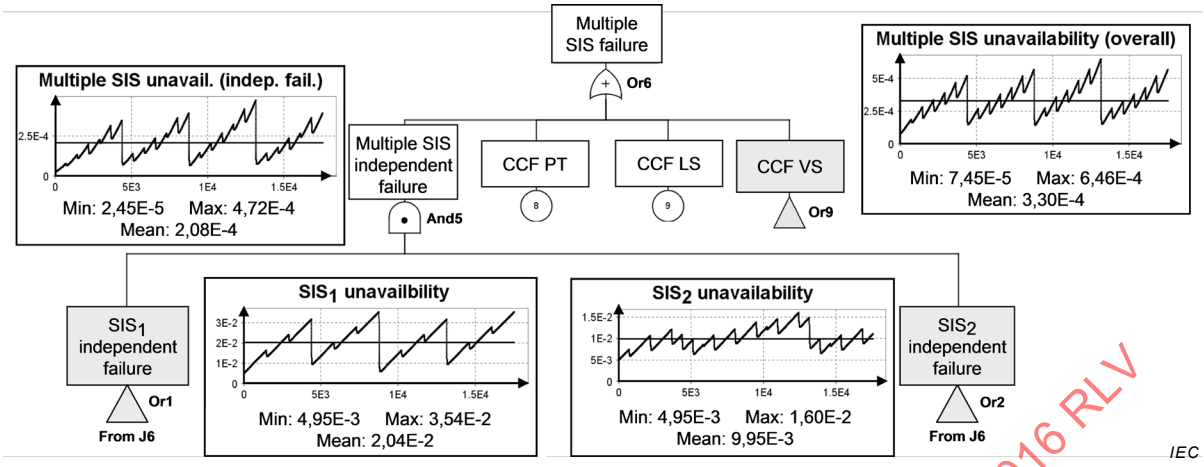


Figure J.9 – Effect of partial stroking

In Figure J.9 the failure modes of the safety valve have been split between those which are detected by partial stroking and those which are detected by full stroking. The average unavailability of the two SIS considered as a whole is 3,30 x 10^{-4} and the overall risk reduction has increased to 3 034. This is about twice that expected from a semi-quantitative approach.

J.5 State-transition approach

The fault tree approach is very efficient when the components are reasonably independent. This is not the case when the components are strongly dependent as for example when the repair occurs at the second failure, when the logic is changed (e.g., from 2oo3 to 1oo2) instead of repairing, when the delay to start the repair is long due to the mobilisation of the repair tools (e.g., a dynamic positioning vessel for subsea repairs), etc. In this case it is necessary to move to state-transition models allowing to properly representing the dynamic behaviours of the components. The Markovian approach (see IEC 61508-6:2010, Annex B) is the most popular state transition approach but when dealing with multiple safety systems, a great number of components have to be modelled and this is likely to provoke the combinational explosion of the number of states. Therefore other approaches which do not suffer this shortcoming have to be considered. Among them the Petri net (PN) approach has proven to be very effective (see IEC 61508-6:2010 Annex B and IEC 62551:2012) to model the complex dynamic behaviour of big systems. Analytical calculations are not possible with such models and it is necessary to swap to Monte Carlo simulation but this presents no real difficulties thanks to the computation power of the present time personal computers.

Figure J.10 illustrates a Petri net modelling the multiple safety system presented in Figure J.5. It is similar to the fault tree presented in Figure J.6 except that the repair resources are shared between all the components and should be mobilised before the interventions start (e.g., subsea systems needing a dynamic positioning vessel to be repaired).

This is a reliability block diagram driven Petri net where the reliability block diagram of Figure J.5 (drawn in dotted lines) has been used as guideline and where each bloc has been fulfilled by standardized sub-PN coming, for example, from a sub-PN library. Two kinds of sub-PN have been used: dangerous undetected failures (PTs, CCF on PT_2 and PT_3 and the SVs) and dangerous detected failures (for LSs). Building Petri nets in this way allows handling very big models with hundreds of components.

NOTE 1 A basic Petri net is made of places (circles) which represent local states, transitions (rectangles) which represent events which may occur and upstream arcs linking places to transitions and downstream arcs linking transitions to places. Tokens (small black circles) are placed into places to identify which local states are actually present at a given moment.

Tokens and upstream arcs are used to validate the transitions and, when a transition is valid, it can be "fired" (that means that the related event occurs): one token is removed from each upstream places and one token is added in each of the downstream places. Therefore the marking of the places (i.e. the state of the modelled system) change.

The date of the firing of transitions may be governed by stochastic delays (e.g. exponential distributions with constant failure or repair rates). In this case the PN are named stochastic Petri nets.

NOTE 2 More information about Petri nets can be found in IEC TS 62556:2014.

One pressure transmitter (e.g., PT_1) is normally in good state (W). When it fails it enters into a dangerous undetected state (DU) and its indicator variable (e.g., PT_1) goes to 0. When a proof test is performed, then the failure is detected (DD) and the variable *Nd* which counts the number of detected failures is increased by one. When the repair resource is on location (OL) the repair can start (R). When the repair is finished the indicator variable (e.g., PT_1) goes back to 1 and *Nd* is decreased by one. The same modelling is applied to the three PTs and the two SVs. For the logic solvers the state (DU) has been removed but the principle is similar.

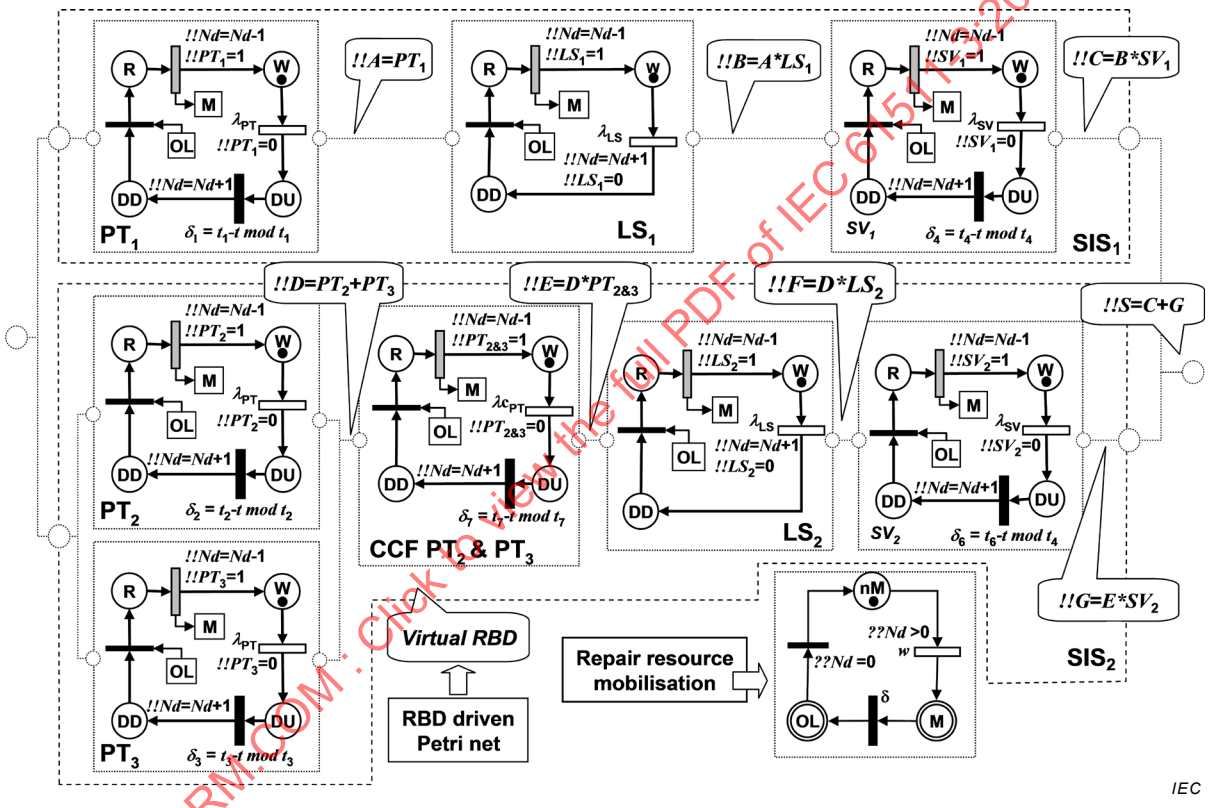


Figure J.10 – Modelling of repair resource mobilisation

When *Nd* becomes positive, (i.e., when at least one failure has been detected), then the mobilisation process starts (sub-PN "Repair resources mobilisation"). When it is achieved (token in M), then the resources move to the location of failures to be repaired (OL). Then the token in place OL is taken by one of the failures waiting for repair and this prevents other repairs at the same time. When the repair is finished one token is put back in place M and the resources can move to the location of another failure. This process is repeated until all the failures have been repaired (*Nd*=0) and that the resource is demobilised.

Global assertions have been introduced to model the virtual nodes of the reliability block diagram. The symbol "*" represents the logical AND, and the symbol "+" represents the logical OR. For example, $B=A*LS_1$ means that the output *B* of LS_1 is equal to 1 when LS_1 is not failed and its input is also equal to 1. $!!S=C+G$ means that the multiple safety system is OK (i.e., *S*=1) when SIS_1 is OK (*C*=1) or SIS_2 is OK (*G*=1).

Then the use of Monte Carlo simulation allows to produce statistical samples of the variables *C*, *G* and *S* and to obtain the safety measures related to SIS_1, SIS_2 and to the multiple safety system itself.

As shown in Figure J.11, it is possible to obtain the saw-tooth curves. They are less smooth than those obtained with fault tree calculations but similar. Nevertheless they should not be used to calculate the average unavailability because the average unavailability can be more accurately obtained directly from the Monte Carlo simulation: the average value of 1-*C* gives P_1, the average value of 1-*G* gives P_2 and the average value of 1-*S* gives the overall average unavailability.

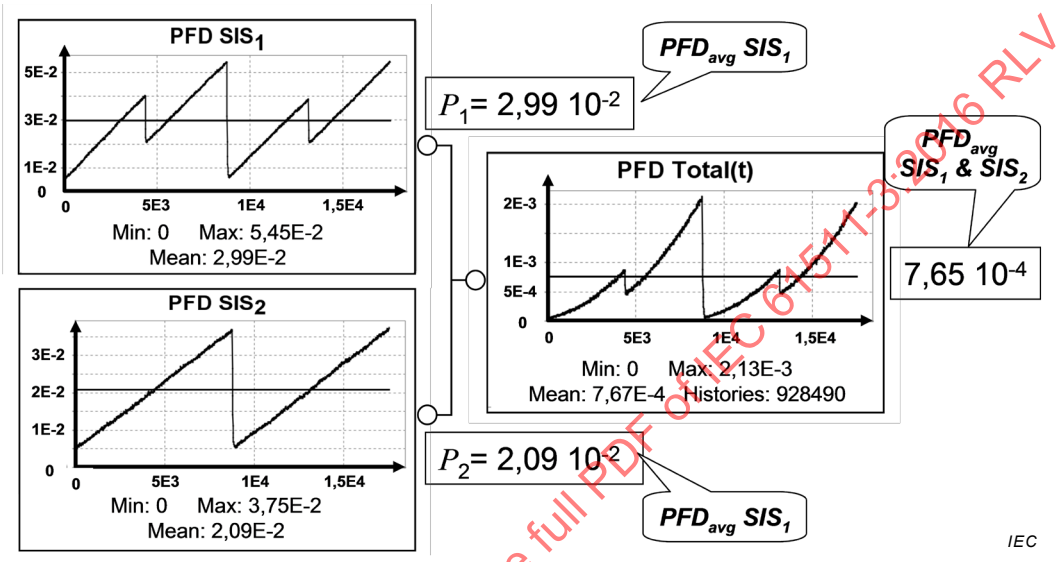


Figure J.11 – Example of output from Monte Carlo simulation

In Figure J.11 the mobilisation time and the time to reach the location of a given failure are equal to 0. Therefore the difference with the results of Figure J.6 is only due to the sharing of the repair resources. The impact is light for P_1 and P_2 and a little bit more important for the overall multiple safety system: 1/7,65x 10^{-4} = 1 307 instead of 1 360. Therefore, in this case, the dependency due to a shared repair team is light and this is why the fault tree approach which considers as many repair teams as failure modes is relevant when the probability to have two failures at the same time is small or/and when the repair times are negligible compared to the tests intervals.

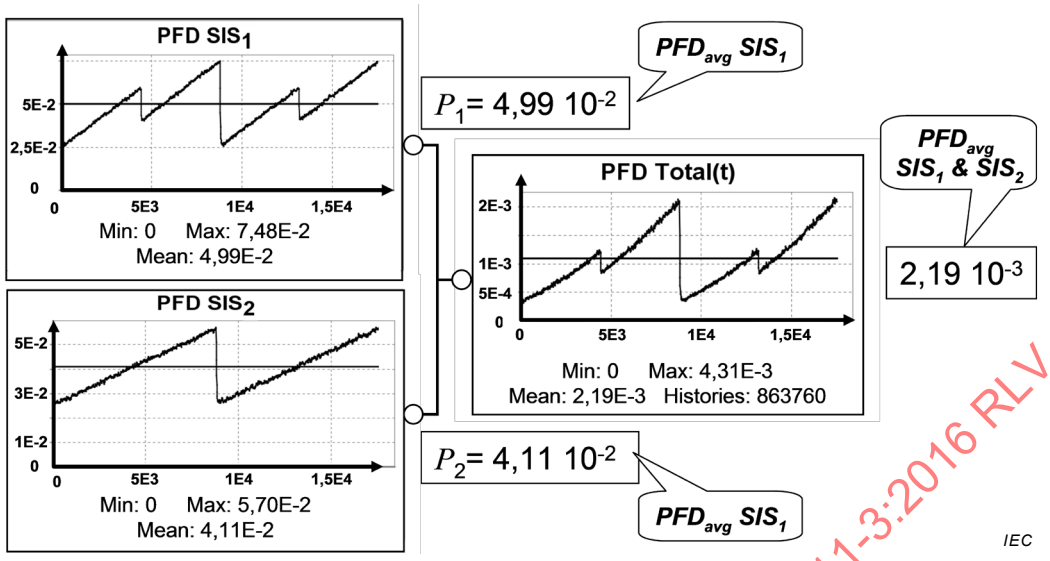


Figure J.12 – Impact of repairs due to shared repair resources

When the mobilisation time of the shared resources is not equal to 0, the repair times of individual failures are increased. In Figure J.12, the mobilisation has been taken equal to 24 h and the delay needed to reach the location of failure equal to 10 h. Then the first failure is delayed for 34 h and the other for 10 h. This impacts mainly the detected failures (i.e. the logic solver failures in our example) and almost multiplies by 2 the average unavailability's of SIS_1, SIS_2 and by 3 this of the multiple safety system: the overall risk reduction drops to 1/2,19 10 3= 457. This is about the third of the result obtained with the fault tree in Figure J.6.

The other examples presented in Figure J.7, Figure J.8 or Figure J.9 can be handled in the same way.

Annex K
(informative)

As low as reasonably practicable (ALARP) and tolerable risk concepts

K.1 General

Annex K considers one particular principle (ALARP) which can be applied during the determination of tolerable risk and the safety integrity level (SIL). ALARP is a concept which can be applied during the determination of the SIL. It is not, in itself, a method for determining SIL. Those intending to apply the principles indicated in Annex K 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)~~

UK HSE publication (2001) "*Reducing Risks, Protecting People*" ISBN 0 7176 2151 0.

K.2 ALARP model

K.2.1 ~~Introduction~~ Overview

Clause K.2 provides more detail to help understand the criteria associated with the ALARP method.

Clause K.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 items 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 item 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 K.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).

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.

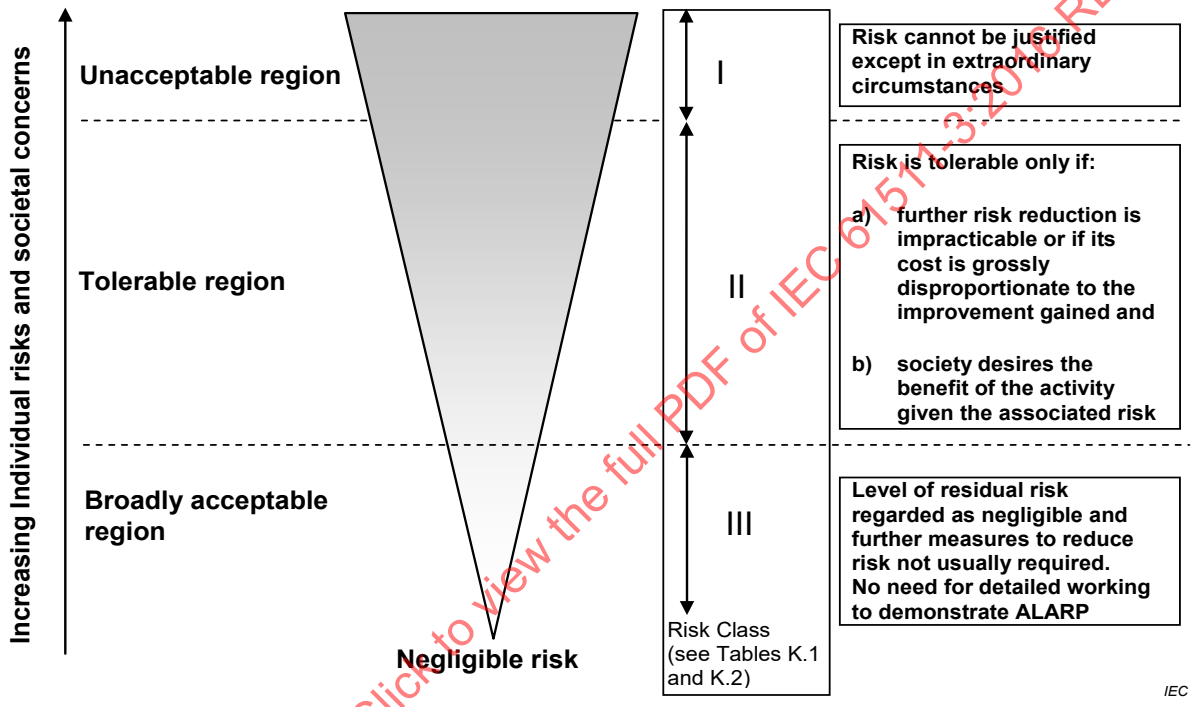


Figure K.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Sublause K.2.2 outlines a method for quantitative risk targets. (Annexes C and I (see I.4.5)) outline 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.

K.2.2 Tolerable risk target

In order to apply the ALARP principle, it is necessary to define the 3 regions of Figure K.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 K.1 is an example showing three risk classes (I, II, III) for a number of consequences and frequencies. Table K.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 K.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 K.1, the risk classes are as follows:

– 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 K.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 K.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 SIL of safety instrumented function (SIF) using, for example, one of the methods outlined in Annexes B to I.

Table K.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	III	III	III	III
NOTE 1 See Table K.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~~ can be seen as an example of how such a table could be populated, rather than as a specification for future use.				

Table K.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 SIF, see Annexes B to I.	

Bibliography

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61165:2006, *Application of Markov techniques*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61882:2001, *Hazard and operability studies (HAZOP studies) – Application guide*

IEC 62551:2012, *Analysis techniques for dependability – Petri net techniques*

IEC TS 62556:2014, *Ultrasonics – Field characterization – Specification and measurement of field parameters for high intensity therapeutic ultrasound (HITU) transducers and systems*

ISO/TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

INNAL F., Contribution to modeling safety instrumented systems and assessing their performance – Critical analysis of IEC 61508:2010 standard. Thesis of the University of Bordeaux, France, 2008.

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

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008).

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

Layer of Protection Analysis-Simplified – Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

ISA-S91.00.01 *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, 2001

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

VDI/VDE 2180 (2015) *Safeguarding Of Industrial Process Plants By Means Of Process Control Engineering – Calculating Methods Of Reliability Characteristics Of Safety Instrumented Systems*

Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design, Welding Research Council, PO Box 1942, New York, NY 10156, 2005, ISBN 1-58145-505-4

Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system, American Petroleum Institute, 1220 L Street, NW, Washington, D.C. 20005, 2007

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2007, ISBN 0-4719-7940-6

Guidelines for Initiating Events and Independent Protection Layers in LOPA, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2013

"*Using risk graphs for Safety Integrity Level (SIL) assessment – first edition*"; Clive De Salis, C; Institution of Chemical Engineers", 2011

Critical analysis of IEC 61508 standard. Thesis of the University of Bordeaux, France, 2008

SIGNORET J-P. & al., Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering and System Safety 113 (61-75), Elsevier, 2013

IEC 61511-3

Edition 2.0 2016-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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 exigés d'intégrité de sécurité

IEC 61511-3:2016-07(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. 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, control and automation.

This second edition cancels and replaces the first edition published in 2003. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:

Additional H&RA example(s) and quantitative analysis consideration annexes are provided.

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

FDIS	Report on voting
65A/779/FDIS	65A786/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.

A list of all parts in the IEC 61511 series, published under the general title *Functional safety – Safety instrumented systems for the process industry sector*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. A process hazard and risk assessment is carried out to enable the specification for SIS 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 SIS. The SIS includes all devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application: SIS safety life-cycle and safety integrity levels (SIL).

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010.

The IEC 61511 series sets out an approach for SIS safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

– a hazard and risk assessment is carried out to identify the overall safety requirements;
– an allocation of the safety requirements to the SIS is carried out;
– works within a framework which is applicable to all instrumented means 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;
– addressing all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
– enabling existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example national, federal, state, province, county, city) have established process safety design, process safety management, or other regulations, these take precedence over the requirements defined in the IEC 61511-1.

The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk assessment. The information herein is intended to provide a broad overview of the wide range of global methods used to implement hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016should be reviewed. The informative annexes in the IEC 61511-3 address the following:

Annex A provides information that is common to each of the hazard and risk assessment methods shown herein.

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.

Annex G provides a layer of protection analysis using a risk matrix.

Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.

Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.

Annex J provides an overview of the impact of multiple safety systems on determining the required SIL

Annex K provides an overview of the concepts of tolerable risk and ALARP.

Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that the IEC 61511 series plays in the achievement of functional safety for SIS.

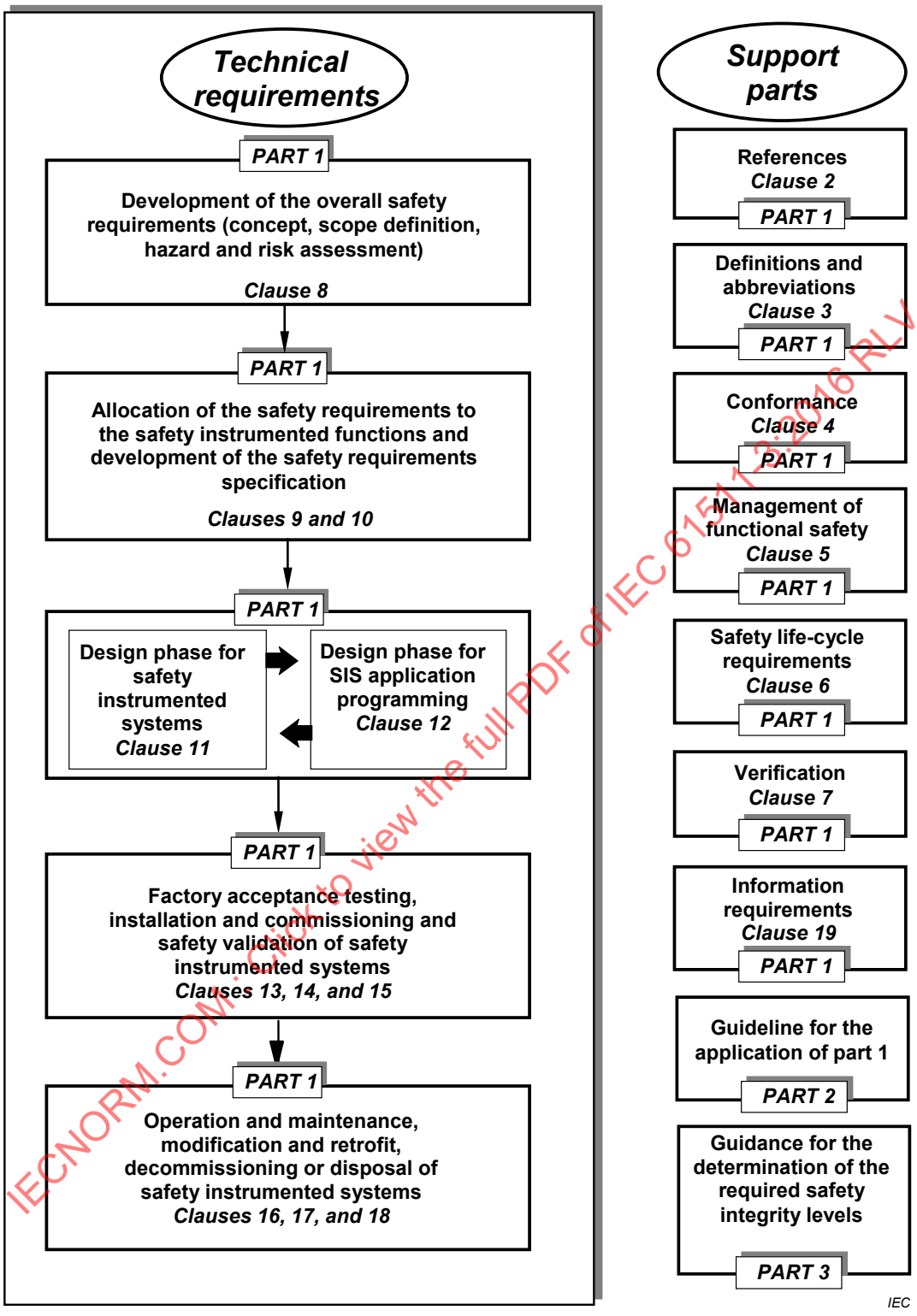


Figure 1 – Overall framework of the IEC 61511 series

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

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

1 Scope

This part of IEC 61511 provides information on:

– the underlying concepts of risk and the relationship of risk to safety integrity (see Clause A.4);

– the determination of tolerable risk (see Annex K);

– a number of different methods that enable the safety integrity level (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);

– the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;

d) illustrates techniques/measures available for determining the required SIL;

e) provides a framework for establishing SIL but does not specify the SIL required for specific applications;

f) does not give examples of determining the requirements for other methods of risk reduction.

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction means.

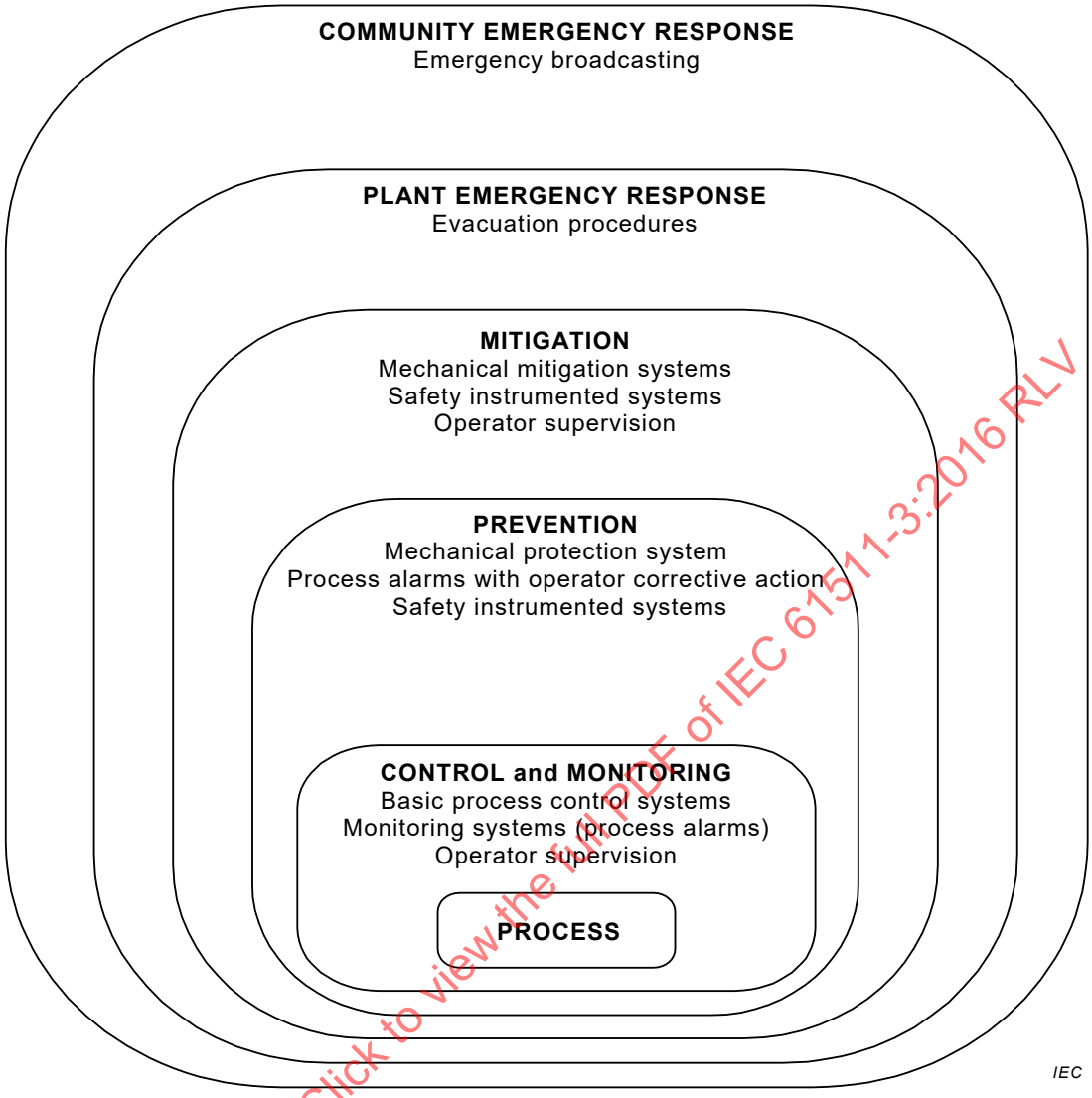


Figure 2 – Typical protection layers and risk reduction means

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61511-1:2016 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements*

3 Terms, definitions and abbreviations

For the purposes of this document the terms, definitions, and abbreviations given in IEC 61511-1:2016apply.

The annexes in this Part 3 are informative and not normative. Also, the application of any particular method described in Part 3 annexes does not guarantee compliance with the requirements of IEC 61511-1:2016.

Annex A
(informative)

Risk and safety integrity – general guidance

A.1 General

Annex A provides information on the underlying concepts of risk and the relationship of risk to safety integrity. This information is common to each of the hazard and risk assessment methods shown herein.

A.2 Necessary risk reduction

The necessary risk reduction (which may be stated either qualitatively (see Note 1) or quantitatively (see Note 2) is the reduction in risk that has to be achieved to meet the tolerable risk (for example, the 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 (SRS) for the SIF (in particular, the safety integrity requirement). The purpose of determining the tolerable risk (for example, the 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 A.2) 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.

NOTE 1 In determining the necessary risk reduction, the tolerable risk is established. Annexes D and E of IEC 61508-5: 2010 outline qualitative methods and semi-quantitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly rather than stated explicitly.

NOTE 2 For example, that a hazardous event, leading to a specific consequence, would typically be expressed as a maximum frequency of occurrence per year.

A.3 Role of safety instrumented systems

A safety instrumented system (SIS) implements the SIF(s) 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 SRS 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 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.

A SIF can operate in a demand mode of operation or a continuous mode of operation.

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.

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 SIF together with any other protection layer has to be such as to ensure that:

– the accident frequency due to the failure 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 A.1 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:

  - mechanical protection system;
  - safety instrumented systems;
  - non-SIS instrumented systems;
  - mechanical mitigation system.

NOTE 1 Figure A.1 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 SIS or other protection layers. The resulting risk model may therefore differ from that shown in Figure A.1.

The various risks indicated in Figures A.1 and A.2 are as follows:

– Process risk – The risk existing for the specified hazardous events for the process, the basic process control system (BPCS) and associated human factor issues – no designated safety protective features are considered in the determination of this risk;

– Tolerable risk (for example, the 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 BPCS, the IEC 61511 series 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 A.1.

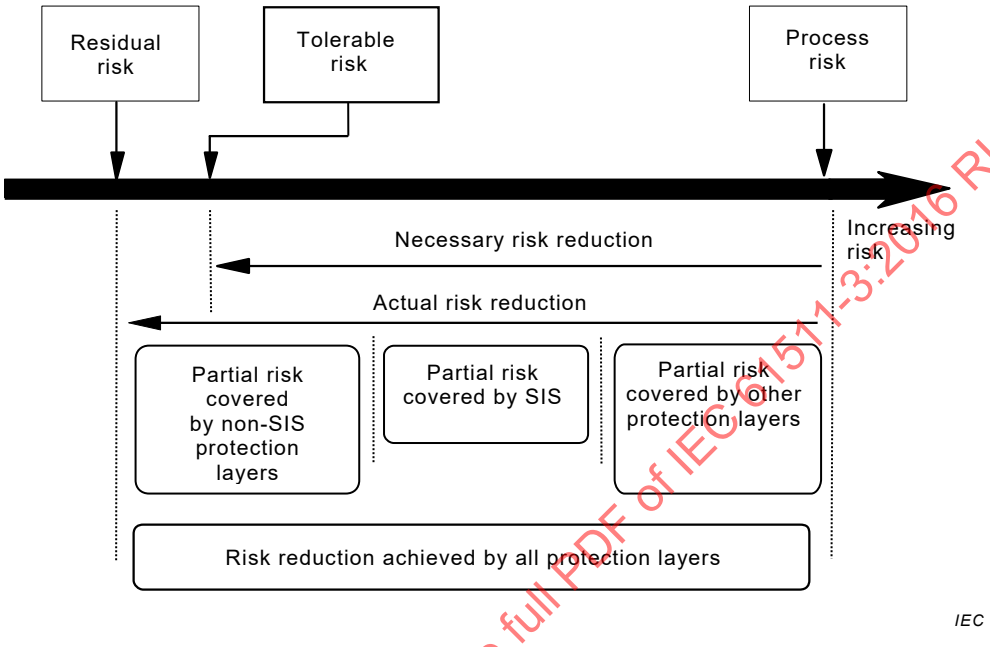


Figure A.1 – Risk reduction: general concepts

NOTE 2 In some applications, risk parameters (e.g., frequency and probability of failure on demand) cannot be combined simply to achieve the risk target as depicted in Figure A.1 without considering the factors noted in Annex J. This may be due to overlapping, common cause failure, and holistic dependencies between the various protection layers.

A.4 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 A.1). 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 risk reduction. 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 can 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 A.1 and A.2.

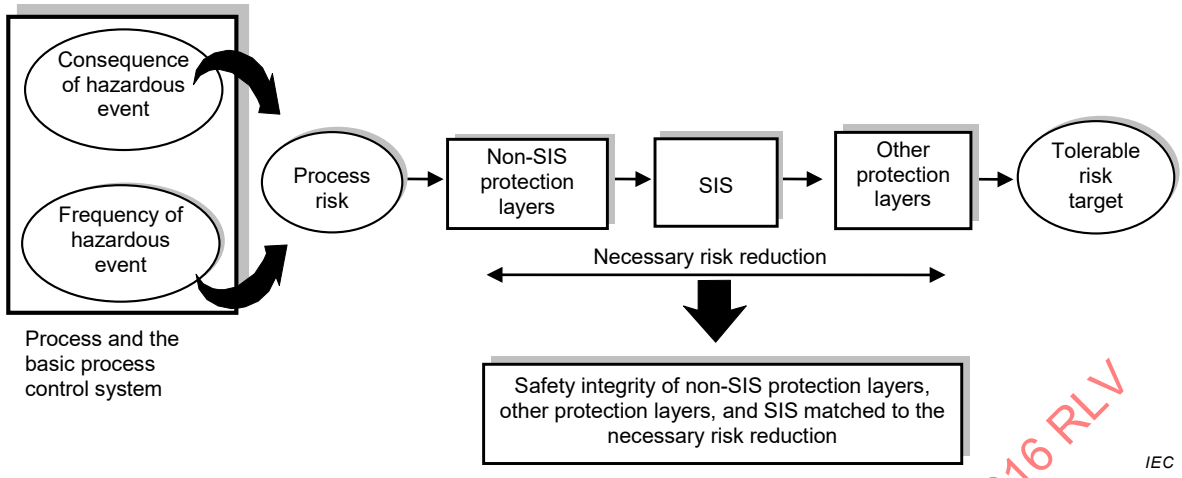


Figure A.2 – Risk and safety integrity concepts

A.5 Allocation of safety requirements

The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the SIS and other protection layers is shown in Figure A.4. The requirements of the allocation process are given in Clause 9 of IEC 61511–1: -.

The methods used to allocate the safety integrity requirements to the SIS, 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 through I inclusive).

A.6 Hazardous event, hazardous situation and harmful event

The terms “hazardous event” and “hazardous situation” are used often in the subsequent annexes illustrated herein. Figure A.3 is intended to illustrate the difference between the terms by showing the progression from hazardous event to hazardous situation through loss of control to the occurrence of a harmful event.

Figure A.3 uses harm to people but can equally apply to the outcome of harm to the environment, or damage to property.

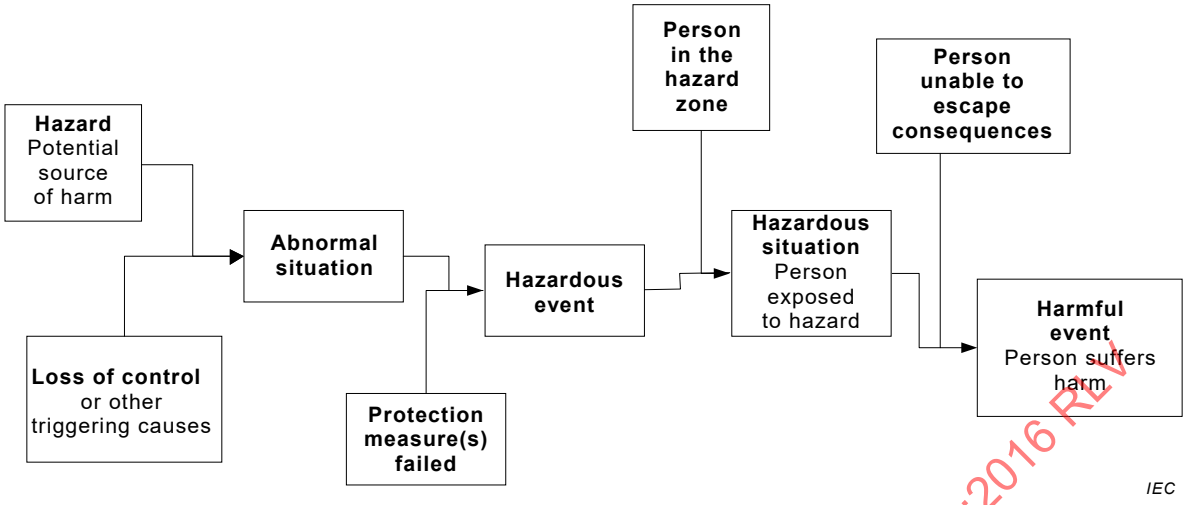


Figure A.3 – Harmful event progression

Figure A.3 shows how loss of control, or any other initiating cause result in an abnormal situation and place a demand on protective measures, such as safety alarms, SIS, relief valves etc. A hazardous event results when a demand occurs and the relevant protective measures are in a failed state, and do not function as intended. A hazardous event in and of itself does not necessarily cause harm, but should a person(s) be in the impact zone (or effect area), thus exposed to the hazardous event, this results in a hazardous situation. If the person is unable to escape the harmful consequences of exposure, this is characterized as a harmful impact due to the personnel injury.

A.7 Safety integrity levels

In the IEC 61511-1:2016, four SILs are specified, with SIL 4 being the highest level and SIL 1 being the lowest.

The target failure measures for the four SIL are specified in Tables 4 and 5 of IEC 61511–1: -. Two parameters are specified, one for SIS operating in a low demand mode of operation and one for SIS operating in a continuous/high demand mode of operation.

NOTE For a SIS operating in a low demand mode of operation, the target failure measure of interest is the average probability of failure to perform its designed function on demand. For a SIS operating in a continuous/high demand mode of operation, the target failure measure of interest is the average frequency of a dangerous failure, see 3.2.83 and Table 5 of IEC 61511-1:2016.

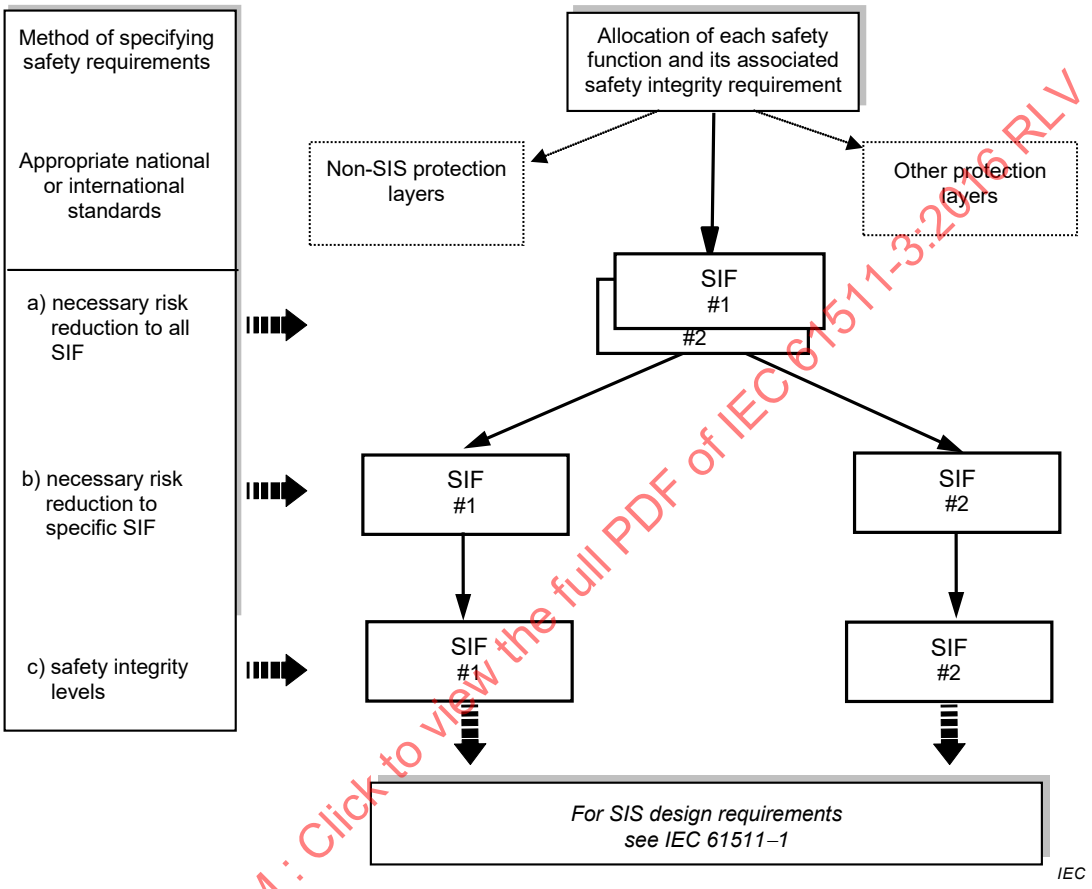
A.8 Selection of the method for determining the required safety integrity level

There are a number of ways of establishing the required SIL for a specific application. Annexes B to I 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 (see Figure A.4);
– the information available on SIS currently in use in the particular applications, such as those described in industry standards and practices.

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.

It is important that whichever method(s) are selected for application, that the site risk criteria should be used for the assessment.



NOTE Safety integrity requirements are associated with each SIF before allocation (see IEC 61511-1:2016, Clause 9).

Figure A.4 – Allocation of safety requirements to the non-SIS protection layers and other protection layers

Annex B
(informative)

Semi-quantitative method – event tree analysis

B.1 Overview

Annex B outlines how the target safety integrity levels (SIL) can be determined if a semi-quantitative approach is adopted. A semi-quantitative approach utilizes both qualitative and quantitative techniques and 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).

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

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008).

B.2 Compliance with IEC 61511-1:2016

The overall objective of Annex B is to outline a procedure to identify the required safety instrumented functions (SIF) and establish their SIL. The basic steps required to comply are the following:

a) Establish the safety target (tolerable risk) for the process;

b) Perform a hazard and risk assessment to evaluate existing risk for each specific hazardous event;

c) Identify safety function (s) needed for each specific hazardous event;

d) Allocate safety function (s) to protection layers;

NOTE Protection layers are assumed to be independent from each other. The allocation process can ensure that the common cause, common mode, and systematic failures are sufficiently low compared to the overall risk reduction requirements.

e) Determine if a SIF is required;

f) Determine required SIL of the SIF.

Step a) establishes the process safety target. Step b) focuses on the risk assessment of the process, and Step c) derives from the risk assessment what safety functions are required and what risk reduction they need to meet the process safety target. After allocating these safety functions to protection layers in Step d); it will become clear whether a SIF is required (Step e)) and what SIL it will need to meet (Step f)).

Annex B proposes the use of a semi-quantitative risk assessment technique to meet the objectives of the IEC 61511-1:2016, Clause 8. A technique is illustrated through a simple example.

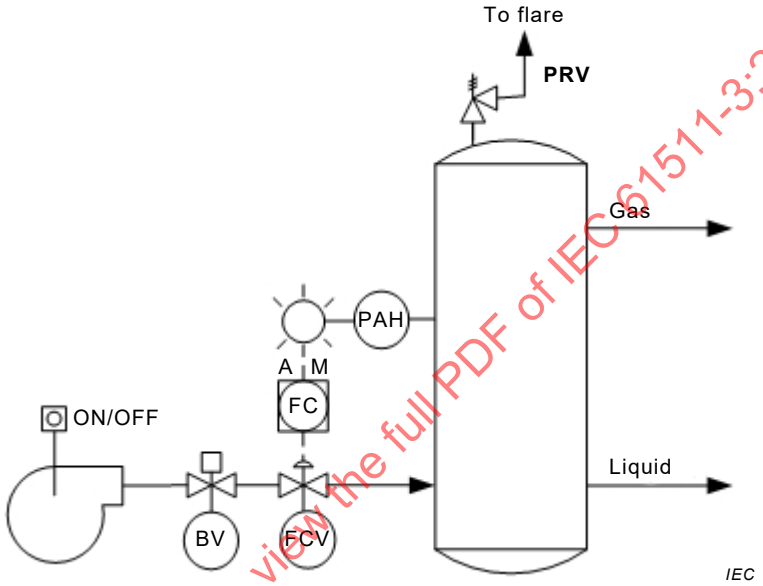
B.3 Example

B.3.1 General

Consider a process comprised of a pressurized vessel with a pumped in feed and two exits (liquid and gas) containing a mixture of gas and 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 flow 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, which is a pressure relief valve, to address the hazards associated with high vessel pressure. Releases from the pressure relief valve 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 instrumented protection systems and associated operator action(s).



Key

FC	Flow controller
FCV	Flow control valve
PAH	Pressure alarm high
BV	Block valve
PRV	Pressure relief valve

Figure B.1 – Pressurized vessel with existing safety systems

B.3.2 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 (or 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 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.

B.3.3 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. High pressure is a process deviation that could propagate into a hazardous event that causes various scenarios 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	Deviations	Causes	Consequences	Safeguards	Action
Vessel	High flow	Flow control loop fails	High flow leads to high pressure (see Note below)		
	High pressure	1) Flow control loop fails 2) External fire	Vessel damage and release to environment	1) High pressure alarm 2) Deluge system 3) Pressure relief valve	Evaluate design conditions for pressure relief valve release to environment
	Low/no flow	Flow control loop fails	No consequence of interest		
	Reverse flow		No consequence of interest		

NOTE For this example, assume the vessel can experience high pressure due to the inability of the downstream equipment to handle full gas flow from the vessel when the feed flow is too high.

B.3.4 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.

a) Identify process hazards;
b) Identify initiating events;
c) Develop hazardous event scenarios for every initiating event;

d) Identify protection layer composition;

NOTE 1 Safety functions are allocated to protection layers to safeguard a process and includes SIS and other risk reduction means (see Figure B.2).

NOTE 2 This step applies to the above example since it involves an existing process with existing protection layers.

e) Ascertain the frequency of occurrence of the initiating events and the reliability of existing safety functions using historical data or modelling techniques (for example, event tree analysis, failure modes and effects analysis, or fault tree analysis);

f) Quantify the frequency of occurrence of significant hazardous events;

g) Evaluate the consequences of all significant hazardous events;

h) Integrate the results (consequences and frequency of an accident) into risk assessment 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 function 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 led to the stated outcome and provides a system for life-cycle management.

For the illustrative example, one hazardous event – over-pressurization – 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 B.3.4 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 SIF.

B.3.5 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 over-pressurization, is caused due to the failure of the BPCS (e.g., flow control loop), 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, and the frequency of external fire is considered to be negligible in comparison. 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} per year. Note that each cause shown in Figure B.2 is assumed to be independent (i.e., no overlapping) of other causes, with failure rate expressed as events per year.

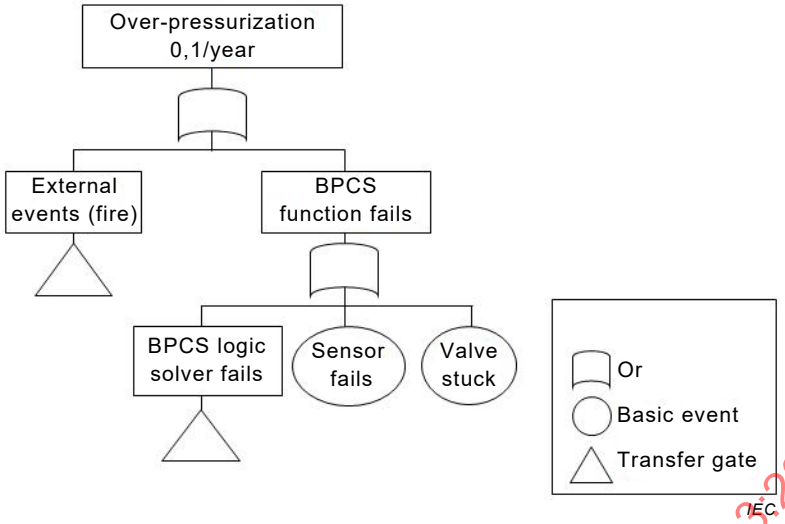


Figure B.2 – Fault tree for overpressure of the vessel

NOTE 1 Figure B.2 illustrates the fault tree without consideration of protective measures.

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 or predicted system performance. Figure B.3 shows the potential outcome scenarios that could occur given an overpressure condition. The results of the event modelling are: a) the frequency of occurrence of each event sequence; and b) the qualitative consequences of the event outcome.

In Figure B.3, five outcome scenarios are identified, each with a frequency of occurrence and a qualitative consequence. Outcome scenario 1 involves operator response to the high pressure alarm, occurs at a frequency of 8×10^{-2} per year and results in reduced production with no release. This is an acceptable design condition of the process and the operator is trained and tested on the appropriate response to achieve the risk reduction.

Furthermore, outcome scenarios 2 and 4 involve release of material to the flare, occurs at a combined frequency of $1{,}9 \times 10^{-2}$ per year ($9 \times 10^{-3} + 1 \times 10^{-2}$) and are also considered as a design condition of the process. The remaining outcome scenarios 3 and 5 have a combined frequency of occurrence of $1{,}9 \times 10^{-4}$ per year ($9 \times 10^{-5} + 1 \times 10^{-4}$) and result in vessel damage and release material to the environment (see Note 2).

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 flow sensor. Such common cause failure could lead to a significant increase in the frequency of occurrence for outcome 3 and hence the overall risk.

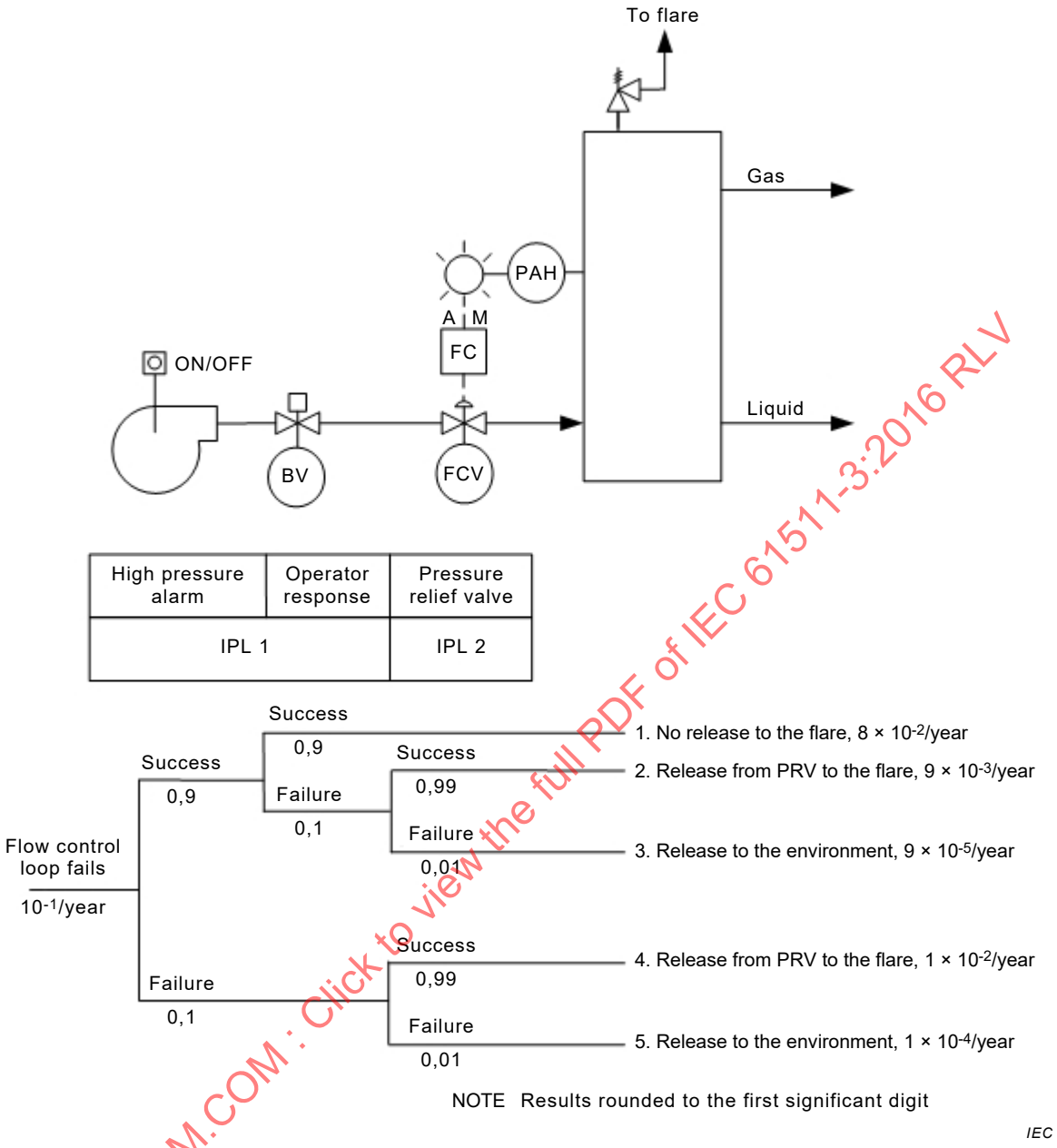


Figure B.3 – Hazardous events with existing safety systems

NOTE 2 In some applications the frequency and probability of failure on demand cannot be multiplied as shown in Figure B.3. This may be due to overlapping, common cause failure, and holistic dependencies between the various protection layers. See Annex J.

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

B.3.6 Events that do not meet the process safety target

As was stated earlier, plant specific guidelines establish the process safety target as: no release of material to the environment with a frequency of occurrence greater than 10^{-4} in one year. The overall frequency of environmental releases is 9×10^{-5} (scenario 3) + $1{,}0 \times 10^{-4}$ (scenario 5) = $1{,}9 \times 10^{-4}$ per year, which is greater than the process safety target. Given the frequency of occurrence of the hazardous events and consequence data in Figure B.3, additional risk reduction is necessary in order for outcome scenarios 3 and 5 to be below the process safety target.

B.3.7 Risk reduction using other protection layers

Protection layers of other technologies should be considered prior to establishing the need for a SIF implemented in a SIS. A deluge system is listed as a safeguard in Table B.1, but it does not prevent the vessel damage or release to the environment.

Given that the intent of the analysis is to minimise the risk due to a release of material to the environment, it can be assumed that the deluge system is not an acceptable risk reduction scheme for vessel damage or release to the environment. The deluge system does reduce the risk to personnel and for event escalation, which is not being assessed in this example.

B.3.8 Risk reduction using a safety instrumented function

The process safety target cannot be achieved using protection layers of other technologies. In order to reduce the overall frequency of releases to the atmosphere, a new SIL 2 SIF is required to meet the process safety target. The new SIF is shown in Figure B.4.

It is not necessary at this point to perform a detail design on the SIF. A general SIF design concept is sufficient. The goal in this step is to determine if a new SIL 2 SIF will provide the required risk reduction and allow the achievement of the process safety target. Detail design of the SIF will occur after the process safety target has been defined for the SIF. For this example, the new SIF uses dual, safety dedicated, pressure sensors in a 1oo2 configuration (not shown in Figure B.4) sending signals to a logic solver. The output of the logic solver controls the shutdown valve and the pump.

NOTE 1oo2 means that either one of the pressure sensors can initiate shutdown of the process.

The new SIL 2 SIF is used to minimize the frequency of a release from the pressurized vessel due to an overpressure. Figure B.4 presents the new protection 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 process safety target can be met provided the SIF can be evaluated to be consistent with SIL 2 requirements.

In Figure B.4, seven outcome scenarios are identified, each with a frequency of occurrence and a qualitative statement of consequence. The frequency of outcome scenario 1 is the same as previously discussed. Operator response results in reduced production at a frequency of 8×10^{-2} per year.

In this design case, successful operation of the SIS results in a shutdown of the process and occurs at a frequency of $1{,}9 \times 10^{-2}$ per year. The SIS reduces the process demand rate on the pressure relief valve. The frequency of scenario outcome 3 involving release from the PRV to the flare is reduced two orders of magnitude from the previous case to 9×10^{-5} per year. Scenario outcome 4, the hazardous event with release of material to the environment has a frequency of occurrence of 9×10^{-7} per year.

Scenario outcome 5 results in no release due to shutdown of the process by the SIS and occurs at a frequency of 1×10^{-2} per year. If the SIS fails to operate, the PRV provides the next safety function as shown in scenario outcome 6 and opens to the flare. The PRV opening occurs at a frequency of 1×10^{-4} per year. The total frequency of releases to the flare is determined by scenarios 3 and 6, which occur at an overall frequency of $9 \times 10^{-5} + 1 \times 10^{-4}$ or $1{,}9 \times 10^{-4}$. Releases from the flare are an acceptable design condition for the process. Scenario outcome 7 addresses the failure of all of the safety functions and occurs at 1×10^{-6} per year.

The total frequency of vessel failure with release to the environment (sum of frequencies of scenarios 4 and 7) has been reduced to $1{,}9 \times 10^{-6}$ per year, below the process 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 and holistic dependencies between the high pressure alarm and the SIL 2 SIF. There may also be potential for common cause failure and holistic dependencies between the safety functions and the failure of the BPCS flow sensor.

Such common cause failures may lead to a significant increase in the probability of failure on demand of the protective functions and hence a substantial increase in the overall risk.

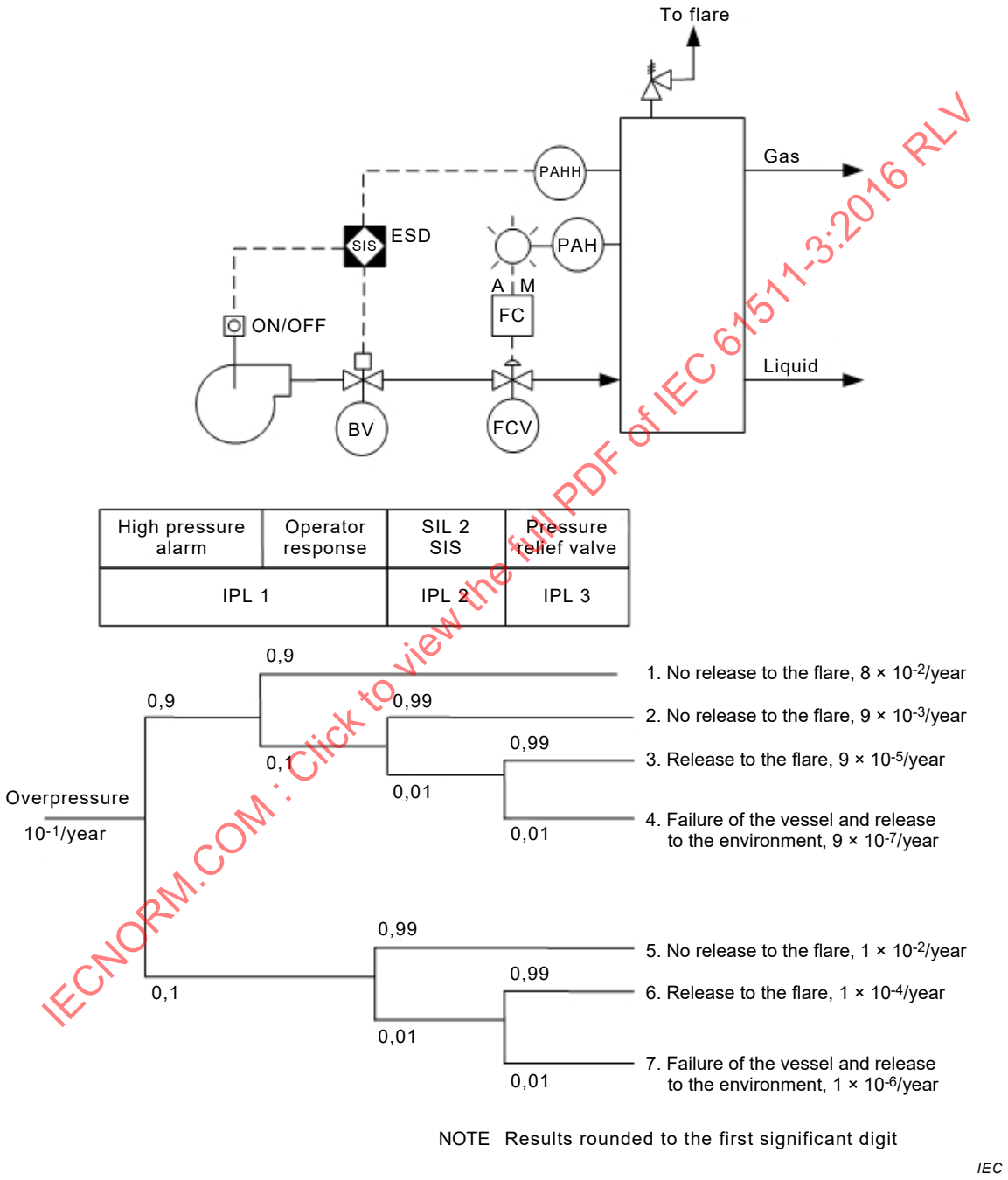


Figure B.4 – Hazardous events with SIL 2 safety instrumented function

Annex C
(informative)

The safety layer matrix method

C.1 Overview

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, 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 Figure C.1 below, each protection layer consists of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate process risk.

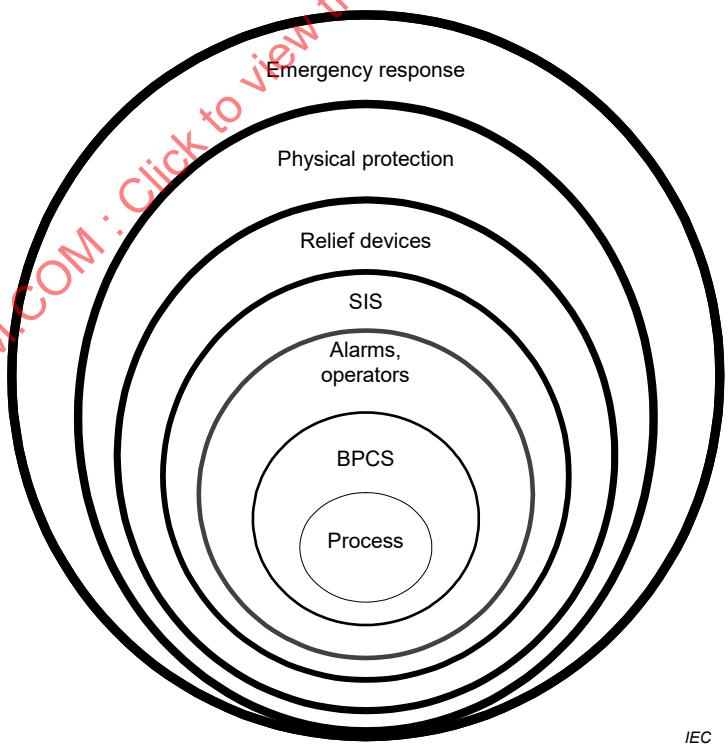


Figure C.1 – Protection layers

The concept of protection layers relies on three basic concepts:

a) 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.

b) 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 virtue of addressing both random failures and systematic failures in its design.

   • Auditability – a PL is designed to facilitate regular validation of the protective functions.

c) A safety instrumented system (SIS) protection layer is a protection layer that meets the definition of a SIS in IEC 61511-1:2016 Clause 3.2.69 (“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

– *Layer of Protection Analysis-Simplified – Process risk assessment,* American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

– CCPS/AIChE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, Wiley-Interscience, New York (2007)

– ISA 84.91.01: *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industries*, The Instrumentation, Society of Automation, 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 (or tolerable risk) 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 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;
– 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.

HAZOP is detailed in such standards as IEC 61882:2001. 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. Guidewords 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 additional safety measures or follow-up actions for management consideration.

Frequently, process experience and the HAZOP study results for a particular process can be generalized so as 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 assessment 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.

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

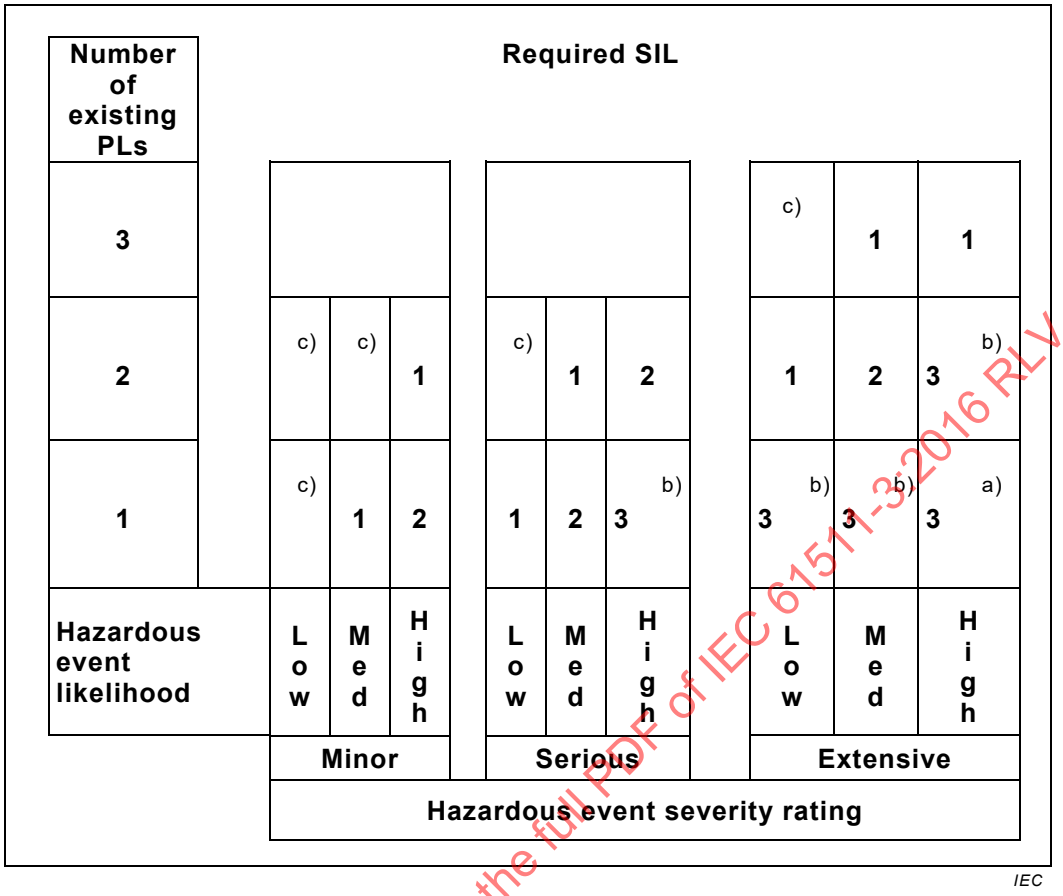
Type of events	Likelihood
	Qualitative ranking
Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels.	Low
Events such as dual instrument, valve failures, or major releases in loading/unloading areas.	Medium
Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	High
NOTE The system can be in accordance with the IEC 61511-1:2016 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 process safety target 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 process safety target.



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

b) One SIL 3 SIF may not provide sufficient risk reduction at this risk level. Additional review is required.

c) SIS protection layer is probably not needed.

NOTE 1 Total number of PLs – includes all the PLs protecting the process including the SIF being classified (i.e., number of PLs after the analysis is completed, including the new SIF (if required)).

NOTE 2 Hazardous event likelihood – refers to the likelihood that the hazardous event occurs without any of the PLs in service. See Table C.1 for guidance.

NOTE 3 Hazardous event severities – the impact associated with the hazardous event. See Table C.2 for guidance.

NOTE 4 This approach is not considered suitable for SIL 4.

Figure C.2 – Example of safety layer matrix

C.6 General procedure

a) Establish the process safety target.

b) Perform a hazard identification (for example, HAZOP studies) to identify all hazardous events of interest.

c) Establish the hazardous event scenarios and estimate the hazardous event likelihood using company specific guidelines and data.

d) Establish the severity rating of the hazardous events using company specific guidelines.

e) Identify existing PLs (Figure C.2). The estimated likelihood of hazardous events should be reduced by a factor of 10 for every PL.

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

g) Identify the SIL from Figure C.2.

h) The user should adhere to Clause C.1 b).

Annex D
(informative)

A semi-qualitative method: calibrated risk graph

D.1 Overview

Annex D is based on the general scheme of risk graph implementation described in Clause E.1 of IEC 61508-5:2010. Annex D has been adapted to be more suited to the needs of the process industry.

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

The approach uses a number of parameters, which together describe the nature of the hazardous situation when a SIS fails or is not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the SIL allocated to the SIF. 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 Annex D is to provide guidance on the above issues.

Annex D starts with protection against personnel hazards. It presents one possibility of applying the general risk graph of Figure E.1 of IEC 61508-5:2010 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 61511-1:2016). Typically, in the process sector, risk is a function of the following four parameters:

– the consequence of the hazardous event (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 SIF being considered) (W).

When a risk graph is used to determine the SIL 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 (see Table D.1) should represent the risk factors that relate best to the application characteristics involved. Consideration will also need to be given to the mapping of the SIL 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 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 can 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	Probability that exposed persons are able to avoid the hazardous situation which exists if the SIF 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 SIF 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:

a) 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.

b) To ensure the SIL selected for an application is in accordance with corporate risk criteria and takes into account risks from other sources.

c) 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 SIF under consideration. Each of the parameters is assigned a range of values such that when applied in combination, a graded assessment of the risk that exists in the absence of the safety 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 SIL. The relationship between the combinations of risk parameters and SIL is established by considering the tolerable risk associated with specific hazards. See Annex I as a description of the calibration process (Subclause I.2 and I.4.7).

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.

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 criterion for societal risk is based on the likelihood, *F*, of *N* or more 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. Guidance on developing criteria for risks giving rise to societal concerns is included in the UK HSE publication “Reducing Risks, Protecting People” ISBN 0 7176 2151 0.

The four risk parameters referred to in Clause D.2 are included in a decision tree of the form represented in Figure D.1. 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 SILs 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 SIL. 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.

The team normally considers each SIF in turn. The team will need comprehensive information on the process and the likely number of persons exposed to the risk. The team should include

a person with previous experience of using the risk graph method and understands the basic concepts that the method is based on. The chairman should ensure that everyone feels free to ask questions and express views.

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 and relates to the probability of a fatality should the hazardous event occur, The P parameter is a measure that relates to preventing the hazardous event. 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.

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.

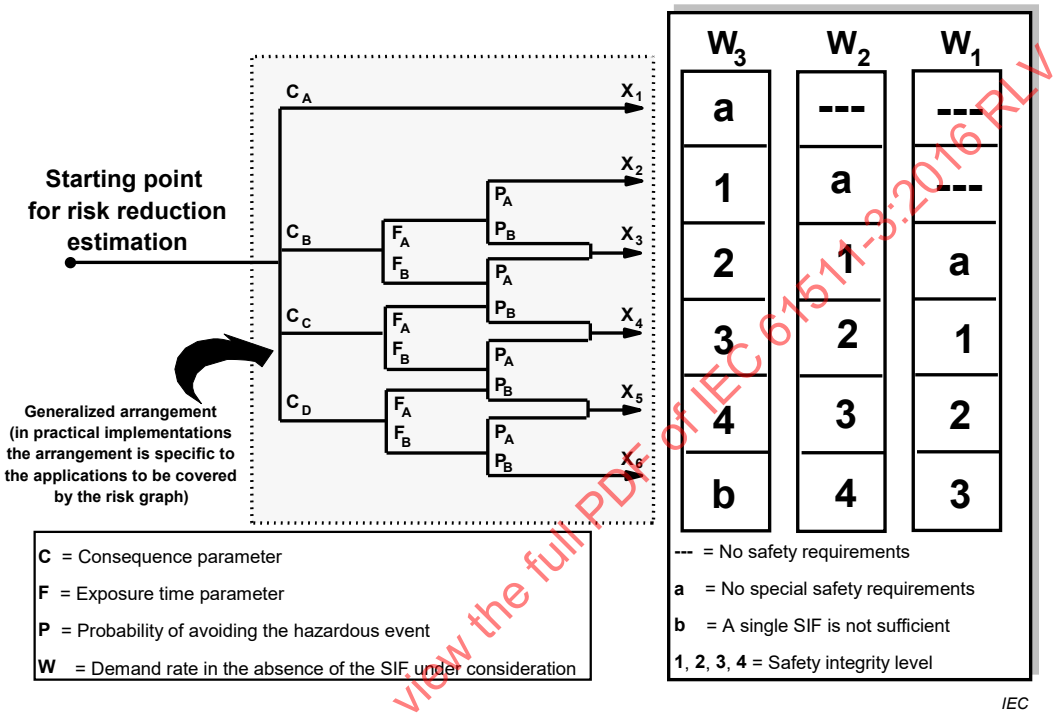


Figure D.1 – Risk graph: general scheme

Figure D.1 should not be used without re-calibration to align with site risk criteria. Any site without appropriate risk criteria should not attempt to use this method. The way in which calibration is carried out will depend on how the tolerable risk criteria are expressed. Parameter descriptions should be adjusted so that they fit with the range of intended applications and the risk tolerability. Values of C, F, P or W may be modified. Table D.2 shows an example calibration where the value of W is adjusted by a calibration factor D so as to align with specified risk criteria.

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

Risk parameter		Classification	Comments
Consequence (C) Number of fatalities 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. The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: 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	CA CB CC CD	Minor injury Range 0,01 to 0,1 Range >0,1 to 1,0 Range >1,0	a) The classification system has been developed to deal with injury and death to people. b) For the interpretation of CA, CB, CC and CD, the consequences of the accident and normal healing should be taken into account.
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 FA 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.	FA FB	Rare to more frequent exposure in the hazardous zone. Occupancy less than 0,1 Frequent to permanent exposure in the hazardous zone	c) See comment a) above.
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	PA PB	Adopted if all conditions in column 4 are satisfied Adopted if any one of the conditions are not satisfied	d) PA 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 h 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.	W1	Demand rate less than 0,1 D per year	e) The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS.

Risk parameter		Classification	Comments
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. Demand rate (W) is equal to the demand rate on the SIF under consideration.	W2 W3	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	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 3.2.39.2 of IEC 61511-1:2016. f) D is a calibration factor, the value of which should be determined so that the risk graph results in a level of residual risk which is tolerable taking into consideration other risks to exposed persons and corporate criteria. The numeric values to be used against each value of W in the table should be derived by undertaking risk graph calibration as described in Clause D.3 or Annex I.
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 can be agreed with those involved, taking into account tolerable risk, see Clauses 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. Table D.3 shows consequences in environmental terms. 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.

Table D.3 – General environmental consequences

Risk parameter		Classification	Comments
Consequence (C)	CA	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
	CB	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
	CC	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
	CD	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. 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 although the value of the calibration factor D may need to be modified to align with environmental risk criteria.

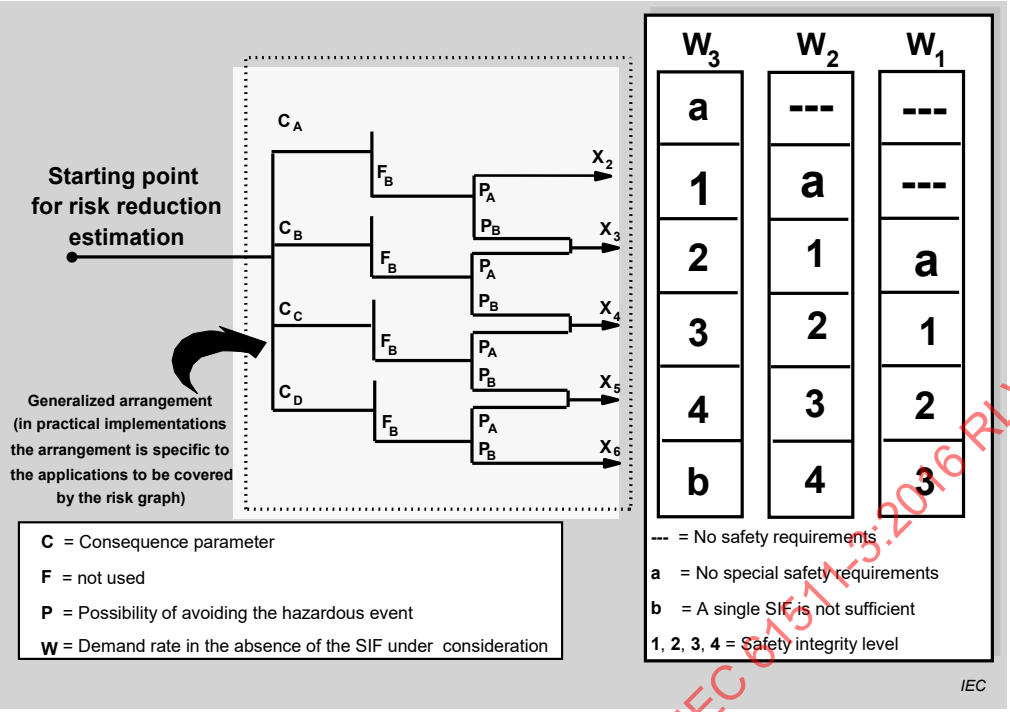


Figure D.2 – Risk graph: environmental loss

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 although the value of the calibration factor D may need to be modified to align with asset risk criteria.

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.

Annex E
(informative)

A qualitative method: risk graph

E.1 General

Annex E describes the risk graph method for determining the safety integrity levels (SIL) of the safety instrumented functions (SIF). This is a qualitative method that enables the SIL of a SIF to be determined from knowledge of the risk factors associated with the process and basic process control system (BPCS).

The approach uses a number of parameters which together describe the nature of the hazardous situation when SISs fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the SIL allocated to the SIF. 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.

The method presented in Annex E is shown in more detail in VDI/VDE 2180 (2015).

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:

– BPCS;

– process monitoring systems;

– SIS.

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.

BPCS 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. BPCS are in continuous operation or frequently requested to act and intervene before the reaction of a SIS is necessary (BPCS systems do not normally need to be implemented according to the requirements of the IEC 61511-1:2016).

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 the IEC 61511-1:2016).

SIS either prevents a dangerous fault state of the process plant (“protection system”) or reduces the consequences of a hazardous event.

If there is no SIS, a hazardous event leading to personnel injury is possible.

In contrast to the functions of a BPCS, the functions of SIS 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 SIS 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 SIS exists, although typical non-SIS 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 SIS in place (but all other risk reduction means are operating) – this is termed the probability of the unwanted occurrence.

This produces the following four risk parameters:

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

When a risk graph is used to determine the SIL of a SIF 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 SIL 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 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.

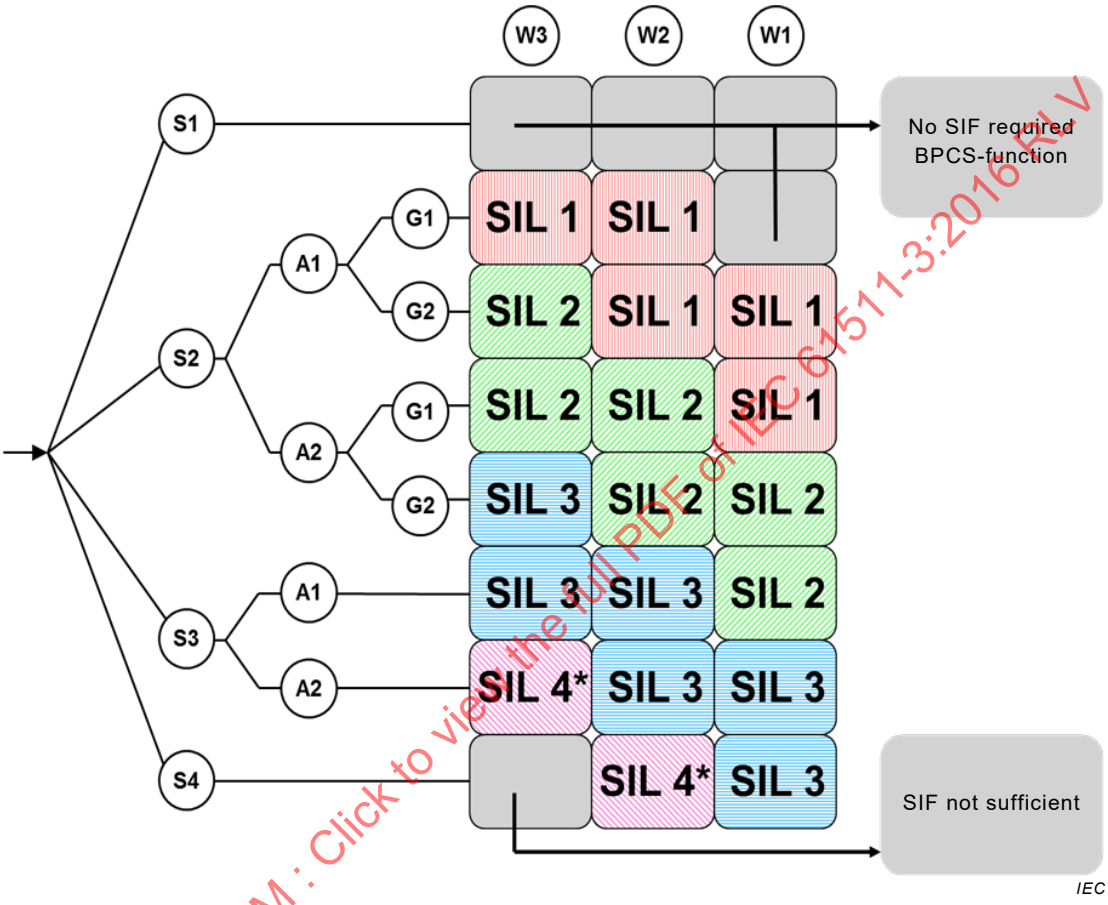
E.4 Risk graph implementation: personnel protection

The combination of the risk parameters described above enables a risk graph as shown in Figure E.1. Higher parameter indices indicate higher risk ($S_1 < S_2 < S_3 < S_4$; $A_1 < A_2$; $G_1 < G_2$; $W_1 < W_2 < W_3$). 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 SIL required for it.

When determining the risk to be prevented by SIS, the risk has to be assumed without the existence of the SIS 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 VDI/VDE 2180, 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 SIS and therefore generally the more stringent the requirements and resulting measures.

For the process industry, SIL 4 is not covered by SIS alone. Non-process control measures are needed to reduce the risk to at least SIL 3.



Key: * = SIF not recommended

NOTE Different colours are used to facilitate identification of different SIL values.

Figure E.1 – VDI/VDE 2180 Risk graph – personnel protection and relationship to SILs

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

Risk parameter		Classification	Comments
Consequence of the hazardous event. Severity (S)	S1	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.
	S2	Serious permanent injury to one or more persons; death of one person	
	S3	Death of several persons	
	S4	Catastrophic effect, very many people killed	
Frequency of presence in the hazardous zone multiplied with the exposure time (A)	A1	Rare to more frequent exposure in the hazardous zone	2) See comment 1 above.
	A2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the consequences of the hazardous event (G)	G1	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); – 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).
	G2	Almost impossible	
Probability of the unwanted occurrence (W)	W1	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 SIS (E/E/PE or other technology) but including any external risk reduction facilities.
	W2	A slight probability that the unwanted occurrences occur and few unwanted occurrences are likely	
	W3	A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely	

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 clear and understandable terms to ensure consistency in the method application.

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

Annex F
(informative)

Layer of protection analysis (LOPA)

F.1 Overview

Annex F describes a process hazard analysis tool called Layer of Protection Analysis (LOPA). The method starts with data developed during hazard identification 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 SIF, the LOPA methodology allows the determination of the appropriate SIL for the SIF.

Annex F 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:

Guideline 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.

See also IEC 61511-2: -, Clause F.11 for example applications of LOPA.

The values illustrated in Annex F should not be taken as generic and used in specific layer of protection analysis applications.

The SIS safety life-cycle defined in IEC 61511-1:2016 requires the determination of a SIL 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 the SIL of the SIF. 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 identification process. Table F.1 shows the relationship between the data required for the Layer of Protection Analysis (LOPA) and the data developed during the hazard identification process (HAZOP study for this example). Figure F.1 shows a typical spreadsheet that can be used for the LOPA.

LOPA analyses hazards to determine if SIFs are required and if so, the required SIL of each SIF.

F.2 Impact event

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

F.3 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.

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.2 F.13.2	Severity level F.3 F.13.2	Initiating cause F.4 F.13.3	Initiation likelihood per year F.5 F.13.4	General process design F.13.5	BPCS F.13.6	Alarms, etc. F.13.7	Additional mitigation, restricted access, F.7 F.13.8	IPL additional mitigation dikes, pressure relief F.7 F.13.9	Inter-mediate event likelihood per year F.9 F.13.10	SIF integrity level F.10 F.13.11	Mitigated event likelihood per year F.11 F.13.11	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 0,01	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	0,1	PRV 0,01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC

Key

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

NOTE If independent protection layers have not been properly selected frequency and probability of failure on demand cannot be multiplied as shown in Figure F.1. See Annex J.

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.4 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.5 Initiation likelihood

Likelihood values of the initiating causes occurring, in events per year, are entered into column 4 of Figure F.1. Table F.3 shows typical initiating cause likelihoods. The experience of the team is very important in determining the initiating cause likelihood.

Values in Table F.3 are not to be used for specific assessments (see Note 1).

Table F.3 – 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	$f < 10^{-4}$, /year
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	$10^{-4} < f < 10^{-2}$, /year
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	$10^{-2} < f < 100$, /year
NOTE 1 This table is illustrative. These values cannot be taken as generic frequencies and cannot be used in specific assessments. NOTE 2 "*f*" = Initiating event frequency (initiating event likelihood).		

F.6 Protection layers

Figure 2 in Clause 1 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.8).

Process design to reduce the likelihood of an impact event from occurring, when an initiating cause occurs, is 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 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.4.

Values in Table F.4 are not to be used for specific assessments (see Note).

Table F.4 – Typical protection layers (prevention and mitigation) PFD_{avg}

Protection layer	PFD_{avg}
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	$1,0 \times 10^{-1}$ to $1,0 \times 10^{-2}$
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)

NOTE The figures in Table F.4 are illustrative of the range of values that could appear in assessments. These values cannot be taken as generic probabilities and used in specific assessments. Human error probabilities can be appropriately assessed on a case by case basis.

F.7 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 PFD_{avg} for all mitigation layers and list them in column 6 of Figure F.1.

F.8 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 10-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;
  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 (IPL).

F.9 Intermediate event likelihood

The intermediate event likelihood is calculated by multiplying the initiating likelihood (column 4 of Figure F.1) by the PFD_{avg} 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 process safety target level 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 SIS are applied. If inherently safe design changes can be made, Figure F.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.10 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.11 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.12 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) × (probability of ignition) × (probability of a person in the area) × (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) × (probability of a person in the area) × (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.

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.13 Example

F.13.1 General

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

F.13.2 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 of Figure F.1, respectively.

F.13.3 Initiating cause

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 of Figure F.1.

F.13.4 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 of 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.13.5 General process 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 of Figure F.1 under process design.

F.13.6 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 of Figure F.1 under BPCS (0,1 is the minimum allowable for the BPCS).

F.13.7 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 of Figure F.1 under alarms.

F.13.8 Additional mitigation

Access to the operating area is restricted during process operation. Maintenance is only performed during periods of equipment shutdown and lockout. 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 of Figure F.1 under additional mitigation and risk reduction.

F.13.9 Independent protection layer(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 plugging 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 of Figure F.1 and assigned a PFD_{avg} of 0,01 based on previously discussed operating experience and published industry data.

F.13.10 Intermediate event likelihood

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

F.13.11 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 of 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 of Figure F.1.

F.13.12 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 of Figure F.1 under initiation likelihood.

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 of 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) × (Probability of fatal injury due to fire) = 0,5.

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.

Annex G
(informative)

Layer of protection analysis using a risk matrix

G.1 Overview

Annex G describes a hazard and risk assessment method that uses layer of protection analysis (LOPA) to identify the safety functions that reduce the frequency of loss of primary containment (LOPC) events to a tolerable level. The method encourages the implementation of proactive safeguards that prevent the LOPC, but allows the consideration of consequence mitigation systems as necessary. When consequence mitigation systems are implemented, the method requires the explicit examination of the outcome resulting from the mitigation system deployment. Since the method does not determine the frequency of harm posed by the LOPC, this method does not consider post-release conditions, such as the probability of ignition or occupancy. This simplifies the method and focuses the assessment team on reducing LOPC events through inherently safer design and proactive layers of protection.

This method uses a risk matrix to communicate the risk criteria to the assessment team. The risk matrix has been calibrated to account for the consequence severity potentially posed by the LOPC event. The criteria include consideration for safety, environmental, and economic loss potential.

The method examines hazardous events identified using any hazard identification technique appropriate for the process lifecycle step. At a minimum, the hazard identification should describe the hazardous events that were assessed and should identify the initiating cause(s) and the safeguard(s) that prevent or mitigate the event(s).

The risk assessment is performed using LOPA where the process risk is determined and compared to a tolerable risk as defined by a semi-quantitative risk matrix. When the process risk is above tolerable, safety functions are identified and allocated to independent protection layers (IPLs) as shown in Figure G.1 (adapted from CCPS, 2007). Some IPLs are proactive and act to prevent the hazardous event from occurring. Others are reactive and act to reduce the harm caused by the hazardous event.

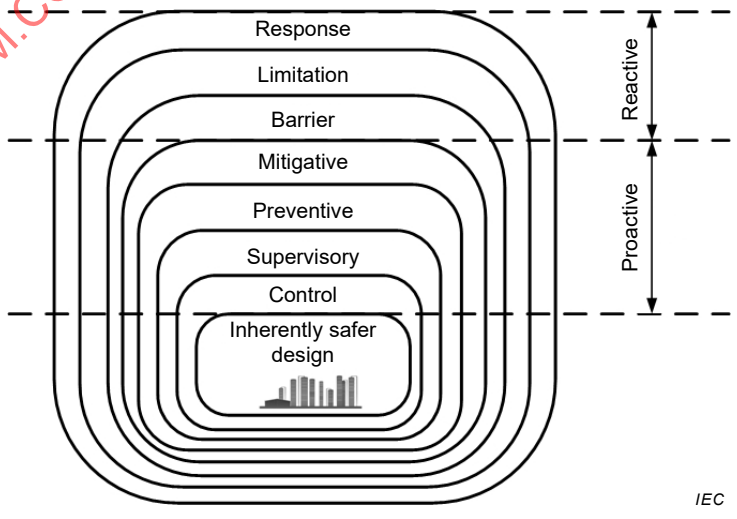


Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL

This method encourages the selection of proactive IPL, which reduce the frequency of the hazardous event (e.g., loss of containment or equipment damage). The use of any protection layer requires the additional consideration of the secondary consequence that results from their successful operation. This is particularly true of mitigative layer IPLs – see step 7 below.

When the study is completed, the identified safety functions have been allocated risk reduction in accordance with guidelines that are established for each type of IPL and associated function. When risk reduction is allocated to a SIS, this risk reduction yields a SIL in accordance with IEC 61511-1:2016 Table 4.

This method does not consider the duration of the operating mode when analysing sequenced, batch, start-up or maintenance risk. In this method, the risk of each operating mode should be reduced to the tolerable frequency regardless of the amount of time the process is in a particular operating mode.

The tolerable frequency for a hazardous event is determined by assessing the worse credible scenario consequence in terms of the health and safety impact to plant personnel and the public, environmental impact, and economic impact (property and business losses). The team is expected to qualitatively estimate the worst credible consequence regardless of likelihood and identify IPLs to reduce the event risk. Again, since this method seeks to reduce the hazardous event frequency (e.g., loss of primary containment or equipment damage), this method does not consider the use of conditional modifiers for occupancy, ignition or fatality, which are typically used to assess the frequency of specific types of harm caused by the event.

NOTE 1 This method leverages the availability of the team and information to assess economic impact of loss of containment events. The implementation of any recommendations for economic-related events is determined by business approval processes.

NOTE 2 The frequency, probability and risk reduction values used are for illustration only and are not to be used as generic values for specific assessments.

Annex G 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 references:

Layer of Protection Analysis Simplified – Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7.

Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design, Welding Research Council, PO Box 1942, New York, NY 10156, 2005, ISBN 1-58145-505-4.

Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system, American Petroleum Institute, 1220 L Street, NW, Washington, D.C. 20005, 2007.

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2007, ISBN 0-4719-7940-6.

Guidelines for Initiating Events and Independent Protection Layers in LOPA, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2015, ISBN: 978-0-470-34385-2.

G.2 Procedure

G.2.1 General

This LOPA procedure results in the identification of the IPLs that can reduce the process risk in accordance with the risk criteria. The following is a step-by-step description of the work process, which is shown graphically in Figure G.2.

G.2.2 Step 1: General Information and node definition

The team members, attendance date, study date, and document revision number are recorded in the Worksheet. The facilitator reviews the node boundary to ensure that each team member is familiar with the process operation and flow sheet (Figure G.3). The P&IDs under review are recorded along with any other documentation reviewed by the team during the study.

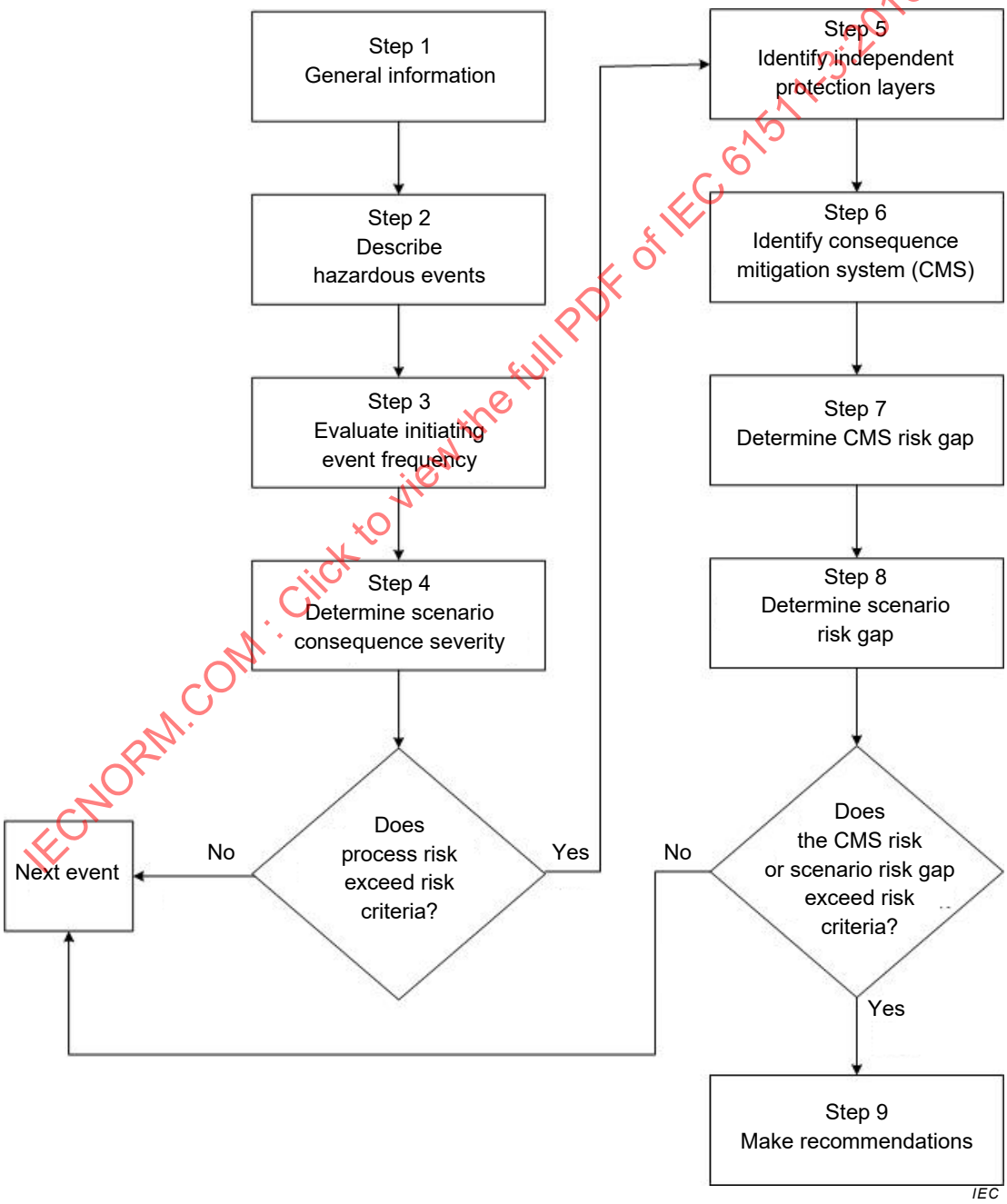
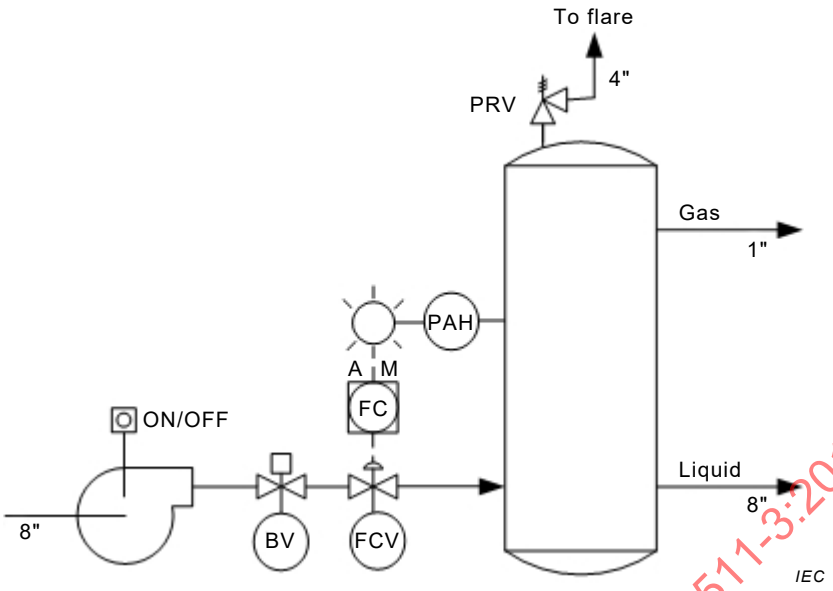


Figure G.2 – Work process used for Annex G



Key

FC	Flow controller
FCV	Flow control valve
PAH	Pressure alarm high
BV	Block valve
PRV	Pressure relief valve

Figure G.3 – Example process node boundary for selected scenario

G.2.3 Step 2: Describe hazardous event

Deviation or What-if? or FMEA: The team should describe the hazardous event selected for review including the deviation, what-if question, or failure mode that was analysed during the hazard identification and how the event propagates to the loss of containment or equipment damage.

Table G.1 is an excerpt from a HAZOP performed on the node illustrated by Figure G.3. This is one of what may be many scenarios that result in overpressure in this process unit. This scenario was selected for illustration purposes.

Hazardous event description: The event propagation should be clearly, yet concisely, described from the process hazard to the worst credible consequence assuming no safeguards. It is important to thoroughly describe the hazardous event, so that each team member understands what is being analysed. It should also be recognized that this documentation assists in the management of change process and in future revalidations, so it is important that the description be clear and easily understood.

As an example, Table G.2 lists a high-pressure deviation that is caused by a flow control loop failure and results in pressure that exceeds the Maximum Allowable Working Pressure (MAWP) of the vessel. The consequence is stated as “High flow leads to pressures above 1,5 × MAWP. Potential vessel damage and release to environment within 5 minutes.” (Note that this 1,5 MAWP is only allowed by certain vessel design codes). This description provides later teams with an understanding of the degree of overpressure and the speed with which pressure propagates to an unacceptable level.

Table G.1 – Selected scenario from HAZOP worksheet

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Causes	Consequence	Rank Consequence		Safeguards	Risk Ranking		PHA Recommendation
			Cat	S		L	RR	
1. High pressure	1. Flow control loop fails	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes.	S	4	1. High pressure alarm	B	2	
			E	4		B	2	
			A	3	2. High pressure shutdown of inlet block valve	B	1	
					3. Pressure relief valve			
					4. Operator response to high pressure alarm			

NOTE See Table G.4 for consequence categories and severity ranking.

Table G.2 – Selected scenario from LOPA worksheet

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity(S) and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes.	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1.Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	10
		E	4	1 000								
		A	3	100								

NOTE See Table G.4 for consequence categories and severity ranking.

Table G.2 continued at step 6

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+ CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. None, Vents to flare	100	S	1	TR	10	TR	1 000	1000	TR		
			E	1	TR		TR	1 000		TR		
			A	1	TR		TR	100		TR		

G.2.4 Step 3: Evaluate initiating event frequency

Once the hazardous event is described, the initiating cause(s) that lead to the hazardous event are documented. An event may be initiated by a single initiating cause or multiple causes. The team should consider various types of causes, such as human error, equipment failures, procedural errors, etc.

There may be instances where the team deems there is no credible cause or combination of causes. This may be due to inherently safe process design or because the occurrence of the scenario would violate the laws of chemistry or physics. In these cases “No credible initiating cause” should be listed in the initiating cause portion of the worksheet along with an explanation of the reasoning, and the team should continue to the next scenario.

Frequency: The frequency of the initiating event is evaluated without the consideration of any IPLs (safeguards). Guidance is provided in Table G.3 based on industry published data and good engineering practice. The team should determine whether the data is appropriate based on plant historical performance or experience with the initiating cause(s) under similar plant conditions. If the team determines that a higher frequency is warranted (e.g., 1/year rather than 1/10 years), the reasoning is documented and the revised number is entered into the worksheet. In this example, the frequency of flow control loop failure is 1/10 years.

Enabling conditions: Some process deviations can lead to hazardous events only in the presence of a co-incident condition, called an enabling condition. This procedure allows the consideration of an enabling condition, when the condition is independent of the initiating cause and is necessary for propagation of the hazardous event. The combination of the enabling condition and the initiating cause results in the propagation of the hazardous event.

The frequency of the initiating event can be estimated based on the average probability of the enabling condition being present and the frequency of the initiating cause. As an example, if the operator leaves a valve open incorrectly and a process upset downstream occurs, there could be backflow through the open valve. The process upset is assumed to happen 1/year. An operator opens and closes the valve 3 times per day. Failure is assumed 1/100 opportunities. Valve position is verified every 8 hours (by the next shift operator). So the average probability of the valve being open is:

P_{avg}(open) = (3/24 hours) × (1/100) × 8 hours = 0,01

The initiating event frequency is 0,01 × 1/year = 1/100 years.

Overall frequency. The overall event frequency is the highest frequency of the listed initiating causes. If a hazardous event has more than 3 initiating causes of similar frequency, consideration is given to assigning a higher overall event frequency based on an analysis of the common cause aspects of the causes. In the example (Table G.2), there is only one cause listed, so the initiating event frequency is 1/10 year.

Table G.3 – Example initiating causes and associated frequency

Initiating cause	Conditions	MTBF[a] in years
Basic Process Control Loop (BPCS)	Complete instrumented loop, including the sensor, controller, and final element.	10
Operator Action (SOP)	Action is performed daily or weekly per procedure. The operator is trained on the required action. {This value can be reduced by a factor of 10 (value=1 in 10 years) based on experience. The team should document job aids, procedures, and/or training used to achieve 1 in 10 years.}	1
	Action is performed monthly to quarterly per procedure. The operator is trained on the required action.	10
	Action is performed yearly, after turnaround or temporary shutdown per procedure. The operator is trained on the required action.	100
Instrumented Safety Device (OTHER)	Instrumented safety device spuriously operates, e.g., closure of block valve, pump shutdown, and opening of vent valve.	10

[a] The initiating causes listed can be assumed to occur more frequently (e.g., changed from 1/100 year to 1/10 year based on process experience. The values cannot be made less frequent without additional justification and approval by process safety. Additional analysis should be submitted as part of the justification. This would include human factors analysis, failure modes and effects analysis (FMEA), event tree analysis or fault tree analysis.

G.2.5 Step 4: Determine hazardous event consequence severity and risk reduction factor

The hazardous event is assessed to determine the worst credible consequence in terms of the health and safety impact to plant personnel and the public, environmental impact, and economic impact (property and business losses).

Severity: The consequence severity is assessed according to standardized definitions in Table G.4 "Consequence severity decision table". In the example (see Table G.2), the team determined that there was the potential for a significant flammable hydrocarbon release. Since an operator made frequent rounds through the unit, a fatality was possible. The consequence severity for safety was ranked as “4.” The environmental severity ranking was also determined to be consequence level 4, while the asset severity ranking was consequence level 3.

Risk assessment: The process risk is determined by the overall initiating event frequency (Step 3) and consequence severity (Step 4). These ranking are used as input to Table G.8 Risk reduction factor matrix. The matrix shows the risk reduction factor (RRF) required to reduce the process risk to a tolerable level. If the RRF yields a result of TR (tolerable risk), the risk falls within the risk criteria without additional IPLs. Those hazardous events that indicate other than TR should be assessed further.

In the example (see Table G.2), a consequence severity of 4 and a frequency of 1/10 years results in a required risk reduction of 1 000 (see Table G.5).

In some instances, IPLs may not be required from a risk standpoint, but may be required by code, practice, or regulation. The requirements of codes, practices, or regulations supersede this procedure.

Table G.4 – Consequence severity decision table

RANK	SAFETY (S)	ENVIRONMENTAL (E)	ASSET (A)
5	Multiple fatalities across a facility and/or Injuries or fatalities to the public	Catastrophic off-site environmental damage with long-term containment and clean-up	Expected loss greater than $10,000,000 and/or substantial damage to buildings located off-site
4	Hospitalization of three or more personnel (e.g., serious burns, broken bones) and/or one or more fatalities within a unit or local area and/or Injuries to the public	Significant off-site environmental damage (e.g., substantial harm to wildlife) with prolonged containment and clean-up	Expected loss between $1,000,000 and $10,000,000 and/or extended downtime with significant impact to the facility operation and/or minor damage (e.g., broken windows) to buildings located off-site
3	Hospitalization injury (e.g., serious burns, broken bones) and/or multiple lost work day injuries and/or Injury to the public	On-site release requiring containment and clean-up and/or off-site release causing environmental damage with quick clean-up	Expected loss between $100,000 And $1,000,000 and/or downtime of several days severely impacting the facility operation
2	Lost work day injury and/or recordable injuries (e.g., skin rashes, cuts, burns) and/or minor impact to public	On-site release requiring containment and clean-up by emergency personnel and/or off-site release (e.g., odour) but no environmental damage	Expected loss between $10,000 and $100,000 and/or downtime of more than day causing impact to facility operation and/or reportable quantity event
1	Recordable injury and/or no impact to the public	On-site release requiring containment and clean-up by on-site personnel	Expected loss of less than $10,000 and/or downtime of less than a day with minor impact to the facility operation

Table G.5 – Risk reduction factor matrix

REQUIRED RISK REDUCTION FACTOR						
CONSEQUENCE SEVERITY	5	100 000	10 000	1 000	100	10
	4	10 000	1 000	100	10	TR
	3	1 000	100	10	TR	TR
	2	100	10	TR	TR	TR
	1	10	TR	TR	TR	TR
		1	10	100	1 000	10 000
		FREQUENCY (1 in x years)				

G.2.6 Step 5: Identify independent protection layers and risk reduction factor

Safeguards are identified during the H&RA, which provide some measure of protection against the hazardous event under review. Each identified safeguard is evaluated against the IPL criteria.

Not all safeguards meet the design and management criteria necessary to be classified as IPLs. It is also important to ensure adequate independence of the selected safeguards so that the potential for common cause, common mode, and systematic issues is sufficiently low compared to the overall risk reduction requirement.

Table G.6 provides guidance on the RRF for example safety functions that may be classified as IPLs. The risk reduction factor is based on specific IPL design and management criteria,

which is briefly described in Table G.6. The restrictions provided in the table shall be met for the IPL to be allocated the listed risk reduction.

A safeguard that does not meet the criteria may be listed in the worksheet with RRF=1, if desired. A safeguard may only be allocated a RRF>1, when the process safety information demonstrates that the safeguard meets the criteria.

In the example (see Table G.2), the team determined that there was not sufficient time for the operator to respond to the alarm. A previous analysis of the SIS showed that it achieved SIL 1, so the team allocated an RRF of 10 to it (see Table G.2).

G.2.7 Step 6: Identify consequence mitigation systems and risk reduction factor

The successful action of any IPL results in a new operating or shutdown state. This new state is referred to as the secondary consequence of the IPL. The risk associated with the secondary consequence shall be acceptable or additional/alternate IPL shall be applied. Since successful action of most mitigative proactive IPL and reactive IPL result in the reduction of the consequence severity, these IPL are collectively referred to as Consequence Mitigation Systems (CMSs).

CMS IPL, which act to reduce the harm resulting from the hazardous event, may be credited if a review (Note 1) verifies that the CMS IPL is designed and managed to address the particular hazardous event and (Note 2) determines that the secondary consequence risk is acceptably managed.

NOTE 1 If there are no documents to support the claim that the CMS IPL is properly designed, located, and maintained to reduce the consequence of the particular release scenario, no RRF may be taken.

NOTE 2 The successful action of a CMS IPL reduces the consequence of the hazardous event under review. The reduced consequence resulting from the proper functioning of the CMS IPL can still be unacceptable. The risk associated with the IPL's operation is determined by evaluating this secondary consequence severity and release frequency. This value is compared to the risk criteria to determine if additional risk reduction is required.

Table G.7 lists the CMSs considered during study and RRF for specific safety functions that may be classified as IPLs. It is important for the team to review the CMS to verify that the CMS is designed and managed to address the hazard scenario. Only CMS that proactively reduce the frequency of the primary consequence event (LOPC) are considered in this method.

In this example (see Table G.2), the team determined that the pressure relief valve was designed for overpressure caused by flow control loop failure. The team allocated an RRF of 100 to it.

Table G.6 – Examples of independent protection layers (IPL) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)

IPL	Conditions	RRF	PFD
Basic Process Control System (BPCS)	The BPCS IPL should be designed and managed to achieve the RRF. It is a typically a control loop whose normal action prevent the scenario. The BPCS IPL shall run in automatic mode during all operating phases where the hazard scenario could occur.	10	0,1
Operator response to alarm with ≥10 minutes response time (ALARM)	Operator response does not have to perform troubleshooting or diagnostics to take the action. Alarm may be implemented in the BPCS or independent of the BPCS.	10	0,1
Operator response to alarm with ≥40 minutes response time (ALARM)	Operator response requires minor troubleshooting or diagnostics prior to taking action. Alarm may be implemented in the BPCS or independent of the BPCS.	10	0,1
SIL 1 (SIS)	Safety Integrity Level 1	10	0,1
SIL 2 (SIS)	Safety Integrity Level 2	100	0,01
SIL 3 (SIS)	Safety Integrity Level 3	1 000	0,001

Table G.7 – Examples of consequence mitigation system (CMS) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)

CMS	Conditions	RRF	PFD
Pressure Relief Valve	Clean Service. Designed for the hazardous event	100	0,01
Vessel Rupture Disk	Designed for the hazardous event	100	0,01
Vacuum Breaker	Designed for the hazardous event	100	0,01
Overflow Line	Overflow line is designed to discharge to containment area which is sized to address the hazardous event. Any valves in line shall be administratively controlled to ensure the CMS is available when needed.	100	0,01

G.2.8 Step 7: Determine CMS risk gap

As with any IPL, there are two potential states when a process demand occurs: 1) success where the CMS works as designed and 2) failure where the CMS does not work as designed. In Step 7, the CMS risk is addressed by assessing the consequence when the CMS works as designed. In Step 8, the risk associated with the CMS not working as designed is assessed.

To determine the CMS risk (i.e., works as designed), it is necessary to first evaluate the severity of the secondary consequence. The consequence severity is assessed according to standardized definitions in Table G.4 "Consequence severity decision table". The CMS risk is determined by CMS consequence severity and the frequency of the CMS use. This frequency is determined by multiplying the overall initiating event frequency (Step 3) by the RRF of each IPL that prevents the initiating event from placing a demand on the CMS. These IPL were identified in Step 5.

The CMS risk is evaluated using Table G.5 RRF matrix. If the CMS risk gap is reduced to "TR," no further risk reduction is required. The team may identify functions that improve the risk reduction, if desired. If the CMS risk gap is 10, 100, 1 000, or 10 000, the team shall identify more IPLs, as appropriate. If these safeguards do not exist in the current design, recommendations are made.

In this example (Table G.2 and Figure G.4), the team determined that the flare availability was good at the site and the material released to the flare did not pose any unacceptable

consequence. When the PRV operates as designed, the scenario releases material to the flare and was determined to be at the tolerable risk level.

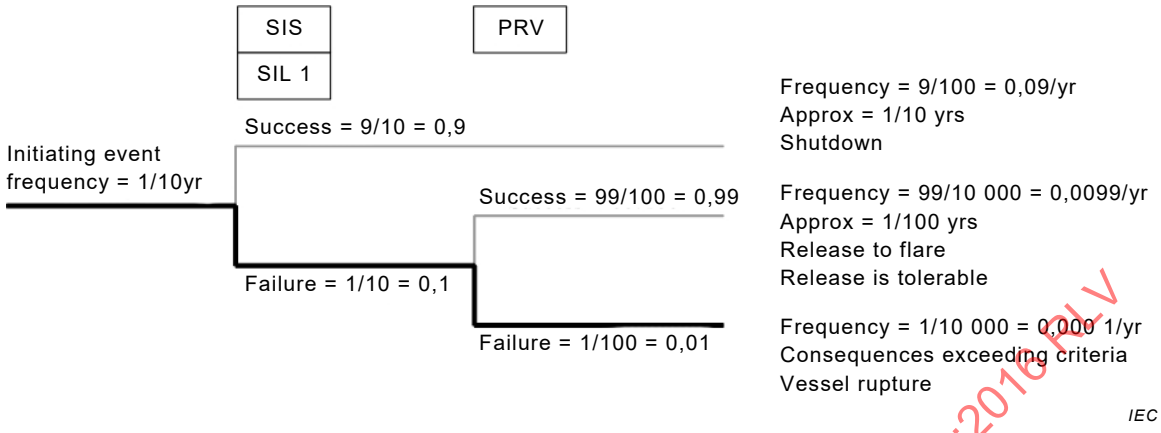


Figure G.4 – Acceptable secondary consequence risk

After the study was completed, a flare study determined that the release from the pressure relief valve could overload the flare and cause excessive backpressure in the relief system. Figure G.5 updates the event tree to show the revised secondary consequence – an overpressure event with significant consequence that occurs 1/100 years.

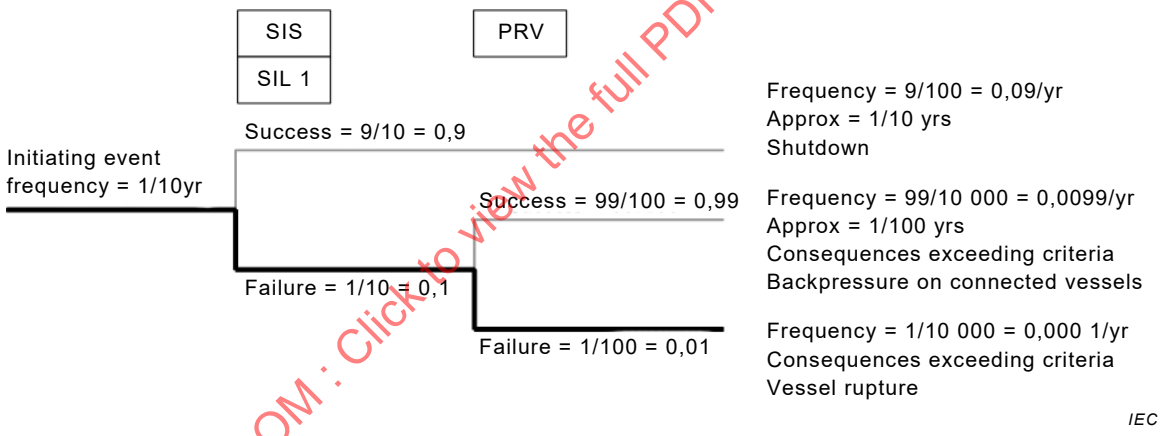


Figure G.5 – Unacceptable secondary consequence risk

Table G.8 updates Table G.2 with the revised assessment of the release from the PRV to the flare, showing the consequence created by the lifting of the pressure relief valve. The team determined that it was possible for the back-pressure generated by this relief scenario to cause overpressure in other units during a simultaneous relief event. The consequence of opening the relief valve was determined to be as high as the scenario considering failure of the PRV (see failure path for PRV). While the risk associated with the primary scenario (rupturing the vessel) is reduced to the tolerable risk (TR) level, the risk associated with the secondary consequence (overloading the relief system) is higher than the risk tolerance. The CMS risk gap is RRF = 100 for the safety and environmental consequence rankings, while the asset CMS is RRF = 10.

The CMS risk gap is determined by first evaluating the consequence of successful operation of the CMS using Table G.4. Then the challenge frequency for the CMS is determined by the scenario initiating event frequency (including enabling conditions) as reduced by the proactive IPLs operating prior to the CMS challenge (see the event trees Figures G.4 and G.5). The CMS risk gap is then taken from Table G.5.

Table G.8 – Step 7 LOPA worksheet *(1 of 2)*

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes. What If Consequence 1.1.1.1	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1. Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	10
		E	4	1 000								
		A	3	100								

Table G.8 *(2 of 2)*

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. Overloads relief system causing excessive backpressure	100	S	4	1 000	10	100	1 000	1000	TR		
			E	4	1 000		100	1 000		TR		
			A	3	100		100	100		TR		

Applying this new risk reduction requirement, it was determined that the SIS should be upgraded to SIL 3 in accordance with recommendations from API 521 *Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system* and ASME *Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design*. A SIL3 SIS reduced the demand frequency on the PRV and achieved an acceptable level of risk as shown in Figures G.5 and G.6.

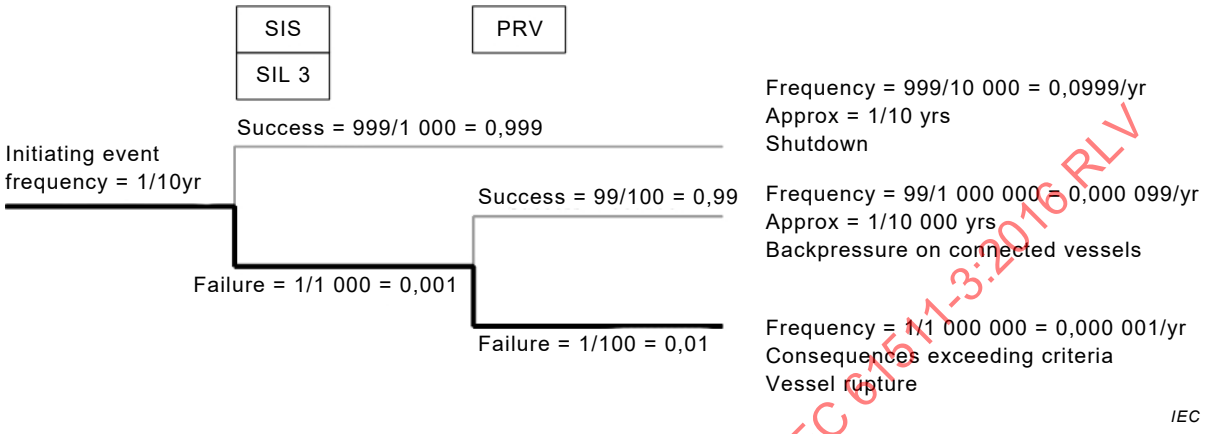


Figure G.6 – Managed secondary consequence risk

G.2.9 Step 8: Determine scenario risk gap

The scenario risk gap is determined from its consequence severity (Step 4) and its frequency given the presence of identified IPLs (Step 5) and CMSs (Step 6). Each frequency is determined by multiplying the overall initiating event frequency by the RRF of each IPL preventing the scenario and each CMS mitigating the scenario. IPLs were identified in Step 5 and CMSs were identified in Step 6.

The scenario risk is compared to the risk criteria as shown in Table G.9 using Table G.5. If the scenario risk gap is reduced to "TR," no further risk reduction is required. The team may identify functions that improve the risk reduction, if desired. If the scenario risk gap is 10, 100, 1 000, or 10 000, the team shall identify more IPLs or CMSs, as appropriate. If these do not exist in the current design, recommendations are made.

In this example (Table G.9), the scenario needed a total risk reduction of 1 000 to achieve the tolerable risk. With a SIL 3 SIS providing an RRF of 1 000 and a pressure relief valve providing an RRF of 100, an overall risk reduction of 100 000 is provided by the IPL design against overpressure of the vessel. Table G.9 shows the scenario risk gap meets tolerable risk.

G.2.10 Step 9: Make recommendations when needed

Recommendations shall be listed when the CMS or scenario risk gap is not reduced to "TR." Any listed recommendation should describe the safety function, classify it as a specific IPL type, and provide the required risk reduction. Other recommendations shall be listed by the team, if desired.

Table G.9 – Step 8 LOPA worksheet *(1 of 2)*

System Name: 1. Vessel 101 feed

Drawing: Drawing ABC-123

Design Intent & Process Control Method(s): Mixture X is fed into Vessel 101 for gas liquid separation

Deviation	Assess Consequence Severity (S) and RRF				Evaluate Initiating Event Frequency				Identify IPLs and RRF			
	Consequence	Cat	S	RRF RQ'D	Initiating Causes	Type	Freq.	Overall Freq.	Safeguards (Non-IPL)	IPLs	Type	RRF
1. High pressure	1. High flow leads to pressures above 1,5 x MAWP. Potential vessel damage and release to environment within 5 minutes. What If Consequence 1.1.1.1	S	4	1 000	1. Flow control loop fails	BPCS	10	10	1. Insufficient time for operator response to high pressure alarm	1. High pressure shutdown of inlet block valve	SIS	1 000
		E	4	1 000								
		A	3	100								

Table G.9 *(2 of 2)*

Identify CMS and RRF			Determine CMS Risk Gap					Determine Scenario Risk Gap			Recommendations (LOPA)	
CMS	CMS Consequence	RRF	Cat	S	CMS RRF RQ'D	Total IPL RRF	CMS RRF Gap	RRF RQ'D	Total RRF (IPL+CMS)	Scenario RRF Gap	Recommendation	Target RRF
Pressure relief valve	1. Overloads relief system causing excessive backpressure	100	S	4	1 000	1000	TR	1 000	100 000	TR		
			E	4	1 000		TR	1 000		TR		
			A	3	100		TR	1 000		TR		

Annex H
(informative)

A qualitative approach for risk estimation & safety integrity level (SIL) assignment

H.1 Overview

Informative Annex H provides one example of a qualitative approach for risk estimation and SIL assignment that can be applied to SIFs in the process industry.

NOTE 1 The methodology described in Annex H uses qualitative estimation of risk and is intended to be generally applied for the assignment of a SIL(s) to safety instrumented function (SIF(s)) in the process industry. The risk parameters (see Figure H.2) used whilst applying this methodology to particular processes and their specific hazards can be subject to agreement with those involved to ensure that the SIS can provide adequate risk reduction.

NOTE 2 The process industry risk graph parameters used in Annex H are from Table D.1.

NOTE 3 Annex H is not intended to be a definitive account of the method but is intended to illustrate the general principles.

For each hazardous event, the safety integrity requirements should be determined separately for the SIFs to be performed by the SIS (see IEC 61511-1:2016, Subclause 6.3.1, Tables 3 and 4).

Figure H.1 is an example of a practical way of carrying out a risk assessment at a specific hazardous event leading to estimation of a SIL for a SIF. This methodology should be performed for each hazardous event where the risk has to be reduced. Figure H.1 should be used in conjunction with the guidance information in Annex H.

It is important that the risk graph and its calibration is agreed to at a senior level within the organization taking responsibility for safety.

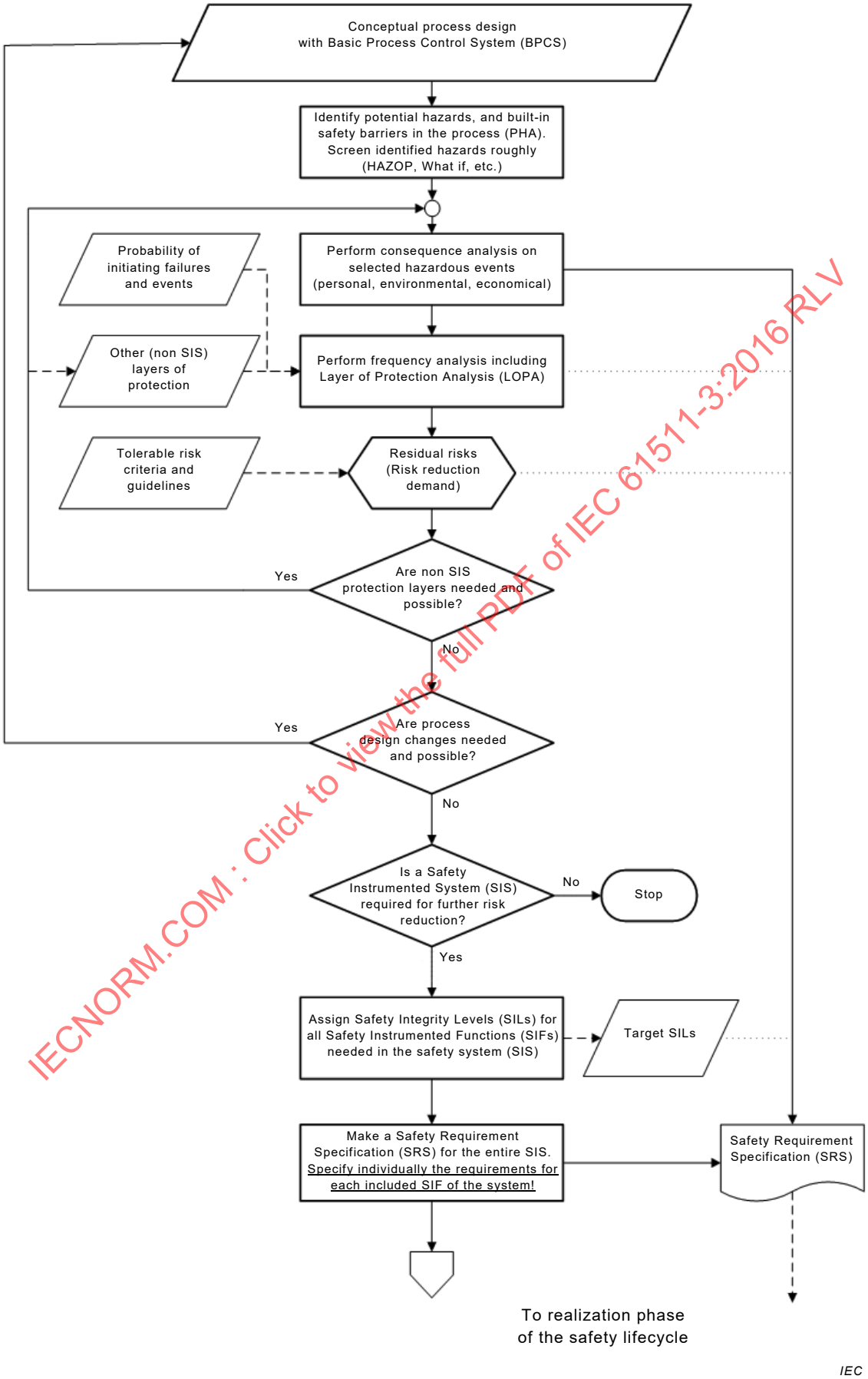


Figure H.1 – Workflow of SIL assignment process

Risk estimation is an iterative process; this means that the process may need to be carried out more than once.

H.2 Risk estimation and SIL assignment

H.2.1 General

Clause H.2 provides guidance on what and how to achieve risk guidance and SIL assignment.

H.2.2 Hazard identification/indication

Indicate the hazardous event, including those from reasonable foreseeable misuse, whose risks are to be reduced by implementing a SIF. List them in the hazardous event column in Table H.1.

Table H.1 – List of SIFs and hazardous events to be assessed

SIF No.	Hazardous event description	Safety Instrumented Function (SIF) description
01		
02		
03		
04		

H.2.3 Risk estimation

The risk graph matrix is used for SIL assignment for SIF. SILs are established by combining the risk graph consequence parameter C and the likelihood summarized as the risk graph parameters F, P and W. For each hazardous event SIL could be determined individually for health, environment and financial aspects. The overall target SIL of the considered SIF will be decided by the maximum determined SIL among these three aspects (health, environment and asset).

Risk estimation should be carried out for each hazardous event by determining the risk parameters shown in Figure H.2 and should be derived from the following:

– consequence of harm (C), and

– probability of occurrence of that harm, which is a function of:

  - occupancy parameter (F) which is the probability that the exposed area is occupied at the time of the hazardous event;
  - avoidance parameter (P) the probability that exposed persons are able to avoid the hazardous situation, which exists if the SIF fails on demand;
  - demand rate parameter (W) is the residual demand rate or frequency of the hazardous event if considering SIF is not implemented.

Risk related to the identified hazardous event	=	H.2.4 Consequence of the possible harm, C	&	H.2.5.2 Probability that the exposed area is occupied at the time of the hazardous event, F H.2.5.3 Probability that exposed persons are able to avoid the hazardous situation, P H.2.5.4 Residual demand rate or frequency of the hazardous event, W	H.2.6 Probability of occurrence of that harm

IEC

Figure H.2 – Parameters used in risk estimation

For each hazardous event many different sequences of events could exist that lead to this hazardous event. All these sequences should be handled separately because the probability of occurrence could differ (F, P and W).

H.2.4 Consequence parameter selection (C) (Table H.2)

This is the 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.

Severity level (C) is the estimated consequence of the hazardous event. Select proper level for health, hnvironmental and financial hazards. Fill in the chosen severity letter (A-F) for each individual hazard in the C column.

Determining proper severity levels presupposes consequence categories calibrated to meet the tolerable risk levels established by company risk management and authorities.

Table H.7 provides examples of consequence categories.

Table H.2 – Consequence parameter/severity level

Consequence parameter		
Severity Level		C
CF	Catastrophic	F
CE	Extensive	E
CD	Serious	D
CC	Considerable	C
CB	Marginal	B
CA	Negligible	A

H.2.5 Probability of occurrence of that harm

H.2.5.1 General

Clause H.2.5 provides guidance on key parameters related to probability of harm occurrence.

Each of the three parameters of probability of occurrence of harm (i.e., F, P and W) should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that under specification of a SIL does not occur.

H.2.5.2 Occupancy parameter section (Table H.3)

Assess 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).

Exposure probability (F) is the probability that the exposed area is occupied at the time of the hazardous event. The exposure probability is only valid for health risks (H). If occupancy is permanent or if credit already has been given for reduced occupancy likelihood when the health severity level was chosen, the "Permanent" alternative (F_D) shall be chosen. Exposure probability (F_C) shall be chosen if occupancy is frequent or if the occupancy is dependent on the hazardous situation. Exposure probability (F_B) should be chosen if the area is occupied just occasionally and human presence is obviously independent of the hazardous situation. Exposure probability (F_A) should only be chosen if the hazardous area is confined and human presence rare and independent of the hazardous situation. Fill in the selected correlating number (0-2) in the (F) column. A value of 1 for the occupancy parameter is predefined for the environmental and financial hazards.

Table H.3 – Occupancy parameter/Exposure probability (F)

Occupancy parameter			
Frequency of human presence in the hazardous zone. Credit for limited occupancy shall not have been taken choosing the consequence categories.			
Exposure probability			F
FD	Permanent	=1	2
FC	Frequent	0,1-1	2
FB	Occasionally	0,01-0,1	1
FA	Rare	<0,01	0

H.2.5.3 Avoidance parameter selection (Table H.4)

This parameter describes the probability for exposed persons to be able to avoid the hazardous situation which exists even when the SIF has failed 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.

Avoidance probability (P) is the probability of avoiding the hazardous event even if the considered safety function fails to prevent the event. Normal choice is P_B "Avoidance conditions not fulfilled".

P_A could be chosen individually for the health hazard (H) if all persons in the hazardous area are likely to be evacuated to a safe area in time if the SIF fails on demand. This requires that:

- persons have sufficient time to evacuate, and
- independent facilities for alerting and evacuating all people in the hazardous area are existing.

P_A could also be claimed if the hazardous event is likely to be avoided in time by manual operator actions. In this case, P_A is also relevant for environmental and financial hazards. This requires that:

- independent facilities for alerting the operator of the functional failure and for manually bringing the process to a safe state are available,
- at least 1 hour (minimum) is available between operator alert and the hazardous event.

Fill in the correlating number (0 or 1) of the selected avoidance parameter in the P column.

NOTE In Annex H, choosing P_A implies at least 90% probability that the hazard will be avoided.

Table H.4 – Avoidance parameter/avoidance probability

Avoidance parameter		
Probability of avoiding the hazardous event if the SIF fails on demand. Implies independent facilities provided to "shut-down" so hazard can be avoided or enable all persons to escape to a safe area. Conditions to be fulfilled for P_A: Facilities to alert operator that the SIS has failed Independent facilities to bring process to safe state Time between operator alert and hazardous event >1h		
Avoidance probability		P
P_B	Avoidance conditions not fulfilled	1
P_A	All avoidance conditions are fulfilled	0

H.2.5.4 Demand rate parameter selection (Table H.5)

The number of times per year that the hazardous event would occur in the absence of the SIF under consideration 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.

The demand rate parameter (W) is selected by estimating or calculating the residual demand rate or frequency of the hazardous event if the considered SIF is not implemented. This frequency can be determined by combining frequencies of failures and other initialising events leading to the hazardous event. Credit should be given for non SIS implemented safety barriers. The total risk reduction credit for barriers implemented in the normal control system (BPCS), including alarms and operator response, cannot be more than a risk reduction factor of 10 by definition in IEC 61511:- (risk reduction factor >0.1). Fill in the chosen number correlating to the estimated or calculated residual demand rate in column W.

Table H.5 – Demand rate parameter (W)

Demand rate parameter			
Demand rate			W
W9	Often	> 1/ y	9
W8	Frequent	1/1-3 y	8
W7	Likely	/3-10 y	7
W6	Probable	1/10-30 y	6
W5	Occasional	1/30-100 y	5
W4	Remote	1/100-300 y	4
W3	Improbable	1/300-1 000 y	3
W2	Incredible	1/1 000-10 000 y	2
W1	Inconceivable	1/10 000-100 000 y	1

H.2.6 Estimating probability of harm

For each hazardous event, and as applicable, for each aspect (health, environment; financial) add the points from the F, P and W columns and enter the sum into the column SIL in Table H.6.

H.2.7 SIL assignment

Use the risk graph matrix (Table H.6) to read out the SIL for each one of the aspects (health, environment and financial) by combining its severity letter (A-F) with its likelihood sum (1-12). The overall target SIL equals the maximum determined SIL.

Using Table H.6, the intersection point where the severity (C) row crosses the relevant column for likelihood (F+P+W), indicates what kind of action is required.

Example: For a specific hazard when looking at human health with a C assigned as catastrophic, an F as 1, and a P as 1 and a W as 3 then:

F+P+W = 1 + 1 + 3 = 5. Using Table H.6, this would lead to a SIL 2 being assigned to the SIF that is intended to mitigate the specific hazardous event.

Table H.6 may be used to record the results of a SIL assignment exercise when using the methodology described in Annex H.

In Table H.6, 'NR' corresponds to an 'Unclassified' safeguard since PFD>0,1.

Table H.6 – Risk graph matrix (SIL assignment form for safety instrumented functions)

Project: Process:
Issued by: Plant:
Date: System:
Revision: Chart Nr:

Consequence parameter			Risk graph matrix						Occupancy parameter				Avoidence parameter			Demande rate parameter			
			Likelihood sum (F+P+W)						*Frequency of human presence in the hazardous zone. Credit for limited occupancy must not have been taken choosing consequence categories!*				*Probability of avoiding the hazardous event **if the SIF fails on demand**. Implies **independent** facilities provided to "shut-down" so hazard can be avoided or enable all persons to escape to a safe area. Conditions to be fulfilled:*			Estimated SIF demand rate			W
Severity level		C	1-2	3-4	5-6	7-8	9-10	11-12					• Facilities to alert operator that the SIS has failed			W_9	Often	>1/ y	9
C_F	Catastrophic	F	NR	SIL1	SIL2	SIL3	SIL4	NO	Exposure rate			F	• Independent facilities to bring process to a safe state			W_8	Frequent	1/1-3 y	8
C_E	Extensive	E	NR	NR	SIL1	SIL2	SIL3	SIL4					• Time between operator alert and hazardous event			W_7	Likely	1/3-10 y	7
C_D	Serious	D	OK	NR	NR	SIL1	SIL2	SIL3	F_D	Permanent	= 1	2				W_6	Probable	1/10-30 y	6
C_C	Considerable	C	OK	OK	NR	NR	SIL1	SIL2	F_C	Frequent	0,1-1	2	Avoidance probability		P	W_5	Occasional	1/30-100 y	5
C_B	Marginal	B	OK	OK	OK	NR	NR	SIL1	F_B	Occasionally	0,01-0,1	1	P_B	Avoidance conditions not fulfilled	1	W_4	Remote	1/100-300 y	4
C_A	Negligible	A	OK	OK	OK	OK	NR	NR	F_A	Rare	<0,01	0	P_A	All avoidance conditions are fulfilled	0	W_3	Improbable	1/300-1 000 y	3
																W_2	Incredible	1/1 000-10 000y	2
																W_1	Inconceivable	1/10 000-100 000 y	1

SIF-NO:	Hazardous Event Description	Safety instrumented Function (SIF) Description	Consequence		Influence		Demande	Likelib	Integrity		Comments
			Harm	C	F	P	W	Sum	SIL	SIL	
01			*H*	**E**	1	1	3	**5**	1	**2**	
			E	**F**	*I*	1		**5**	2		
			F	**C**				**5**	NR		
02			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		
03			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		
04			*H*					**0**	0	0	
			E		*I*			**1**	0		
			F					**1**	0		

Table H.7 – Example of consequence categories

C	Human harm (H)	Probability loss of life		Max. health consequences due to the hazardous event	Additional comments to the health consequence categories
CF	Catastrophic	PLL > 1		Several (3 or more) dead. Many (10 or more) critical injured.	Several fatalities likely.
CE	Extensive	PLL = 0,1 – 1,0		Some (1 to 2) dead. Several (3 or more) critical injured.	Individual fatality/fatalities likely.
CD	Serious	PLL = 0,01 – 0,1		Some (1 to 2) critical injuries. Several (3 or more) injured.	Several lost time injury/injuries. One or some lasting disablement. Fatality/fatalities not likely but possible.
CC	Considerable	PLL < 0,01		Some (1 to 2) injuries. Serious discomfort.	One or some lost time injury/injuries. Minor probability of lasting disablement. Fatality improbable.
CB	Marginal	PLL = 0		Minor injury/injuries. Lasting discomfort.	No lost time injury/injuries. Medical treatment required.
CA	Negligible	PLL = 0		Negligible injury/injuries. Temporary discomfort.	No lost time injury/injuries. No medical treatment required.
C	Environmental harm (E)	Effluent Influence	Effluent Extension	Max. environmental consequences due to the hazardous event	Additional comments to the environmental consequence categories
CF	Catastrophic	Lasting	Wide	Wide permanent or long time harm. Decontamination impossible or hard.	A liquid spill into river or sea. A wide vapour or aerosol release. The effluent causes lasting or permanent damage to plants and wildlife.

C	Human harm (H)	Probability loss of life		Max. health consequences due to the hazardous event	Additional comments to the health consequence categories
CE	Extensive	Lasting	Confined	Confined permanent or long time harm. Decontamination impossible or hard.	A liquid spill to ground water. A confined vapour or aerosol release. The effluent causes lasting or permanent damage to plants and wildlife.
CD	Serious	Lasting	Limited	Limited permanent or long time harm. Decontamination impossible or hard.	Onsite liquid spill. A limited vapour or aerosol release (within fence). The effluent causes lasting or permanent damage to plants and wildlife.
CC	Considerable	Temporary	Wide/Confined	Wide to confined temporary harm. Decontamination easy or not needed.	A liquid spill into river or sea. A limited vapour or aerosol release. The effluent causes temporary damage to plants and wildlife.
CB	Marginal	Temporary	Limited	Limited (on site) temporary harm. Decontamination easy or not needed.	Onsite liquid spill. A limited vapour or aerosol release (within fence). The effluent causes temporary damage to plants and wildlife.
CA	Negligible	Negligible		Negligible environmental harm. Decontamination not needed.	Moderate leak from flange or valve. Small liquid spill or small soil pollution not effecting ground water. Negligible environmental effects.
C	Financial harm (F)	Damaged property (k€)	Production loss (k€)	Max. financial consequences due to the hazardous event	Additional comments to the financial consequence categories
CF	Catastrophic	>10 000	>50 000	Devastating loss off production, market share and image.	Devastating damage to production unit and/or plant. Event causing or requiring a production stop for more than a year.
CE	Extensive	1 000 – 10 000	5 000 – 50 000	Extensive loss of production. Large loss of market share and/or image	Extensive damage to equipment and/or property. Event causing or requiring a lasting production stop of several months.
CD	Serious	100 – 1 000	500 – 5 000	Large loss of production. Considerable loss of market share and/or image	Serious damage to equipment and/or property. Event causing or requiring a lasting production stop up to a month.
CC	Considerable	10 – 100	50 – 500	Considerable loss of production. Marginal loss of market share.	Considerable damage to equipment and/or property. Event causing or requiring a lasting production stop up to a week
CB	Marginal	1 – 10	5 – 50	Minor loss of production. No loss of market share and/or image.	Minor damage to equipment. Event causing or requiring a day of production stop.
CA	Negligible	<1	<5	Negligible loss of production. No loss of market share and/or image.	Negligible damage to equipment. Event causing or requiring a temporary (hours) production stop.

Annex I
(informative)

Designing & calibrating a risk graph

I.1 Overview

Annex I describes the basic steps involved in designing and calibrating a risk graph that enables the safety integrity level (SIL) of a safety instrumented function (SIF) to be determined from knowledge of the risk factors for the process plant.

A risk graph used to assess the required safety-integrity levels for any process plant application needs to be appropriate for the particular application and calibrated to use the tolerable event frequency values that have been determined to be relevant to the potential risk outcome.

The risk graph methods shown in IEC 61511-3 are example techniques and the user needs to be satisfied that they are appropriate to the application and ensure that the results gained have the correct value. In many cases it is necessary to adapt an example method to make it relevant to the application and calibrate the chosen risk graph to give the correct values.

Annex I is not intended to be a definitive account of the process by which a risk graph is designed and calibrated but is intended to illustrate the general principles. It is based on a method described in more detail in the following reference:

"*Using risk graphs for Safety Integrity Level (SIL) assessment – first edition*"; Clive De Salis, C; Institution of Chemical Engineers", 2011.

I.2 Steps involved in risk graph design and calibration

The steps in the design and calibration of a risk graph may include, but not be limited to, the following:

- decide the assessment parameters to be included in the risk graph;
- draw the overall shape of the risk graph;
- define each of the parameters in detail;
- assign values to each of the parameters that match the definitions;
- identify the tolerable event frequency values to be used for each consequence definition;
- identify the calibration axis line for each consequence;
- calculate all other values in the graph relative to the relevant calibration axis line;
- convert the event probability values into SIL numbers using the relevant tolerable event frequency;
- review the overall risk graph and remove any routes through the risk graph that are contrary to requirements.

I.3 Risk graph development

Clause I.3 provides an overview of how a risk graph may be developed.

The first steps in designing and calibrating a risk graph are to define the parameters that need to be assessed, deciding the overall shape of the risk graph, defining each parameter in detail and deciding the range of values that are relevant for each parameter.

I.4 The risk graph parameters

I.4.1 Choosing parameters

When choosing parameters for use in a SIL assessment for a process plant the user shall select all of the appropriate values to be assessed. Figure I.1 shows the main parameters that should be considered but others may be relevant and may need to be added.

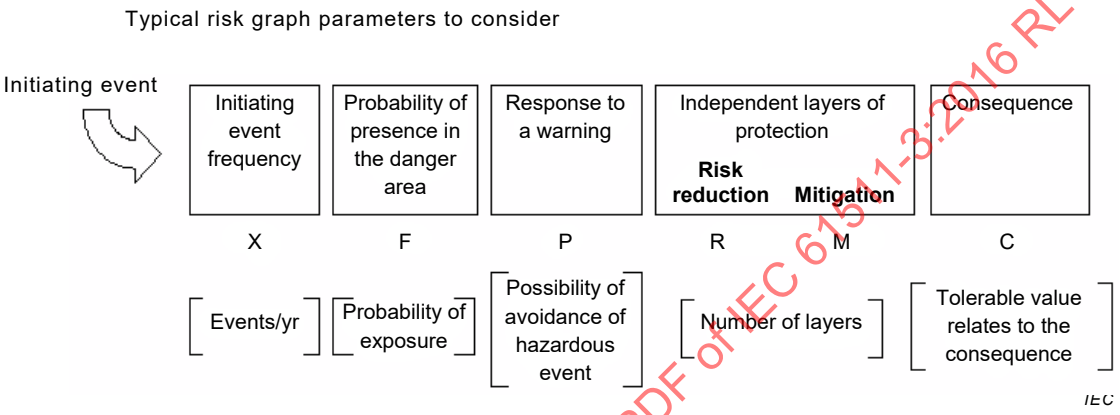


Figure I.1 – Risk graph parameters to consider

An example showing a combination of techniques from Annex D (Figure D.1) and Annex C (Figure C.2) is shown in Figure I.2 to illustrate how a risk graph can be designed to have more parameters.

I.4.2 Number of parameters

Having decided the parameters to be used, now decide the number of each parameter to be used. For example, it may be sufficient to represent the probability of exposure of a person to the risk by simply two values: F1 and F2.

I.4.3 Parameter value

Define each parameter and each value for that parameter. These definitions should be sufficiently detailed for assessment team members to understand the parameter and repeatedly select the correct value.

During this step it may be necessary to revise the decisions made in either or both of the preceding steps.

I.4.4 Parameter definition

When defining parameters to be included consider the meaning of available information.

For example, you may have information on how often an event occurs for a process plant that is under the control of the BPCS in which case your data can be used for how often the event occurs and the BPCS fails to control it as a combined value. Alternatively you may have the initiating event data separately to the BPCS' capability to control that process condition.

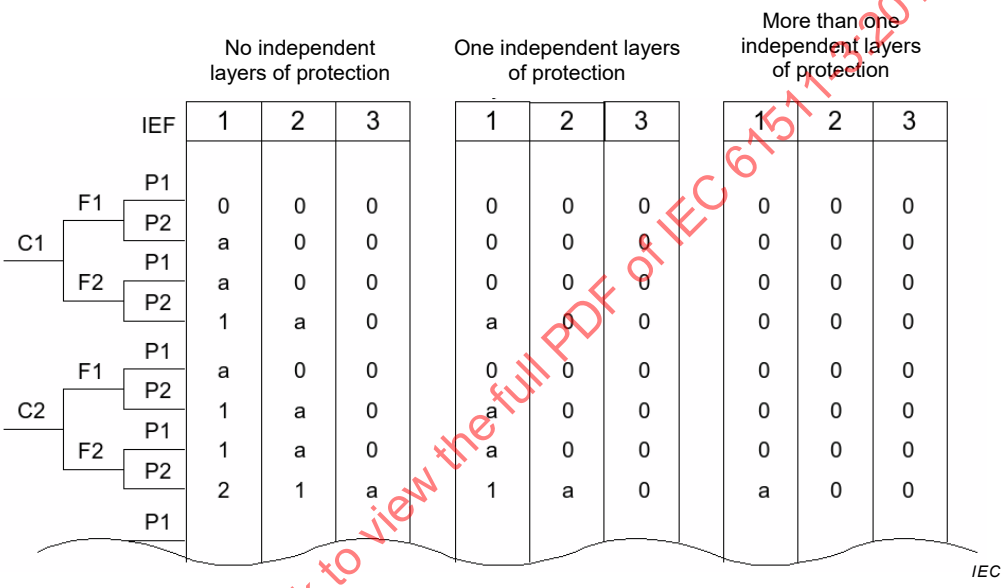
NOTE If a risk graph is designed to use the initiating event frequency then the risk graph can include all other parameters with which to determine the demand rate on the safety function. Therefore the probability of other independent risk reducers will need to be included to properly assess the demand rate on the safety functions.

I.4.5 Risk graph

Draw the risk graph as an overall diagram.

NOTE The diagram will usually be symmetrical in form and include all combinations of possible routes including those routes through the diagram that may later be excluded. For example, your policy can be to exclude consideration of operator response to alarms where the consequence is potentially multiple fatalities. In this example case your diagram will include the operator response lines at this stage of the design but at the final stage the option of operator response will be deleted.

Initiating event frequency, IEF, events per year
1 = less than or equal to once a year.
2 = less than or equal to once every ten years.
3 = life time of the plant



Key 0 = no protection layer needed; a = SIS protection layer probably not needed; 1 and 2 = SIL value needed

Figure I.2 – Illustration of a risk graph with parameters from Figure I.1

I.4.6 Tolerable event frequencies (Tef) for each consequence

I.4.6.1 Tef guidance

Provides guidance when determining tolerable event frequencies.

I.4.6.2 Tef SIL assessment

SIL assessment tolerable event frequencies are different for each consequence. Values assigned are often relative to the single fatality consequence. If the safety case for the process plant has a linear progression from Single fatality = 1, to serious injury = 0,1, minor injury = 0,01 then a full list of these values is made for each consequence defined in Clause I.4.3 and Clause I.4.4 Value progressions are not always linear. For example the values may change for multiple fatalities (N) and it is not unusual to change the values for N=10 or N=50.

I.4.6.3 Risk graph Tef

Ensure that the tolerable event frequency values are correctly used in the risk graph. If the tolerable event frequency is the number of serious injuries per year to an individual but the intended use of the risk graph is to consider a single process plant risk then these two terms

are not directly compatible. An individual will be subject to multiple risks of serious injury from his occupation and so the design shall consider how to convert from expressions of risk to the individual to risks of a single event on a process plant.

I.4.7 Calibration

I.4.7.1 General

Explains the significance of calibration in the risk graph development.

I.4.7.2 Calibration axis line

The calibration axis line for each consequence is the route through the risk graph that corresponds exactly to the consequence.

For example:

A risk graph may have the following parameters (Figure I.1):

– C3 = single fatality;
– F2 = probability of exposure is 1 (i.e., personnel likely to be present);
– P2 = difficult to avoid;
– R0 = no available independent other technology risk reducers;
– M0 = no available independent mitigation measures;
– 1 = initiating event frequency is once per year.

The sequence of this example route through the risk graph means that the outcome is potentially a single fatality, they are present, it is difficult to avoid, there are neither independent risk reducers to prevent it nor mitigation measures to change the outcome and the event happens every year = one fatality per year. This is the calibration axis line for the single fatality consequence because if the tolerable event frequency required for this event is 2×10^{-5} then the probability of failure required of the safety function to avoid this is 2×10^{-5} FD. The mathematical value for each parameter in this sequence is 1 indicating the number of people present and the probability of each parameter failing to avoid the outcome. C3 × F2 × P2 × R0 × M0 × 1 per year = 1 fatality × 1 × 1 × 1 × 1 × 1 per year = 1 fatality per year.

I.4.7.3 Calibration events per year

For each calibration axis line final destination write in the events per year represented by that route through the risk graph.

I.4.7.4 Route events per year

Using the values determined inI.4.3, I.4.4 and I.4.7.3 calculate the events per year that will occur for each route through the risk graph by adjusting one parameter at a time.

This can be illustrated by the same example from I.4.7.2 above in which we change one value, for example F2 becomes F1.

A risk graph may have the following parameters:

– C3 = single fatality;
– F1 = probability of exposure is 0,1 (i.e., less than 10% chance of personnel in the danger zone);
– P2 = difficult to avoid;

– R0 = no available independent other technology risk reducers;

– M0 = no available independent mitigation measures;

– 1 = initiating event frequency is once per year.

The sequence of this example route through the risk graph means that the outcome is potentially a single fatality, they are present for less than 10% of the time, it is difficult to avoid, there are neither independent risk reducers to prevent it nor mitigation measures to change the outcome and the event happens every year = 0,1 fatalities per year. The mathematical value for each parameter in this sequence is 1 indicating the number of people present and the probability of each parameter failing to avoid the outcome, except for the value of F2 which has been defined as a less than 10 % chance of being in the area and therefore has a value of 0,1. C3 × F2 × P2 × R0 × M0 × 1 per year = 1 fatality × 0.1 × 1 × 1 × 1 × 1 per year = 0,1 fatalities per year.

I.4.7.5 PFD_{avg} calculation

With all destination points in the risk graph calculated as the frequency of events, now divide the tolerable event frequency value for the consequence by the calculated value at the destination point. The values now written in the risk graph are the PFD_{avg} required.

I.4.7.6 PFD_{avg} conversion to SIL

Now convert each PFD_{avg} value into the SIL number. When converting a PFD_{avg} value into a SIL number for the risk graph a value should never be rounded down to a less onerous value but always rounded up.

I.4.8 Completion of the risk graph

I.4.8.1 General

Discusses items to consider when finalizing the risk graph.

I.4.8.2 Routes removal

Remove routes through the risk graph that should not be present.

For example, your policy may be to exclude consideration of operator response to alarms where the consequence is potentially multiple fatalities. For this example case the route(s) for the response to a warning being possible would be removed from the risk graph where the potential outcome is multiple fatalities.

I.4.8.3 Risk graph instructions

A detailed set of instructions describing the correct use of the risk graph should be written. The instructions should include a statement describing the limitations of use for the risk graph (i.e., the limits of applicability).

Annex J
(informative)

Multiple safety systems

J.1 Overview

The semi quantitative approaches presented in IEC 61511-3:- annexes are very useful to evaluate quickly the risk reduction which is needed to achieve a given hazardous event frequency target established from a prior risk analysis (refer to Annex A about ALARP approach). Nevertheless, the underlying hypothesis that the risk reduction achieved by a SIS is directly linked to its relevant failure measure (e.g., average unavailability – PFD_{avg}) is true only when a single SIS is implemented. When several safety systems (SIS and non-SIS) are designed to run in sequence to prevent a given hazardous event the risk reduction still increases when the failure measures decrease but the link is not so simple and the risk reduction which is actually provided by a given SIS may be lower than that which can be inferred directly from its individual failure measure. This is true especially when periodically proof tested systems are implemented.

Therefore, when several safety systems working together have been designed according to the approaches developed in IEC 61511-3 annexes it is important to check that common cause failures and dependency effects between the safety systems are negligible or properly taken into account in order to actually achieve the tolerable hazardous event frequency.

NOTE More information can be found in the documents provided in bibliography.

J.2 Notion of systemic dependencies

Figure J.1 illustrates the conventional calculations used in semi quantitative approaches. Two safety instrumented systems (SIS_1 and SIS_2) are working in sequence. When a demand occurs from the process then SIS_1 has to react first. If it fails then SIS_2 has to react in turn and, if it also fails, the hazardous event occurs.

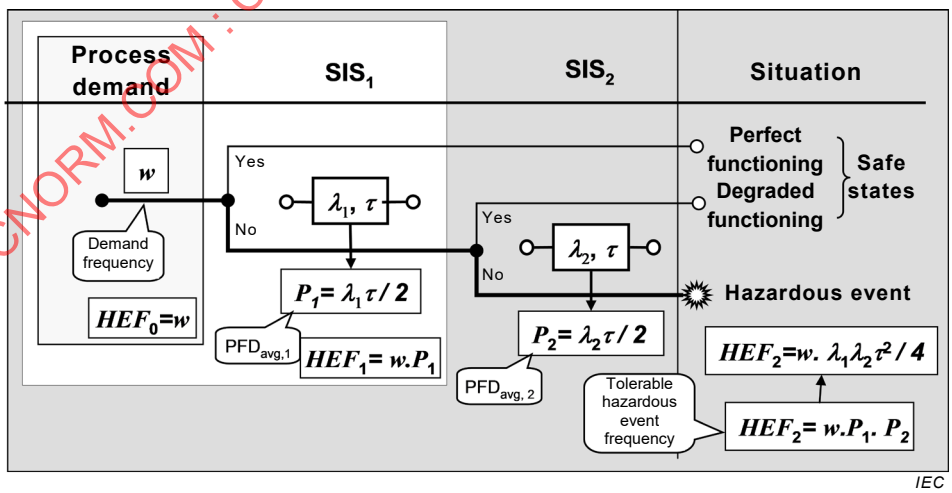


Figure J.1 – Conventional calculations

When using the semi quantitative approaches it is accepted that the risk reduction provided by a SIS is equal to the inverse of its failure measure (e.g., P_i=1/$PFD_{avg,i}$). Therefore, without any SIS, the hazardous event frequency HEF_0 is equal to the demand frequency itself (w). Then, the SIF achieved by SIS_1 provides a risk reduction $HEF_0/HEF_1=1/P_1$ and the risk drops

to $HEF_1=w.P_1$. Afterward the SIF achieved by SIS_2 provides a risk reduction $HEF_1/HEF_2=1/P_2$ and the risk drops to $HEF_2=HEF_1.P_2=w.P_1.P_2$ which is expected to comply with the tolerable hazardous event frequency requirements.

However, the times for proof testing, MTTR, MRT, common cause failure and other factors for each of the SIFs can interact to give a different risk reduction to that presumed in the simplistic view that has so far been described.

In the simple example of Figure J.1, SIS_1 comprises only one sensor (S), one logic solver (LS) and one final element (FE) organised in series and tested at the same time with a periodical proof test interval. Then the failure rate of SIS_1 is $\lambda_1 = \lambda_{1_S} + \lambda_{1_{LS}} + \lambda_{1_{FE}}$ and its average unavailability (i.e., $PFD_{avg,1}$) is $P_1 = \frac{\lambda_1.\tau}{2}$. Similarly, the average unavailability of SIS_2 (i.e., $PFD_{avg,2}$) is given by $P_2 = \frac{\lambda_2.\tau}{2}$. Therefore, with the two safety instrumented systems (SISs), the hazardous event frequency is established at $HEF_2 = w.P_1.P_2 = w.(\frac{\lambda_1.\tau}{2}).(\frac{\lambda_2.\tau}{2}) = w\frac{\lambda_1\lambda_2.\tau^2}{4}$ where the SIF achieved by SIS_1 provides a risk reduction of $HEF_0/HEF_1 = 1/PFD_{avg,1}$ and the SIF achieved by SIS_2 a risk reduction of $HEF_1/HEF_2 = 1/PFD_{avg,2}$.

The above calculation only takes into account the test interval but not the scheduling of the tests according to the time. This is shown in Figure J.2 where the two SIS are tested at the same time. This is a popular current test policy allowing to simplify the maintenance team tasks or to minimize the number of process shut-downs for performing the tests.

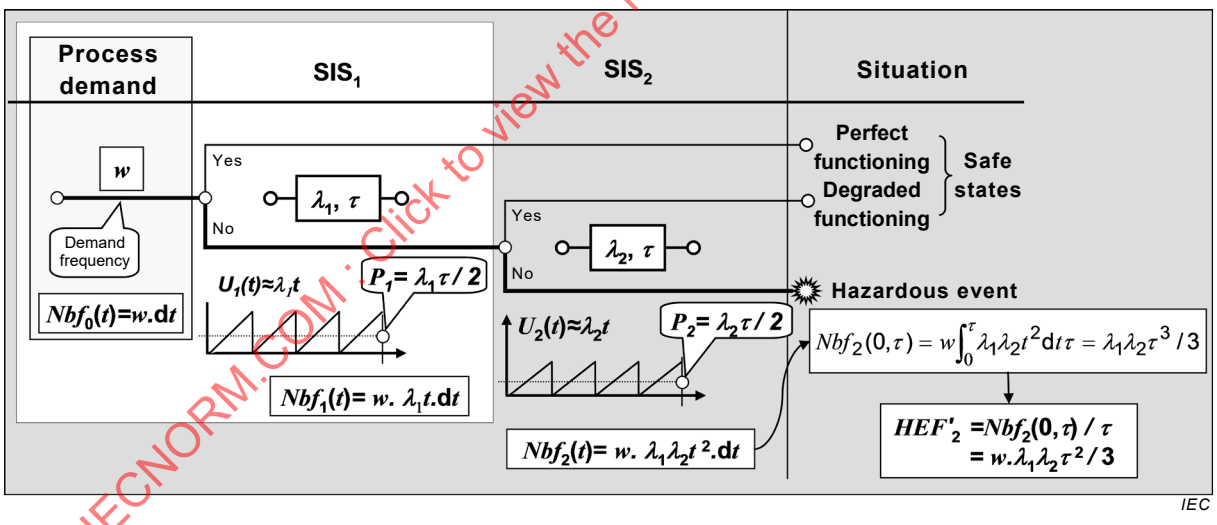


Figure J.2 – Accurate calculations

Within a proof test interval the unavailability of SIS_1 is given by $U_1(t) = 1 - e^{-\lambda_1 t}$ which is approximated by $\lambda_1 t$ when $\lambda_1 t << 1$. Just after a proof test $U_1(t)$ goes to 0 (if the repair time is negligible or if the process is stopped) then it increases until just before the next proof test. This gives the well known saw-tooth shaped curve which is represented in the Figure J.2. This is exactly the same for $U_2(t)$. Therefore $U_1(t)$ and $U_2(t)$ are *correlated* because they are low (just after a test) and high (just before a test) at the same time. This seems insignificant but, in fact, introduces a *systemic* dependency between SIS_1 and SIS_2 which, therefore, are not really completely independent. The term "*systemic dependency*" means that this dependency is a property of SIS_1 and SIS_2 considered as a whole, which cannot be described just by considering SIS_1 or SIS_2 separately. It has to be noted that this type of correlation doesn't exist for immediately revealed failures (e.g., detected by diagnostic tests) because the

unavailability related to these failures reaches asymptotic values which is not the case with proof tested failures.

When a demand occurs, $\lambda_1 \cdot t$ is the probability that SIS_1 fails, $\lambda_1.\lambda_2.t^2$ is the probability that both SIS_1 and SIS_2 fail and $w.\lambda_1.\lambda_2.t^2$ is the probability that the hazardous event occurs. If w is the demand frequency, $Nbf_0 = w.dt$ is the number of demands occurring between t and $t+dt$ (i.e., the number of hazardous events in the absence of safety systems). With the two SIS's, the number of hazardous event occurring over dt becomes $Nbf_2(t) = w.\lambda_1.\lambda_2.t^2 dt$ and a simple integral gives the number of hazardous events occurring within [0, τ]: $Nbf_2(0,\tau) = w.\lambda_1.\lambda_2.\tau^3/3$. Finally the average hazardous event frequency is equal to $HEF'_2 = Nbf_2(0,\tau)/\tau = w.\lambda_1.\lambda_2.\tau^2/3$. Note that the constant demand frequency w is factored. Then $3/\lambda_1.\lambda_2.\tau^3$ represent the risk reduction provided by the equivalent single safety system comprising both SIS_1 and SIS_2.

Finally HEF'_2 = 1,33 HEF_2 which is obviously greater than HEF_2. We can write $HEF'_2 = w.(\frac{\lambda_1.\tau}{2}).\frac{4}{3}.(\frac{\lambda_2.\tau}{2}) = w.P_1$ x 1,33 x P_2 which shows that SIS_1 provides 100 % of the expected risk reductions P_1 and SIS_2 only 3/4 =75 % of P_2 because it acts in second position.

If a third SIS was added and tested at the same time (i.e., $P_3 = \frac{\lambda_3.\tau}{2}$), the hazardous event frequency would become $HEF'_3 = w\frac{\lambda_1\lambda_2\lambda_3.\tau^3}{4} = 2w.(\frac{\lambda_1.\tau}{2})(\frac{\lambda_2.\tau}{2})(\frac{\lambda_3.\tau}{2}) = 2w.P_1.P_2.P_3$ i.e., the risk reduction is only 1/2 = 50 % of what being expected from the semi quantitative approaches. Writing $HEF'_3 = w(\frac{\lambda_1.\tau}{2}).\frac{4}{3}(\frac{\lambda_2.\tau}{2}).\frac{3}{2}(\frac{\lambda_3.\tau}{2}) = HEF'_2$ x 1,5 x P_3 shows that the contribution of the third SIS of only 2/3 = 66 % of the expectation.

We can also write $HEF'_2 = [w.(\frac{\lambda_1.\tau}{2})].\frac{4}{3}(\frac{\lambda_2.\tau}{2}) = w'.\frac{4}{3}(\frac{\lambda_2.\tau}{2})$ where w' is the demand frequency on SIS_2. If w' is considered as a process demand, this shows that systemic dependencies may also exist between the process and the SIS. Therefore even in the case where a single SIS is considered, it may provide a reduction lower than expected.

If now we stagger the tests and perform some mathematical development we will find that an optimum is reached when SIS_2 is tested in the middle of the test interval of SIS_1. In this optimum case, the hazardous event frequency drops to $HEF''_2 = w.\frac{5}{24}\lambda_1\lambda_2.\tau^2$. This can be written $HEF''_2 = w.(\frac{\lambda_1.\tau}{2}).\frac{10}{12}.(\frac{\lambda_2.\tau}{2}) = w.P_1\frac{10 \text{ x } P_2}{12}$. The proof tests are still correlated but now SIS_2 provides a risk reduction of 12/10=120 % of what was expected. Therefore the correlation between the proof tests of the various SIS may be detrimental or beneficial depending of the implemented proof test policy.

As shown on the left hand side of Figure J.3 the multiple safety system analysed above is equivalent to a single redundant SIS. This allows the introduction of the potential common cause failures (CCF) which are likely to exist between SIS_1 and SIS_2 as shown on the right hand side of the figure. Common cause failures also constitute systemic dependencies between SIS_1 and SIS_2.

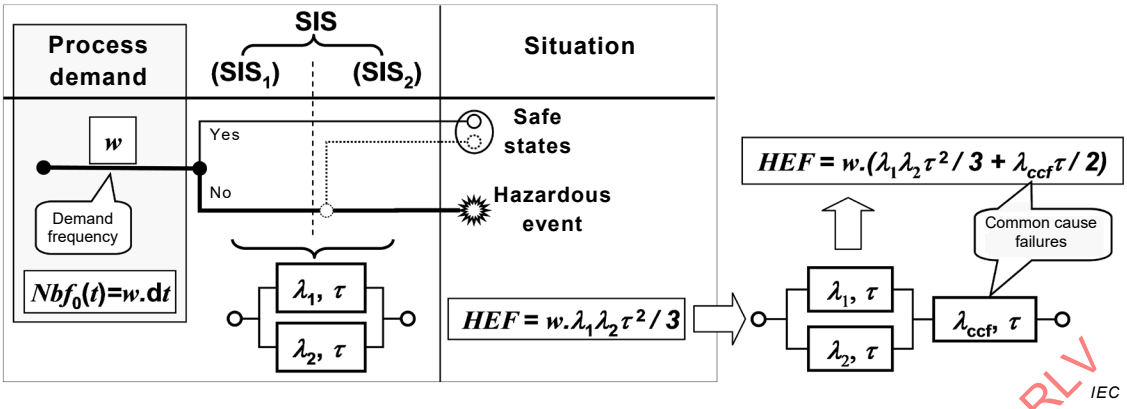


Figure J.3 – Redundant SIS

The CCF impact is generally more important than the correlation of proof tests and it is always detrimental. In the above example where the proof tests are performed at the same time this introduces an additional factor $w.\lambda_{ccf}.\tau/2$ to the hazardous event frequency. This impact can be reduced by staggering the proof tests: when SIS_1 and SIS_2 are not tested at the same time, any test is an opportunity to disclose the CCF provided that relevant procedures are implemented. The CFF proof test interval can be reduced up to $\tau/2$ thus dividing by two the CCF contribution to the hazardous event frequency. With a third SIS similar to SIS_1 and SIS_2, the CCF contribution may be divided by three, etc.

In conclusion the risk reduction provided by multiple SIS running in sequence may be lower, equal or greater than expected from semi-quantitative approaches. When the various safety systems are periodically tested at the same time the semi quantitative approaches leads to non-conservative results and the non-conservativeness increases with the level of redundancy. When complex patterns of proof tests are implemented, the result of the competition between detrimental or beneficial effects is difficult to anticipate. Therefore, when a multiple safety system has been designed according to the individual requirements established from semi quantitative approaches, it is wise to check that the targeted tolerable hazardous event frequency is actually achieved.

NOTE A single safety system with redundant components experiences the same systemic dependencies described above and can be analysed in the same way.

J.3 Semi-quantitative approaches

The semi quantitative approaches can be used to check the hazardous event frequency to take into account the effects of common cause failures and systemic dependencies.

When a proof test staggering policy is implemented (to mitigate the negative impact of proof test correlation) and no common cause failures are identified between the single SISs forming the multiple safety system the conventional calculations can be used. In the other cases some adjustments of the conventional calculations are needed.

If common cause failures are identified, they should be handled at the multiple safety system level as shown in Figure J.3. If proof tests are staggered and a relevant procedure is implemented, then the CCF proof test interval can be reduced to the interval between the successive staggered proof tests.

When no staggering proof test policy is implemented, then the systemic dependencies due to the correlation of proof test should be considered. Corrective coefficients like those presented in Figure J.4 may help to estimate the corrections to be done. This table has been built with the hypothesis that all components are tested at the same time. The correction increases when the number of individual SISs increases and when the length of the scenarios leading to

the hazardous event (the order of the so called minimal cut sets – MCS) increases. The table on the left hand side of Figure J.4 deals with a multiple safety system made of two individual SISs and the table on the right hand side deals with a multiple safety system made of three individual SISs. The corrective coefficients in this table are calculated as m/n where m is the coefficient of the integrals calculated separately and n the coefficient of the integral calculated as a whole. For example, for MCS of order 2 obtained from two separate SISs we compare factors like $\lambda_1\tau/2 \times \lambda_2\tau/2$ (integrals calculated separately) to factors like $\lambda_1\lambda_2\tau^2/3$ (integral calculated as a whole) and that gives a corrective factor of 2 × 2/3 = 4/3 = 1,33.

Multi SS	SIS1	SIS2	
MCS order	MCS order	MCS order	Coefficient
2	1	1	4/3=1,33
3	1	2	6/4=1,50
3	2	1	6/4=1,50
4	1	3	8/5=1,60
4	3	1	8/5=1,60
4	2	2	9/5=1,80
5	1	4	10/6=1,67
5	4	1	10/6=1,67
5	2	3	12/6=2,00
5	3	2	12/6=2,00

Multi SS	SIS1	SIS2	SIS3	
MCS order	MCS order	MCS order	MCS order	Coefficient
3	1	1	1	8/4=2,00
4	1	1	2	12/5=2,40
4	1	2	1	12/5=2,40
4	2	1	1	12/5=2,40
5	1	1	3	16/6=2,67
5	1	3	1	16/6=2,67
5	3	1	1	16/6=2,67
5	1	2	2	18/6=3,00
5	2	1	2	18/6=3,00
5	2	2	1	18/6=3,00

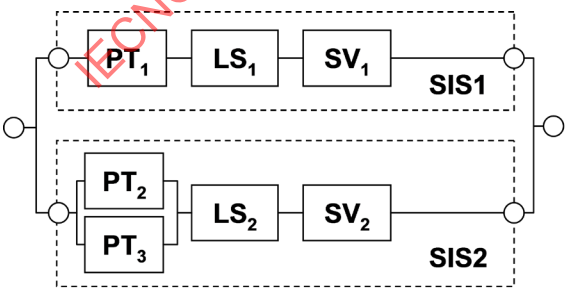
IEC

Figure J.4 – Corrective coefficients for hazardous event frequency calculations when the proof tests are performed at the same time

The tables in Figure J.4 should be applied on the minimal cut sets excluding the common cause failures at the multiple safety system level and the maximum order contributing to the hazardous event frequency should be evaluated and used to find the corrective coefficients (right columns of the tables presented in Figure J.4). For example if the maximum contributing order is 3, and if the multiple safety system comprises two SIS (left hand side of Figure J.4), the hazardous event frequency calculated from a semi quantitative approach should be multiplied by 1,5.

For a maximum contributing order of 4 it should be multiplied by a factor ranging from 1,6 to 1,8. It should be multiplied by a factor ranging from 2,7 to 3 for the minimal cut sets of order 5 of a multiple safety system made of three SIS (right hand side of Figure J.4), etc. When the multiple safety system comprises a mix of several situations, then the bigger coefficient should be used for the sake of conservativeness.

J.4 Boolean approaches



	Failure rate	Repair rate	Test interval
PT_1	4,50E-06	0,125	4380
PT_2	4,50E-06	0,125	8760
PT_3	4,50E-06	0,125	8760
PT_4	6,25E-04	0,125	Detected
PT_5	6,25E-04	0,125	Detected
PT_6	3,55E-06	0,042	8760
PT_7	3,55E-06	0,042	8760

IEC

Figure J.5 – Expansion of the simple example

In order to illustrate how multi safety systems can be handled the example which has been already analysed in Clause J.2 has been slightly modified: now SIS_1 and SIS_2 are not similar and the logic solvers have only detected dangerous failures. With two redundant sensors, the

failure rate of SIS_2 is no longer constant. This new example is detailed and modelled with a reliability block diagram in Figure J.5 where PT stands for "pressure transmitter", LS for "logic solver" and SV for "safety valve". Each SIS comprises sensors (one or two), one logic solver and one safety valve organised in series. The nine failure scenarios (i.e., the so-called minimal cut sets, MCS) derived from this model are the following: {PT_1, PT_2, PT_3}, {PT_1, LS_2}, {PT_1, SV_2}, {LS_1, PT_2, PT_3}, {LS_1, LS_2}, {LS_1, SV_2}, {SV_1, PT_2, PT_3}, {SV_1, LS_2}, {SV_1, SV_2}. The MCS which are related to similar components are candidates for common cause failures. Then three minimal cut sets should be added to the nine previous ones: CCF_P, CCF_{LS} and CCF_{SV}. At the end we have twelve minimal cut sets (3 single failures, 6 double failures and 3 triple failures). Then, the first idea may be to use for each of them some simplified formulae like those proposed in IEC 61508-6:2010, Annex B. This is possible, provided that specific formulae are developed to deal with non-similar components (e.g., different failure modes and/or different proof test interval).

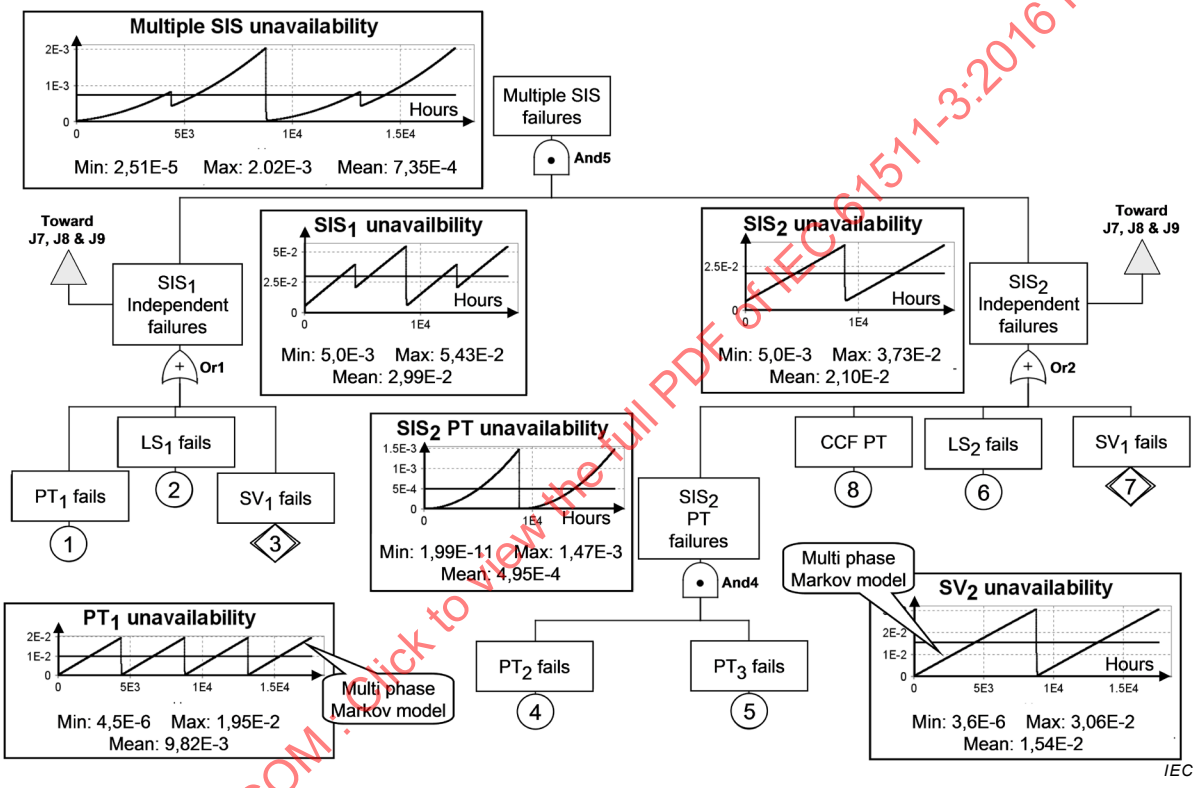


Figure J.6 – Fault tree modelling of the multi SIS presented in Figure J.5

The second idea is to use the fault tree approach which proves to be very effective when the components are reasonably independent (e.g., the probability to have 2 failures at the same time is low) and provided the calculations are handled in a correct way. The fault tree related to the above multiple SIS is presented in Figure J.6.

A fault tree gives directly the instantaneous unavailability of the top event from the instantaneous unavailability of the basic events. As said above and as shown in Figure J.6, the unavailability of a periodically tested event is a saw-tooth curve (see Note). Calculating the fault tree for a relevant number of instants t_i over a given period (e.g., 2 years), gives the unavailability at the logic gate output levels (including the top event). They are more or less complicated saw-tooth curves according to the proof test policy. Calculating the averages of the previous curves over the given period gives the average unavailability (e.g., PFD_{avg}). This averaging operation deals with the systemic dependencies due to the proof tests correlations. Note that a beta factor of 1 % has been considered to model the CCF between PT_2 and PT_3 of SIS_2.

NOTE The input saw-tooth curves can be obtained through a multi-phase Markovian model (see IEC 61508-6:2010 Annex B). Then the fault trees are used to link small Markovian models. This is effective when those small Markovian models are independent from each other. With the data used for this example and for the independent failures we obtain an average availability P_1=2,99. 10^{-2} for SIS_1 and P_2=2,10. 10^{-2} for SIS_2. With a semi quantitative approach this would lead to a risk reduction of $1/P_1P_2$=1 588 when it is of only 1/7,35. 10^{-4}=1 360 (i.e., a difference of about 15 %).

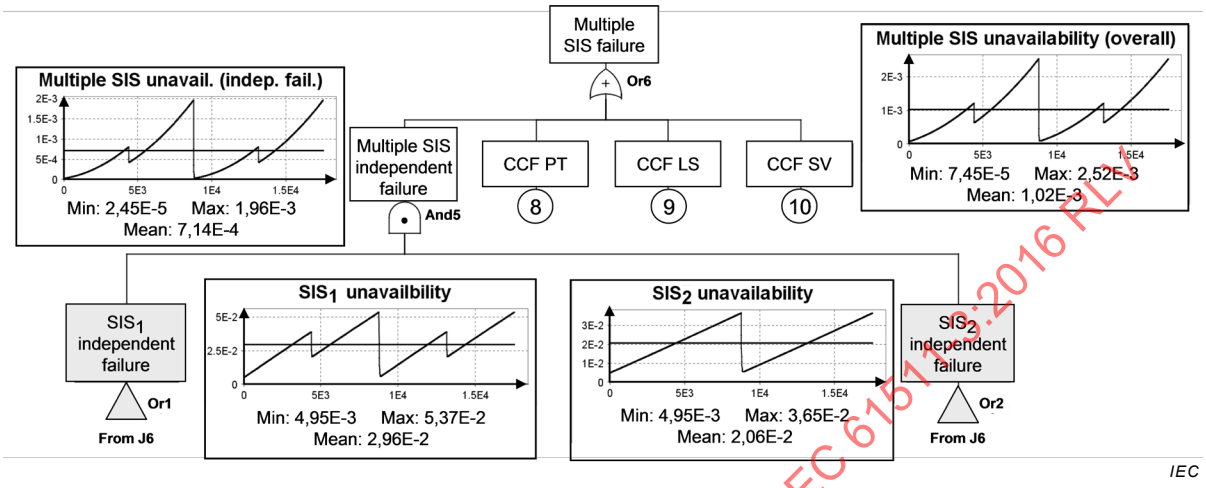


Figure J.7 – Modelling CCF between SIS_1 and SIS_2

The potential CCFs between SIS_1 and SIS_2 are not modelled in Figure J.6. This is done in Figure J.7 where the common cause failures between PTs, LSs and SVs have been considered with a beta factor of 1 %. Now, the average unavailability of the multiple safety system is 1,018 x 10^{-3} and the overall risk reduction has dropped to 982. This is about 62 % of the risk reduction expected from a semi-quantitative approach on the hypothesis that SIS_1 and SIS_2 are fully independent.

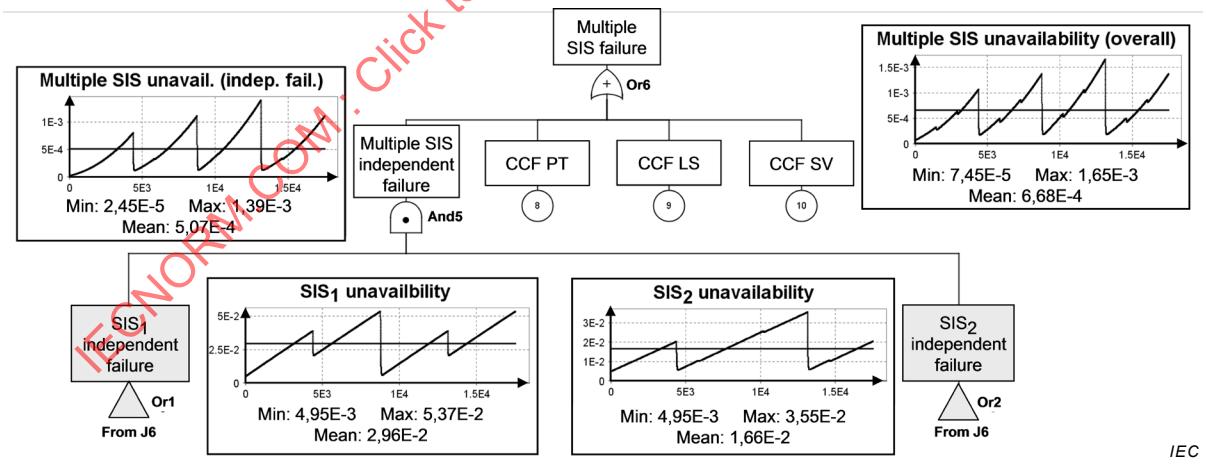


Figure J.8 – Effect of tests staggering

In Figure J.8 the tests of the three PTs have been staggered as well as those of the two SVs. The average unavailability of the two SIS considered as a whole is 6,68 x 10^{-4} and the overall risk reduction has increased to 1 497. This is just a bit lower than expected from a semi-quantitative approach.

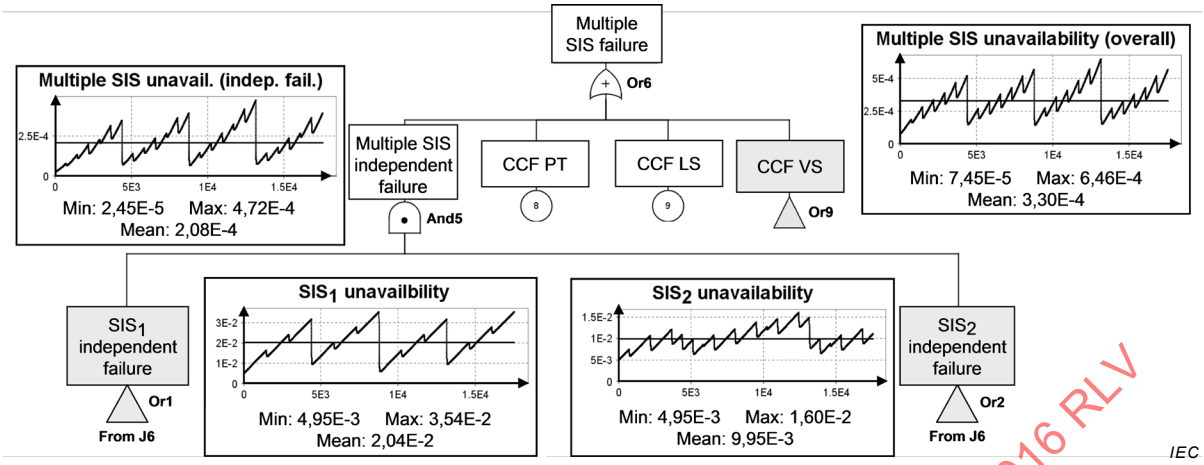


Figure J.9 – Effect of partial stroking

In Figure J.9 the failure modes of the safety valve have been split between those which are detected by partial stroking and those which are detected by full stroking. The average unavailability of the two SIS considered as a whole is 3,30 x 10^{-4} and the overall risk reduction has increased to 3 034. This is about twice that expected from a semi-quantitative approach.

J.5 State-transition approach

The fault tree approach is very efficient when the components are reasonably independent. This is not the case when the components are strongly dependent as for example when the repair occurs at the second failure, when the logic is changed (e.g., from 2oo3 to 1oo2) instead of repairing, when the delay to start the repair is long due to the mobilisation of the repair tools (e.g., a dynamic positioning vessel for subsea repairs), etc. In this case it is necessary to move to state-transition models allowing to properly representing the dynamic behaviours of the components. The Markovian approach (see IEC 61508-6:2010, Annex B) is the most popular state transition approach but when dealing with multiple safety systems, a great number of components have to be modelled and this is likely to provoke the combinational explosion of the number of states. Therefore other approaches which do not suffer this shortcoming have to be considered. Among them the Petri net (PN) approach has proven to be very effective (see IEC 61508-6:2010 Annex B and IEC 62551:2012) to model the complex dynamic behaviour of big systems. Analytical calculations are not possible with such models and it is necessary to swap to Monte Carlo simulation but this presents no real difficulties thanks to the computation power of the present time personal computers.

Figure J.10 illustrates a Petri net modelling the multiple safety system presented in Figure J.5. It is similar to the fault tree presented in Figure J.6 except that the repair resources are shared between all the components and should be mobilised before the interventions start (e.g., subsea systems needing a dynamic positioning vessel to be repaired).

This is a reliability block diagram driven Petri net where the reliability block diagram of Figure J.5 (drawn in dotted lines) has been used as guideline and where each bloc has been fulfilled by standardized sub-PN coming, for example, from a sub-PN library. Two kinds of sub-PN have been used: dangerous undetected failures (PTs, CCF on PT_2 and PT_3 and the SVs) and dangerous detected failures (for LSs). Building Petri nets in this way allows handling very big models with hundreds of components.

NOTE 1 A basic Petri net is made of places (circles) which represent local states, transitions (rectangles) which represent events which may occur and upstream arcs linking places to transitions and downstream arcs linking transitions to places. Tokens (small black circles) are placed into places to identify which local states are actually present at a given moment.

Tokens and upstream arcs are used to validate the transitions and, when a transition is valid, it can be "fired" (that means that the related event occurs): one token is removed from each upstream places and one token is added in each of the downstream places. Therefore the marking of the places (i.e. the state of the modelled system) change.

The date of the firing of transitions may be governed by stochastic delays (e.g. exponential distributions with constant failure or repair rates). In this case the PN are named stochastic Petri nets.

NOTE 2 More information about Petri nets can be found in IEC TS 62556:2014.

One pressure transmitter (e.g., PT_1) is normally in good state (W). When it fails it enters into a dangerous undetected state (DU) and its indicator variable (e.g., PT_1) goes to 0. When a proof test is performed, then the failure is detected (DD) and the variable *Nd* which counts the number of detected failures is increased by one. When the repair resource is on location (OL) the repair can start (R). When the repair is finished the indicator variable (e.g., PT_1) goes back to 1 and *Nd* is decreased by one. The same modelling is applied to the three PTs and the two SVs. For the logic solvers the state (DU) has been removed but the principle is similar.

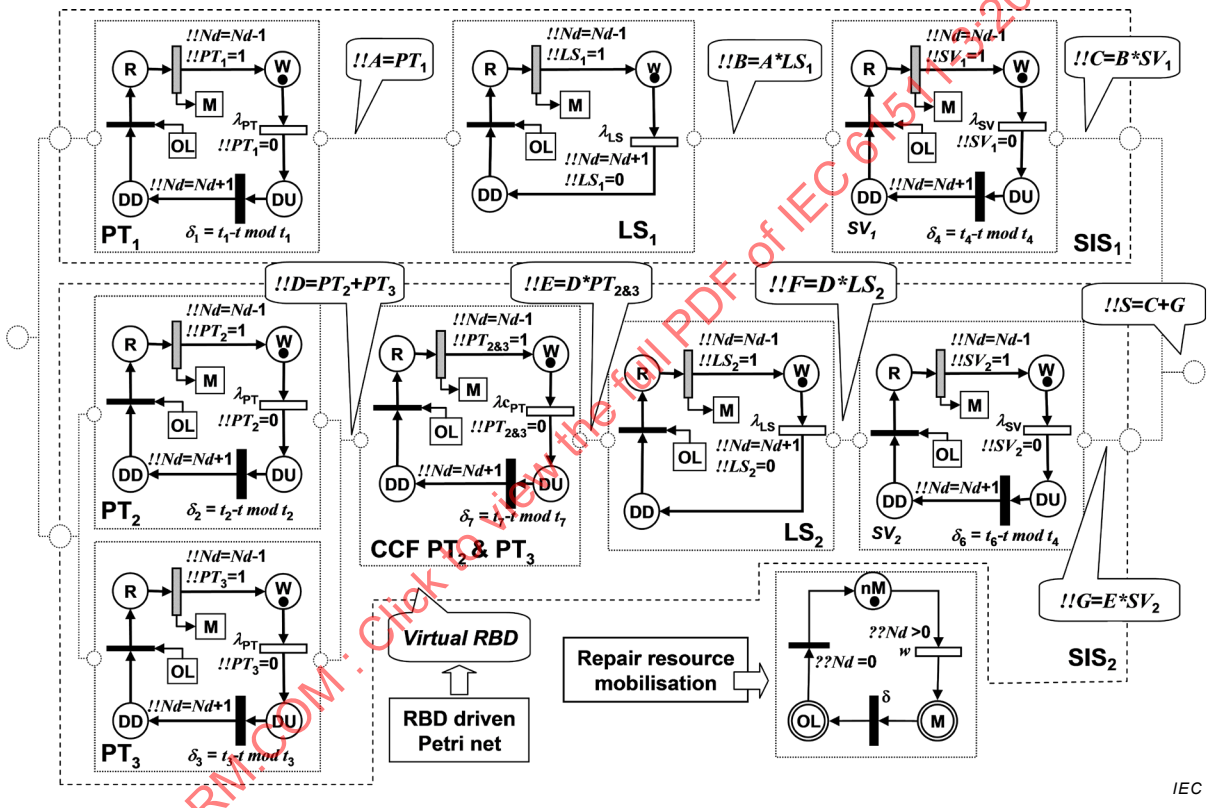


Figure J.10 – Modelling of repair resource mobilisation

When *Nd* becomes positive, (i.e., when at least one failure has been detected), then the mobilisation process starts (sub-PN "Repair resources mobilisation"). When it is achieved (token in M), then the resources move to the location of failures to be repaired (OL). Then the token in place OL is taken by one of the failures waiting for repair and this prevents other repairs at the same time. When the repair is finished one token is put back in place M and the resources can move to the location of another failure. This process is repeated until all the failures have been repaired (*Nd*=0) and that the resource is demobilised.

Global assertions have been introduced to model the virtual nodes of the reliability block diagram. The symbol "*" represents the logical AND, and the symbol "+" represents the logical OR. For example, $B=A*LS_1$ means that the output *B* of LS_1 is equal to 1 when LS_1 is not failed and its input is also equal to 1. $!!S=C+G$ means that the multiple safety system is OK (i.e., *S*=1) when SIS_1 is OK (*C*=1) or SIS_2 is OK (*G*=1).

Then the use of Monte Carlo simulation allows to produce statistical samples of the variables *C*, *G* and *S* and to obtain the safety measures related to SIS_1, SIS_2 and to the multiple safety system itself.

As shown in Figure J.11, it is possible to obtain the saw-tooth curves. They are less smooth than those obtained with fault tree calculations but similar. Nevertheless they should not be used to calculate the average unavailability because the average unavailability can be more accurately obtained directly from the Monte Carlo simulation: the average value of 1-*C* gives P_1, the average value of 1-*G* gives P_2 and the average value of 1-*S* gives the overall average unavailability.

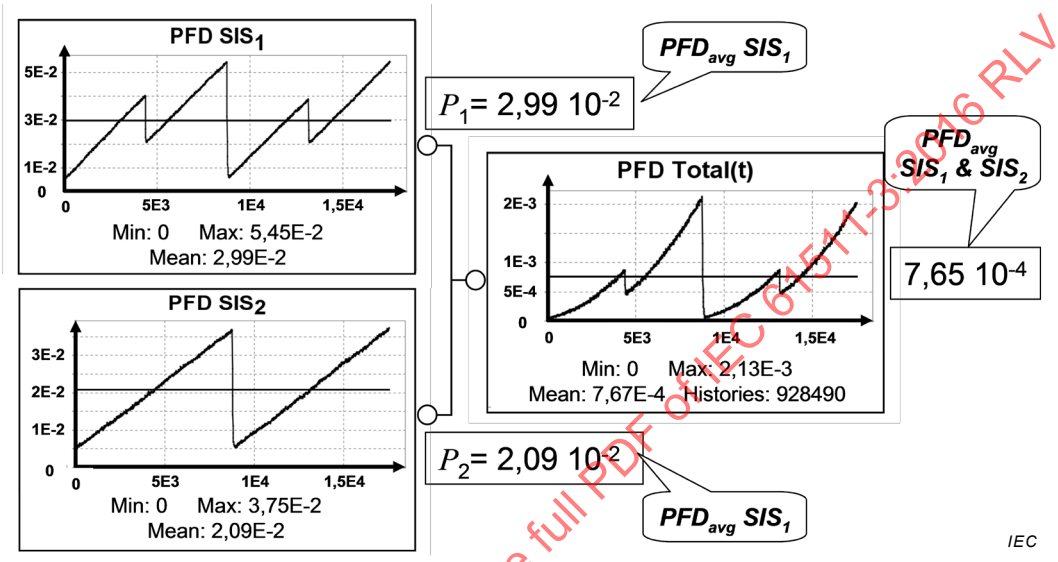


Figure J.11 – Example of output from Monte Carlo simulation

In Figure J.11 the mobilisation time and the time to reach the location of a given failure are equal to 0. Therefore the difference with the results of Figure J.6 is only due to the sharing of the repair resources. The impact is light for P_1 and P_2 and a little bit more important for the overall multiple safety system: 1/7,65x 10^{-4} = 1 307 instead of 1 360. Therefore, in this case, the dependency due to a shared repair team is light and this is why the fault tree approach which considers as many repair teams as failure modes is relevant when the probability to have two failures at the same time is small or/and when the repair times are negligible compared to the tests intervals.

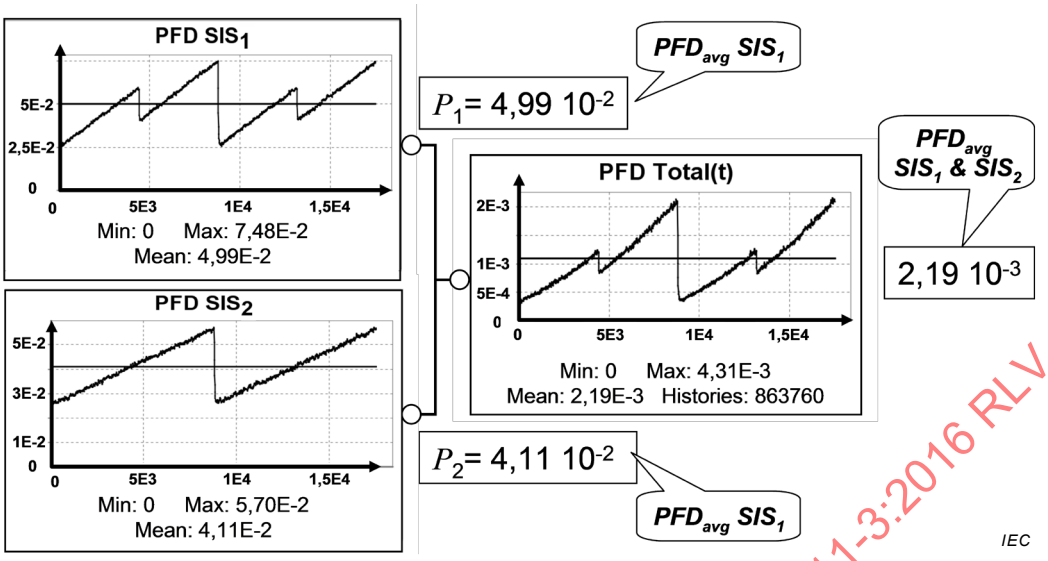


Figure J.12 – Impact of repairs due to shared repair resources

When the mobilisation time of the shared resources is not equal to 0, the repair times of individual failures are increased. In Figure J.12, the mobilisation has been taken equal to 24 h and the delay needed to reach the location of failure equal to 10 h. Then the first failure is delayed for 34 h and the other for 10 h. This impacts mainly the detected failures (i.e. the logic solver failures in our example) and almost multiplies by 2 the average unavailability's of SIS_1, SIS_2 and by 3 this of the multiple safety system: the overall risk reduction drops to 1/2,19 10 3= 457. This is about the third of the result obtained with the fault tree in Figure J.6.

The other examples presented in Figure J.7, Figure J.8 or Figure J.9 can be handled in the same way.

Annex K
(informative)

As low as reasonably practicable (ALARP) and tolerable risk concepts

K.1 General

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

UK HSE publication (2001) "*Reducing Risks, Protecting People*" ISBN 0 7176 2151 0.

K.2 ALARP model

K.2.1 Overview

Clause K.2 provides more detail to help understand the criteria associated with the ALARP method.

Clause K.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 items 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 item 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 K.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).

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.

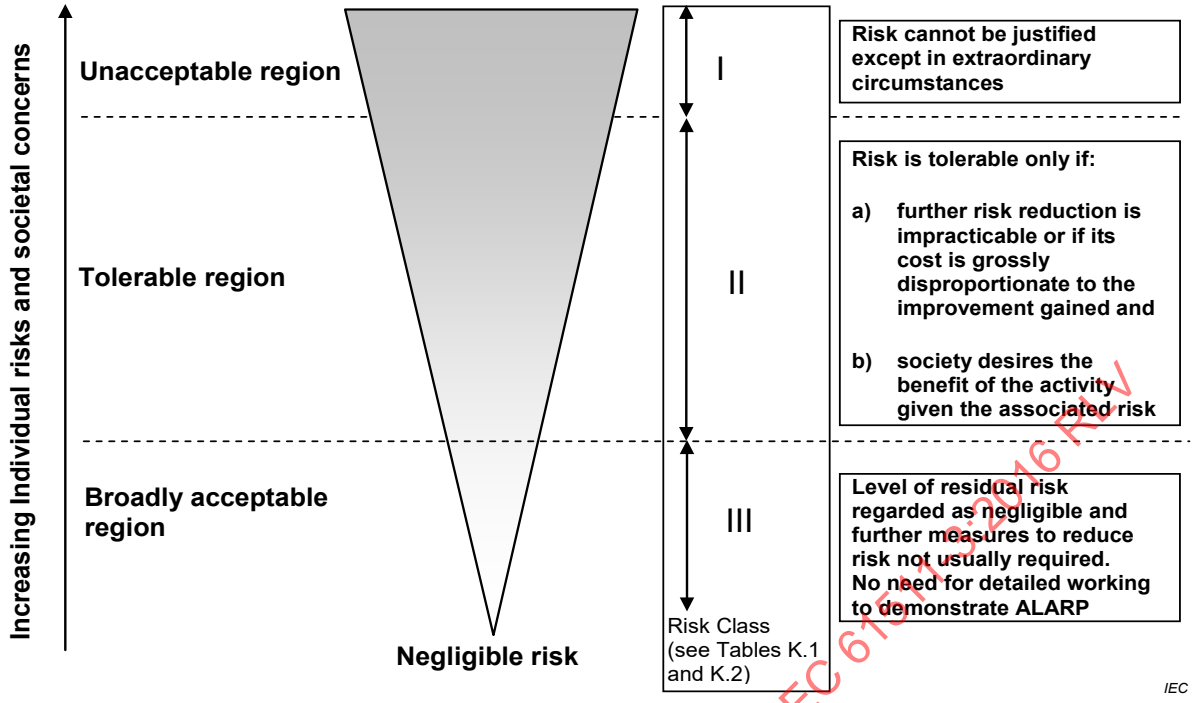


Figure K.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Sublause K.2.2 outlines a method for quantitative risk targets. (Annexes C and I (see I.4.5)) outline 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.

K.2.2 Tolerable risk target

In order to apply the ALARP principle, it is necessary to define the 3 regions of Figure K.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 K.1 is an example showing three risk classes (I, II, III) for a number of consequences and frequencies. Table K.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 K.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 K.1, the risk classes are as follows:

– 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 K.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 K.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 SIL of safety instrumented function (SIF) using, for example, one of the methods outlined in Annexes B to I.

Table K.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	III	III	III	III
NOTE 1 See Table K.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 can be seen as an example of how such a table could be populated, rather than as a specification for future use.				

Table K.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 SIF, see Annexes B to I.	

Bibliography

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61165:2006, *Application of Markov techniques*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61882:2001, *Hazard and operability studies (HAZOP studies) – Application guide*

IEC 62551:2012, *Analysis techniques for dependability – Petri net techniques*

IEC TS 62556:2014, *Ultrasonics – Field characterization – Specification and measurement of field parameters for high intensity therapeutic ultrasound (HITU) transducers and systems*

ISO/TR 12489:2013, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*

INNAL F., Contribution to modeling safety instrumented systems and assessing their performance – Critical analysis of IEC 61508:2010 standard. Thesis of the University of Bordeaux, France, 2008.

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

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008).

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

Layer of Protection Analysis-Simplified – Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

ISA-S91.00.01 *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, 2001

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

VDI/VDE 2180 (2015) *Safeguarding Of Industrial Process Plants By Means Of Process Control Engineering – Calculating Methods Of Reliability Characteristics Of Safety Instrumented Systems*

Guidance on the Application of Code Case 2211 – Overpressure Protection by System Design, Welding Research Council, PO Box 1942, New York, NY 10156, 2005, ISBN 1-58145-505-4

Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries – Pressure relieving and depressuring system, American Petroleum Institute, 1220 L Street, NW, Washington, D.C. 20005, 2007

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2007, ISBN 0-4719-7940-6

Guidelines for Initiating Events and Independent Protection Layers in LOPA, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2013

"*Using risk graphs for Safety Integrity Level (SIL) assessment – first edition*"; Clive De Salis, C; Institution of Chemical Engineers", 2011

Critical analysis of IEC 61508 standard. Thesis of the University of Bordeaux, France, 2008

SIGNORET J-P. & al., Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering and System Safety 113 (61-75), Elsevier, 2013

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61511-3 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2003. Cette édition constitue une révision technique. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

Réalisation d'exemples additionnels H&RA et d'annexes sur la considération d'analyse quantitative.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
65A/779/FDIS	65A/786/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 61511, publiées sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes instrumentés de sécurité (SIS, *Safety Instrumented System*) sont utilisés dans les industries de transformation depuis de nombreuses années pour remplir des fonctions instrumentées de sécurité (SIF, *Safety Instrumented Function*). Si l'instrumentation doit être effectivement utilisée pour réaliser des SIF, il est essentiel que cette instrumentation satisfasse à certaines normes et certains niveaux de performance minimaux.

La série IEC 61511 concerne l'application du SIS aux industries de transformation. Elle exige également de procéder à une analyse de danger et de risque relative au processus pour en déduire la spécification relative aux SIS. D'autres systèmes de sécurité sont considérés uniquement pour que leur contribution puisse être prise en compte lors de l'étude des exigences de performance des SIS. Le SIS inclut tous les appareils et sous-systèmes nécessaires pour acheminer la SIF à partir du ou des capteurs jusqu'à l'élément terminal ou jusqu'aux éléments terminaux.

La série IEC 61511 aborde deux concepts, qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité du SIS et les niveaux d'intégrité de sécurité (SIL, *Safety Integrity Levels*).

La série IEC 61511 concerne les SIS reposant sur l'utilisation d'une technologie électrique (E)/électronique(E)/électronique programmable (PE). Si d'autres technologies sont utilisées pour les solveurs logiques, il convient d'appliquer les principes fondamentaux de la série IEC 61511. La série IEC 61511 concerne également les capteurs et les éléments terminaux des SIS, quelle que soit la technologie utilisée. La série IEC 61511 est propre aux industries de transformation, dans le cadre de la série IEC 61508:2010.

La série IEC 61511 définit une approche concernant les activités relatives au cycle de vie de sécurité des SIS dans le but de satisfaire à ces normes minimales. Cette approche a été adoptée afin de mettre en œuvre une politique technique cohérente et rationnelle.

Dans la plupart des cas, la sécurité est obtenue de la meilleure façon par une conception de processus à sécurité intrinsèque. Si nécessaire, cette approche peut être combinée à un ou plusieurs systèmes de protection afin de couvrir les risques résiduels identifiés éventuels. Les systèmes de protection peuvent reposer sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Il convient que toute stratégie de sécurité prenne en compte chacun des SIS individuellement, dans le contexte des autres systèmes de protection. Pour faciliter cette approche, la série IEC 61511 couvre:

– la réalisation d'une analyse de danger et de risque pour identifier les exigences de sécurité globales;
– la prise en compte de l'affectation des exigences de sécurité aux SIS;
– l'inscription dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
– les détails de l'utilisation de certaines activités (la gestion de la sécurité, par exemple) qui peuvent être applicables à toutes les méthodes permettant d'obtenir la sécurité fonctionnelle;
– la prise en compte de toutes les phases relatives au cycle de vie de sécurité du SIS (concept initial, conception, mise en œuvre, fonctionnement, maintenance, jusqu'au déclassement);
– l'harmonisation des normes de l'industrie de transformation nationales existantes ou nouvelles par rapport à la série IEC 61511.

La série IEC 61511 vise à obtenir un haut niveau de cohérence (des principes sous-jacents, de la terminologie, de l'information, par exemple) dans le secteur des industries de transformation. Il convient qu'il présente des avantages tant du point de vue de la sécurité que du point de vue économique.

Dans les juridictions où les autorités compétentes (nationales, fédérales, étatiques, provinciales, cantonales, municipales, par exemple) ont défini des réglementations relatives à la conception de la sécurité des processus, la gestion de la sécurité des processus ou autres, ces réglementations sont prioritaires par rapport aux exigences définies dans l'IEC 61511-1.

L'IEC 61511-3 donne des lignes directrices pour déterminer le niveau d'intégrité de sécurité (SIL) exigé dans le cadre de l'analyse de danger et de risque. Les informations contenues dans le présent document ont pour but de donner un aperçu général de la grande plage de méthodes globales utilisées pour mettre en œuvre une analyse de danger et de risque. Les informations fournies ne sont pas suffisamment détaillées pour mettre en œuvre ces approches.

Avant de continuer, il convient que le concept et la détermination du SIL présentés dans l'IEC 61511-1 soient passés en revue. Les annexes informatives de l'IEC 61511-3 abordent les points suivants:

L'Annexe A donne les informations communes à chacune des méthodes d'analyse de danger et de risque décrites dans le présent document.

L'Annexe B donne un aperçu général d'une méthode semi-quantitative utilisée pour déterminer le SIL exigé.

L'Annexe C donne un aperçu général d'une méthode utilisant une matrice de sécurité pour déterminer le SIL exigé.

L'Annexe D donne un aperçu général d'une méthode utilisant un graphe de risque semi-qualitatif pour déterminer le SIL exigé.

L'Annexe E donne un aperçu général d'une méthode utilisant un graphe de risque qualitatif pour déterminer le SIL exigé.

L'Annexe F donne un aperçu général utilisant une méthode d'analyse des couches de protection (LOPA, Layer Of Protection Analysis) pour sélectionner le SIL exigé.

L'Annexe G analyse les couches de protection utilisant une matrice de risque.

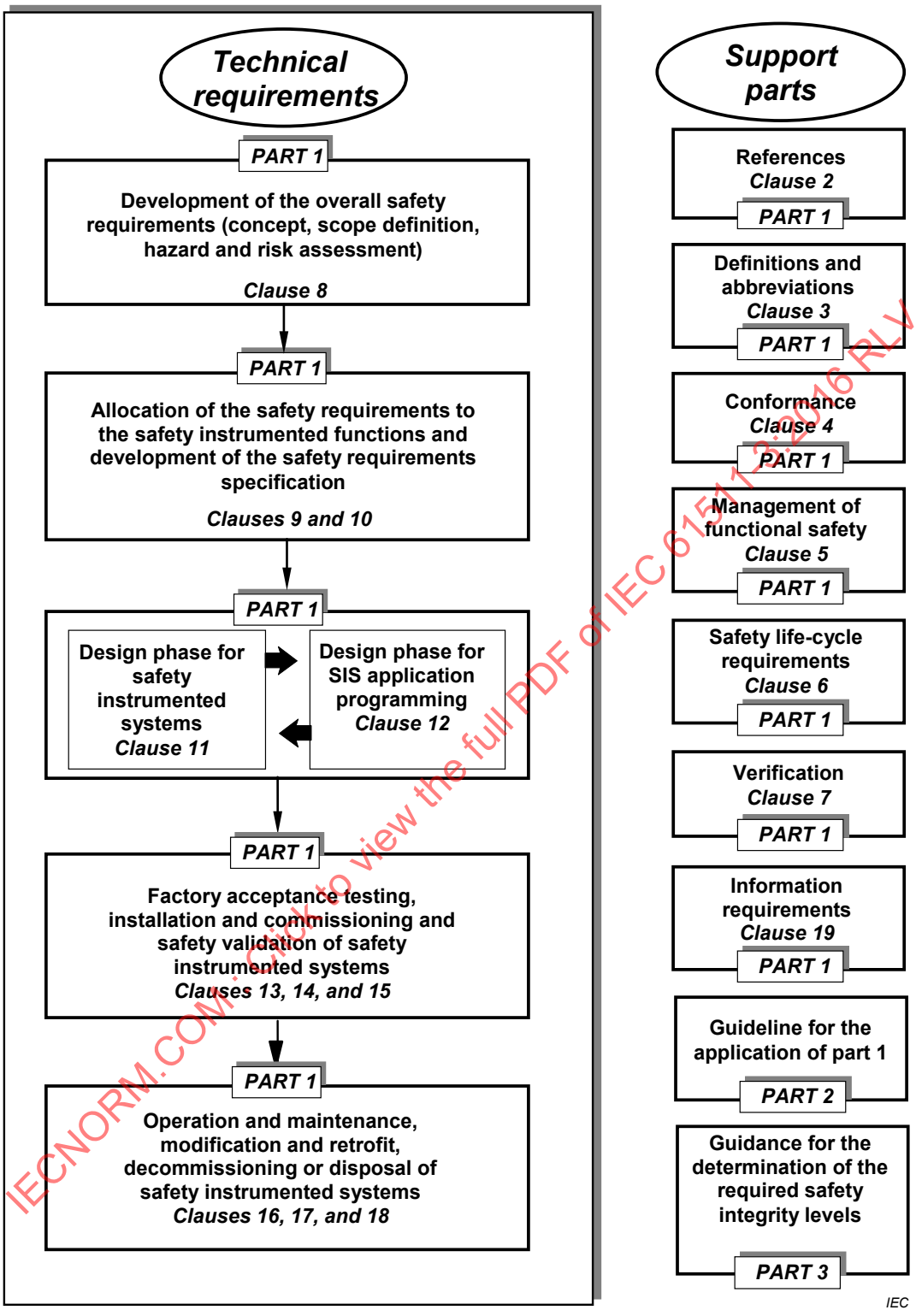
L'Annexe H donne un aperçu général d'une approche qualitative d'estimation du risque et d'allocation du SIL.

L'Annexe I donne un aperçu général des étapes de base de la conception et de l'étalonnage d'un graphe de risque.

L'Annexe J donne un aperçu général de l'impact de plusieurs systèmes de sécurité sur la détermination du SIL exigé.

L'Annexe K donne un aperçu général des concepts de risque tolérable et d'ALARP.

La Figure 1 présente le cadre général de l'IEC 61511-1, de l'IEC 61511-2 et de l'IEC 61511-3 et précise le rôle joué par la série IEC 61511 dans l'obtention de la sécurité fonctionnelle du SIS.



Anglais	Français
Technical requirements	Exigences techniques
PART 1	PARTIE 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment) Clause 8	Développement des exigences de sécurité globales (concept, définition du domaine d'application, analyse de danger et de risque) Article 8
Allocation of the safety requirements to the safety instrumented functions and development of the safety requirements specification Clauses 9 and 10	Affectation des exigences de sécurité aux fonctions instrumentées de sécurité et développement de la spécification des exigences de sécurité Articles 9 et 10
Design phase for safety instrumented systems Clause 11	Phase de conception pour les systèmes instrumentés de sécurité Article 11
Design phase for SIS application programming Clause 12	Phase de conception pour la programmation d'application du SIS Article 12
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems Clauses 13, 14, and 15	Essais de réception en usine, installation et mise en service, et validation de la sécurité des systèmes instrumentés de sécurité Articles 13, 14, et 15
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems Clauses 16,17, and 18	Fonctionnement et maintenance, modification et remise à niveau, déclassement ou mise au rebut des systèmes instrumentés de sécurité Articles 16, 17, et 18
Support parts	Parties de prise en charge
References Clause 2	Références Article 2
Definitions and abbreviations Clause 3	Définitions et abréviations Article 3
Conformance Clause 4	Conformité Article 4
Management of functional safety Clause 5	Gestion de la sécurité fonctionnelle Article 5
Safety life-cycle requirements Clause 6	Exigences relatives au cycle de vie de sécurité Article 6
Verification Clause 7	Vérification Article 7
Information requirements Clause 19	Exigences relatives aux informations Article 19
Guideline for the application of part 1	Ligne directrice pour l'application de la Partie 1
PART 2	PARTIE 2
Guidance for the determination of the required safety integrity levels	Conseils pour la détermination des niveaux exigés d'intégrité de sécurité
PART 3	PARTIE 3

Figure 1 – Cadre général de la série IEC 61511

SÉCURITÉ FONCTIONNELLE – SYSTEMES INSTRUMENTES DE SECURITE POUR LE SECTEUR DES INDUSTRIES DE TRANSFORMATION –

Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité

1 Domaine d'application

La présente partie de l'IEC 61511 donne des informations sur:

– les concepts sous-jacents de risque, et sur la relation entre risque et intégrité de sécurité (voir l'Article A.3);

– la détermination du risque tolérable (voir l'Annexe K);

– les différentes méthodes permettant de déterminer le niveau d'intégrité de sécurité (SIL) des fonctions instrumentées de sécurité (SIF) (voir les Annexes B à K);

– l'impact de plusieurs systèmes de sécurité sur les calculs déterminant la capacité à obtenir la réduction de risque souhaitée (voir l'Annexe J).

En particulier, la présente partie de l'IEC 61511:

a) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs SIF pour la protection du personnel, du grand public ou de l'environnement;

b) peut s'appliquer dans des applications non liées à la sécurité (notamment la protection des biens);

c) présente les méthodes d'analyse de danger et de risque qui peuvent être réalisées pour définir les exigences fonctionnelles de sécurité et le SIL de chaque SIF;

d) identifie des techniques et mesures disponibles pour déterminer le SIL exigé;

e) fournit un cadre pour la détermination du SIL, mais ne spécifie pas le SIL exigé pour des applications spécifiques;

f) ne donne aucun exemple de détermination des exigences relatives à d'autres méthodes de réduction de risque.

Les Annexes B à K décrivent des approches quantitatives et qualitatives qui ont été simplifiées pour présenter les principes sous-jacents. Ces annexes ont été incorporées pour présenter les principes généraux d'un certain nombre de méthodes, mais ne constituent pas une description exhaustive.

NOTE 1 Les personnes qui envisagent d'utiliser les méthodes indiquées dans ces annexes peuvent consulter le document source mentionné dans chaque annexe.

NOTE 2 Les méthodes de détermination du SIL incluses dans la Partie 3 peuvent ne pas convenir à toutes les applications. En particulier, des techniques spécifiques ou des facteurs supplémentaires qui ne sont pas présentés peuvent être exigés pour un fonctionnement en mode à sollicitation élevée ou en mode continu.

NOTE 3 Les méthodes décrites dans le présent document peuvent aboutir à des résultats imprudents lorsqu'elles sont utilisées au-delà de leurs limites sous-jacentes et lorsque des facteurs tels que la cause commune, la tolérance aux anomalies, les considérations holistiques de l'application, le manque d'expérience eu égard à la méthode utilisée, l'indépendance des couches de protection, etc. ne sont pas pris en considération correctement. Voir l'Annexe J.

La Figure 2 donne un aperçu général des couches de protection types et des moyens de réduction de risque.

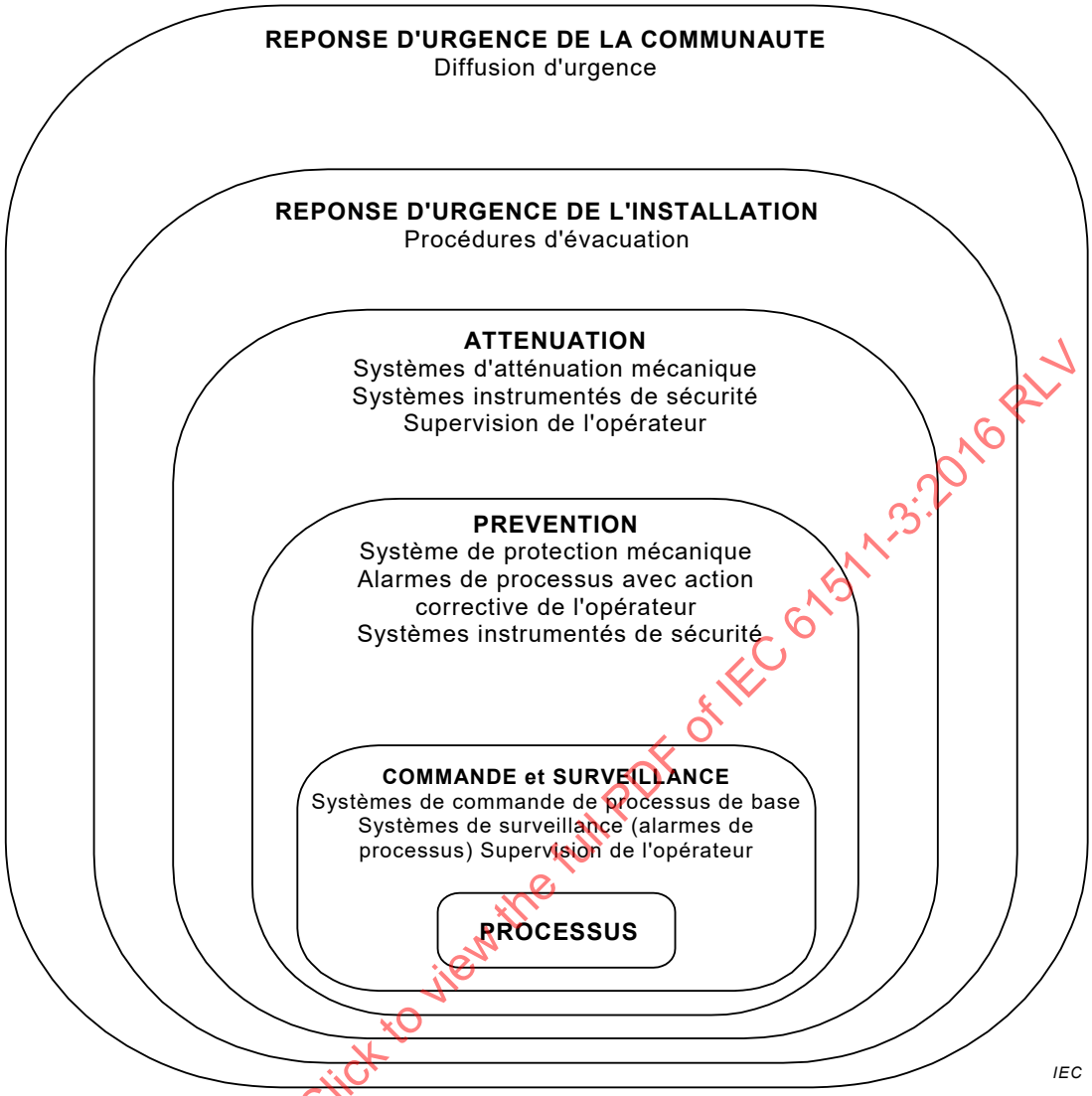


Figure 2 – Couches de protection classiques et moyens de réduction de risque

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61511-1:2016, *Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations de l'IEC 61511-1:2016 s'appliquent.

Les annexes de la présente Partie 3 sont informatives et non pas normatives. De même, l'application d'une méthode particulière décrite dans les annexes de la Partie 3 ne garantit pas la conformité aux exigences de l'IEC 61511-1:2016.

Annexe A
(informative)

Risque et intégrité de sécurité – Lignes directrices générales

A.1 Généralités

L'Annexe A donne des informations sur les concepts sous-jacents de risque et sur la relation entre risque et intégrité de sécurité. Cette information est commune à chacune des méthodes d'analyse de danger et de risque décrites dans le présent document.

A.2 Réduction de risque nécessaire

La réduction de risque nécessaire (qui peut être décrite soit de manière qualitative (voir Note 1) soit de manière quantitative (voir Note 2)) est la réduction de risque qui doit être obtenue pour satisfaire au risque tolérable (le niveau de sécurité cible du processus, par exemple) pour une situation spécifique. L'importance du concept de réduction de risque nécessaire est capitale dans le développement de la spécification des exigences de sécurité (SRS) pour les SIF (en particulier, l'exigence d'intégrité de sécurité). L'objectif de la détermination du risque tolérable (par exemple, le niveau de sécurité cible du processus) pour un événement dangereux spécifique est de définir ce qui est considéré comme raisonnable en ce qui concerne à la fois à la fréquence de l'événement dangereux et ses conséquences spécifiques. Les couches de protection (voir Figure A.2) sont conçues pour réduire la fréquence de l'événement dangereux et/ou ses conséquences.

La perception et les points de vue de ceux qui sont exposés à l'événement dangereux figurent parmi les facteurs importants à prendre en compte lors de l'évaluation du risque tolérable. Pour arriver à ce qui constitue un risque tolérable pour une application spécifique, plusieurs informations peuvent être prises en compte. Elles peuvent inclure:

– les lignes directrices émanant des autorités compétentes;
– les discussions et accords entre les différentes parties concernées par l'application;
– les normes et lignes directrices industrielles;
– les avis émanant de l'industrie, des experts indépendants et du monde scientifique;
– les exigences légales et réglementaires générales et/ou concernant directement l'application spécifique.

NOTE 1 Pour déterminer la réduction de risque nécessaire, le risque tolérable est établi. L'Annexe D et l'Annexe E de l'IEC 61508-5:2010 décrivent des méthodes qualitatives et semi-quantitatives, bien que dans les exemples donnés la réduction de risque nécessaire soit incorporée implicitement plutôt que spécifiée explicitement.

NOTE 2 Par exemple, un événement dangereux conduisant à une conséquence spécifique serait normalement exprimé comme une fréquence maximale d'occurrence par an.

A.3 Rôle des systèmes instrumentés de sécurité

Un système instrumenté de sécurité (SIS) met en œuvre les fonctions instrumentées de sécurité (SIF) exigées pour atteindre ou maintenir un état de sécurité du processus et, en tant que tel, contribue à la réduction de risque nécessaire afin de satisfaire au risque tolérable. Par exemple, la spécification des exigences de sécurité (SRS) peut stipuler que, lorsque la température atteint une valeur *x*, la vanne y s'ouvre pour laisser de l'eau pénétrer dans le récipient.

La réduction de risque nécessaire peut être obtenue par un SIS ou une combinaison de SIS ou d'autres couches de protection.

Une action humaine pourrait faire partie intégrante d'une fonction de sécurité. Par exemple, une personne pourrait recevoir des informations concernant l'état du processus et entreprendre une action de sécurité sur la base de ces informations. Si une action humaine fait partie d'une fonction de sécurité, il convient de prendre en compte tous les facteurs humains.

Une fonction instrumentée de sécurité (SIF) peut fonctionner en mode sollicitation ou en mode continu.

Il est considéré que l'intégrité de sécurité est composée des deux éléments suivants:

a) **Intégrité de sécurité du matériel** – Partie de l'intégrité de sécurité liée aux défaillances aléatoires du matériel dans un mode de défaillance dangereux. La réalisation du niveau spécifié d'intégrité de sécurité du matériel peut être estimée avec un niveau de précision raisonnable, et les exigences peuvent donc être réparties entre les sous-systèmes en utilisant les règles établies pour la combinaison des probabilités et en tenant compte des défaillances de cause commune. L'utilisation de redondances peut s'avérer nécessaire pour obtenir l'intégrité de sécurité du matériel exigée.

b) **Intégrité de sécurité systématique** – Partie de l'intégrité de sécurité liée aux défaillances systématiques dans un mode de défaillance dangereux. Bien que la contribution due à certaines défaillances systématiques puisse être estimée, les données relatives aux défaillances causées par des erreurs de conception et des défaillances de cause commune montrent que la répartition de ces défaillances peut être difficile à prédire. Cela a pour effet d'accroître l'incertitude dans les calculs de probabilité de défaillance pour une situation spécifique (par exemple, la probabilité de défaillance d'un SIS). De ce fait, un jugement doit être porté quant au choix des méthodes les plus à même de réduire cette incertitude. Il est à noter que le fait de prendre des mesures pour réduire la probabilité des défaillances aléatoires du matériel peut ne pas nécessairement réduire la probabilité de défaillance systématique. Les techniques, telles que celles utilisant des redondances de matériel identique, très efficaces pour maîtriser les défaillances aléatoires du matériel, n'ont que peu d'utilité pour réduire les défaillances systématiques.

La réduction de risque totale fournie par les fonctions instrumentées de sécurité (SIF) associées à toute autre couche de protection doit permettre de garantir que:

– la fréquence des accidents dus à la défaillance des fonctions de sécurité est suffisamment faible pour éviter que la fréquence de l'événement dangereux ne dépasse celle exigée pour satisfaire au risque tolérable; et/ou

– les fonctions de sécurité modifient les conséquences de la défaillance au degré exigé pour satisfaire au risque tolérable.

La Figure A.1 donne les concepts généraux de réduction de risque. Le modèle général prend pour hypothèse:

– qu'il existe un processus et un système de commande de processus de base (BPCS, Basic Process Control System) associé;

– qu'il existe des facteurs humains associés;

– que les caractéristiques des couches de protection de sécurité comprennent:

  - un système de protection mécanique;
  - des systèmes instrumentés de sécurité;
  - des systèmes instrumentés non SIS;
  - un système d'atténuation mécanique.

NOTE 1 La Figure A.1 est un modèle général de risque destiné à présenter les principes généraux. Un modèle de risque pour une application spécifique doit être élaboré en tenant compte de la manière spécifique dont la réduction de risque nécessaire est réellement réalisée par les systèmes instrumentés de sécurité (SIS) ou par d'autres couches de protection. De ce fait, le modèle de risque obtenu peut différer de celui donné à la Figure A.1.

Les différents risques indiqués aux Figures A.1 et A.2 sont les suivants:

– Risque de processus – Risque existant pour les événements dangereux spécifiés pour le processus, pour le système de commande de processus de base (BPCS) et pour les questions de facteur humain associées – aucune fonction de protection de sécurité désignée n'est prise en compte lors de la détermination de ce risque;
– Risque tolérable (niveau de sécurité cible du processus, par exemple) – Risque accepté dans un contexte donné en fonction des valeurs actuelles de la société;
– Risque résiduel – Dans le contexte de la présente norme, le risque résiduel est le risque d'occurrence d'événements dangereux après l'ajout de couches de protection.

Le risque de processus dépend du risque associé au processus en question, mais tient également compte de la réduction de risque induite par le système de commande de processus. Pour éviter des revendications injustifiées concernant l'intégrité de sécurité du BPCS, la série IEC 61511 impose des contraintes sur les revendications pouvant être formulées.

La réduction de risque nécessaire est le niveau minimal de réduction de risque qui doit être atteint pour satisfaire au risque tolérable. Elle peut être obtenue par une ou plusieurs techniques de réduction de risque. La réduction de risque nécessaire pour réaliser le risque tolérable spécifié, à partir d'un point de départ du risque de processus, est donnée à la Figure A.1.

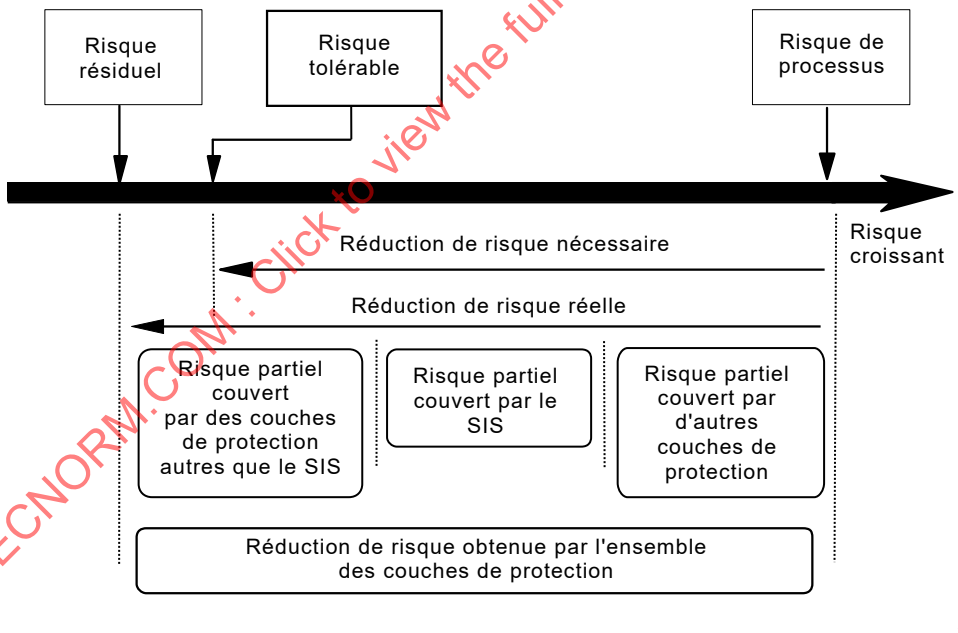


Figure A.1 – Réduction de risque: concepts généraux

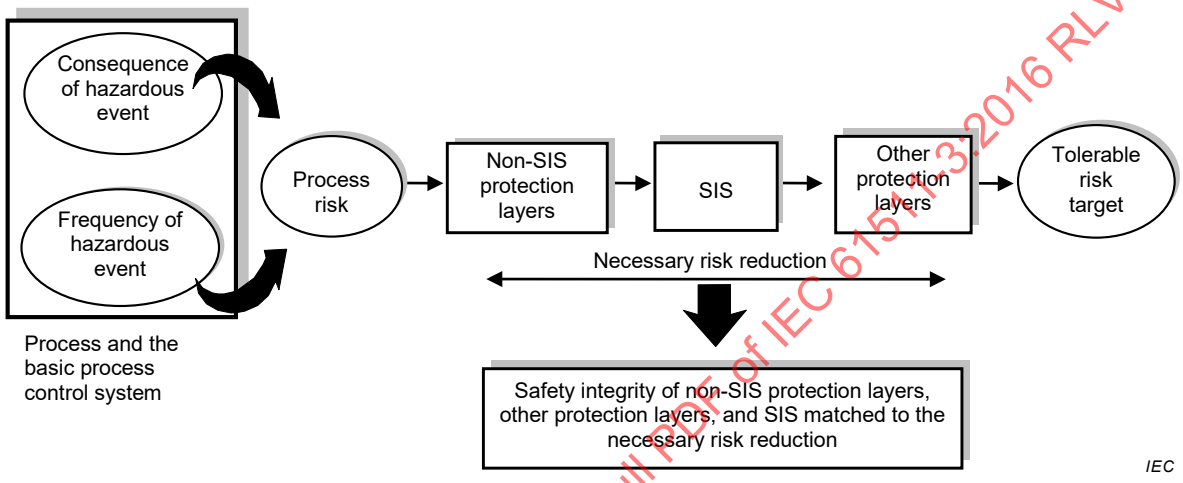
NOTE 2 Dans certaines applications, les paramètres de risque (la fréquence et la probabilité de défaillance en cas de sollicitation, par exemple) ne peuvent pas être simplement associés pour obtenir le risque cible décrit à la Figure A.1 sans tenir compte des facteurs exposés à l'Annexe J. Une superposition, une défaillance de cause commune et des dépendances holistiques entre les différentes couches de protection peuvent en être les raisons.

A.4 Risque et intégrité de sécurité

Il est important de bien faire la distinction entre les deux concepts de risque et d'intégrité de sécurité. Un risque est une mesure de la fréquence et de la conséquence d'un événement

dangereux spécifié lorsqu'il se produit. Ce risque peut être évalué pour différentes situations (risque de processus, risque tolérable, risque résiduel – voir Figure A.1). Le risque tolérable implique la prise en compte de facteurs sociaux et politiques. L'intégrité de sécurité est une mesure de la probabilité que la fonction instrumentée de sécurité (SIF) et d'autres couches de protection réaliseront la réduction de risque spécifiée. Une fois que le risque tolérable a été défini et que la réduction de risque nécessaire a été estimée, les exigences d'intégrité de sécurité peuvent être affectées au système instrumenté de sécurité (SIS).

NOTE L'affectation peut être itérative afin d'optimiser la conception et satisfaire aux différentes exigences. Les Figures A.1 et A.2 représentent le rôle des fonctions de sécurité dans la réalisation de la réduction de risque nécessaire.



Anglais	Français
Consequence of hazardous event	Conséquence de l'événement dangereux
Frequency of hazardous event	Fréquence de l'événement dangereux
Process and the basic process control system	Processus et système de commande de processus de base (BPCS)
Process risk	Risque de processus
Non-SIS protection layers	Couches de protection autres que les SIS
SIS	SIS
Other protection layers	Autres couches de protection
Tolerable risk target	Limite de risque tolérable
Necessary risk reduction	Réduction de risque nécessaire
Safety integrity of non-SIS protection layers, other protection layers, and SIS matched to the necessary risk reduction	Intégrité de sécurité des couches de protection autres que les SIS, d'autres couches de protection et des SIS adaptés à la réduction de risque nécessaire

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

A.5 Affectation des exigences de sécurité

La Figure A.4 présente l'affectation des exigences de sécurité (les fonctions de sécurité et les exigences d'intégrité de sécurité) au SIS et à d'autres couches de protection. Les exigences du processus d'affectation sont données à l'Article 9 de l'IEC 61511–1:-.

Les méthodes utilisées pour affecter les exigences d'intégrité de sécurité aux systèmes instrumentés de sécurité (SIS), aux systèmes relatifs à la sécurité utilisant d'autres technologies et aux installations externes de réduction de risque dépendent principalement de la manière dont la réduction de risque nécessaire est spécifiée, c'est-à-dire sous forme

numérique ou sous forme qualitative. Ces approches sont respectivement des méthodes semi-quantitatives, semi-qualitatives et qualitatives (voir les annexes B à I incluse).

A.6 Evénement dangereux, situation dangereuse et événement préjudiciable

Les termes "événement dangereux" et "situation dangereuse" sont souvent utilisés dans les annexes présentées ci-après dans le présent document. La Figure A.3 a pour objet de présenter la différence entre ces termes. Elle montre la progression de l'événement dangereux vers la situation dangereuse en passant par la perte de contrôle et l'occurrence d'un événement préjudiciable.

La Figure A.3 décrit le dommage causé aux personnes, mais peut également s'appliquer aux résultats d'un dommage subi par l'environnement ou de dommages matériels.

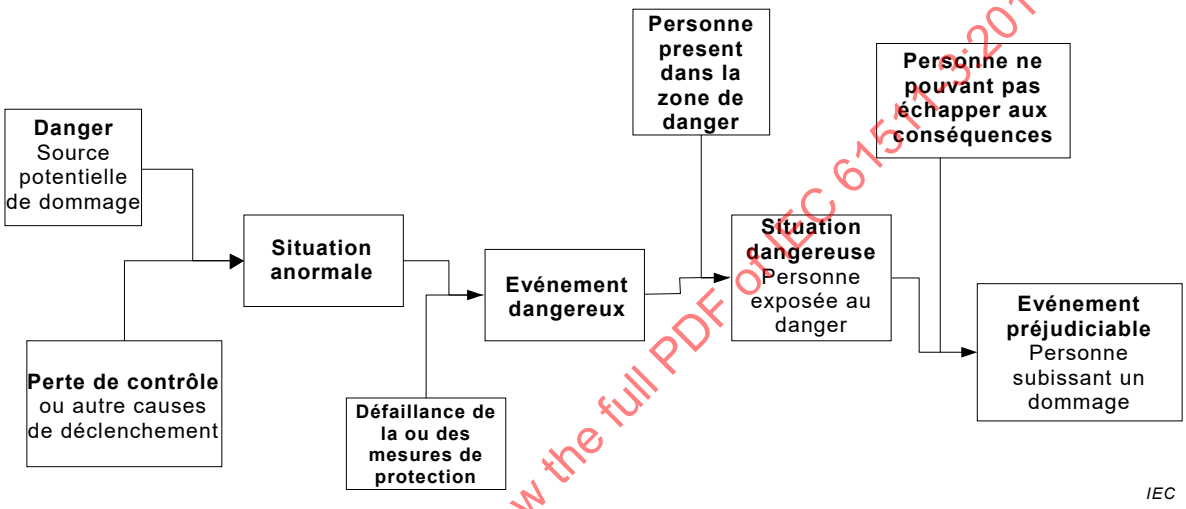


Figure A.3 – Progression de l'événement préjudiciable

La Figure A.3 montre comment la perte de contrôle, ou une autre cause initiatrice, donne lieu à une situation anormale et entraîne une sollicitation des mesures de protection, telles que les alarmes de sécurité, les systèmes instrumentés de sécurité (SIS), les soupapes de sécurité, etc. Cela devient un événement dangereux lorsqu'il y a sollicitation et que les mesures de protection concernées sont en état de défaillance et ne fonctionnent pas comme prévu. Un événement dangereux en soi et au-delà ne conduit pas forcément à un dommage, mais si une ou plusieurs personnes se situent dans la zone d'impact (ou zone d'effet) et se trouvent donc exposées à l'événement dangereux, cela devient une situation dangereuse. Si la personne ne peut pas échapper aux conséquences préjudiciables de l'exposition, l'événement est caractérisé comme étant préjudiciable en raison des dommages corporels.

A.7 Niveaux d'intégrité de sécurité

Dans l'IEC 61511-1:2016, quatre niveaux d'intégrité de sécurité (SIL) sont spécifiés. Le SIL 4 est le niveau le plus élevé et le SIL 1 est le niveau le plus bas.

Les niveaux objectifs de défaillances des quatre SIL sont spécifiés au Tableau 4 et au Tableau 5 de l'IEC 61511–1:2016. Deux paramètres sont spécifiés, l'un pour le SIS fonctionnant en mode à faible sollicitation, et l'autre pour le SIS fonctionnant en mode sollicitation continue/à sollicitation élevée.

NOTE Pour un SIS fonctionnant en mode à faible sollicitation, le niveau objectif de défaillances qui présente un intérêt est la probabilité moyenne de défaillance du système lorsque celui-ci fonctionne sur sollicitation. Pour un SIS fonctionnant en mode sollicitation continue/à sollicitation élevée, le niveau objectif de défaillances qui présente un intérêt est la fréquence moyenne de défaillance dangereuse. Voir 3.2.83 et le Tableau 5 de l'IEC 61511-1:2016.

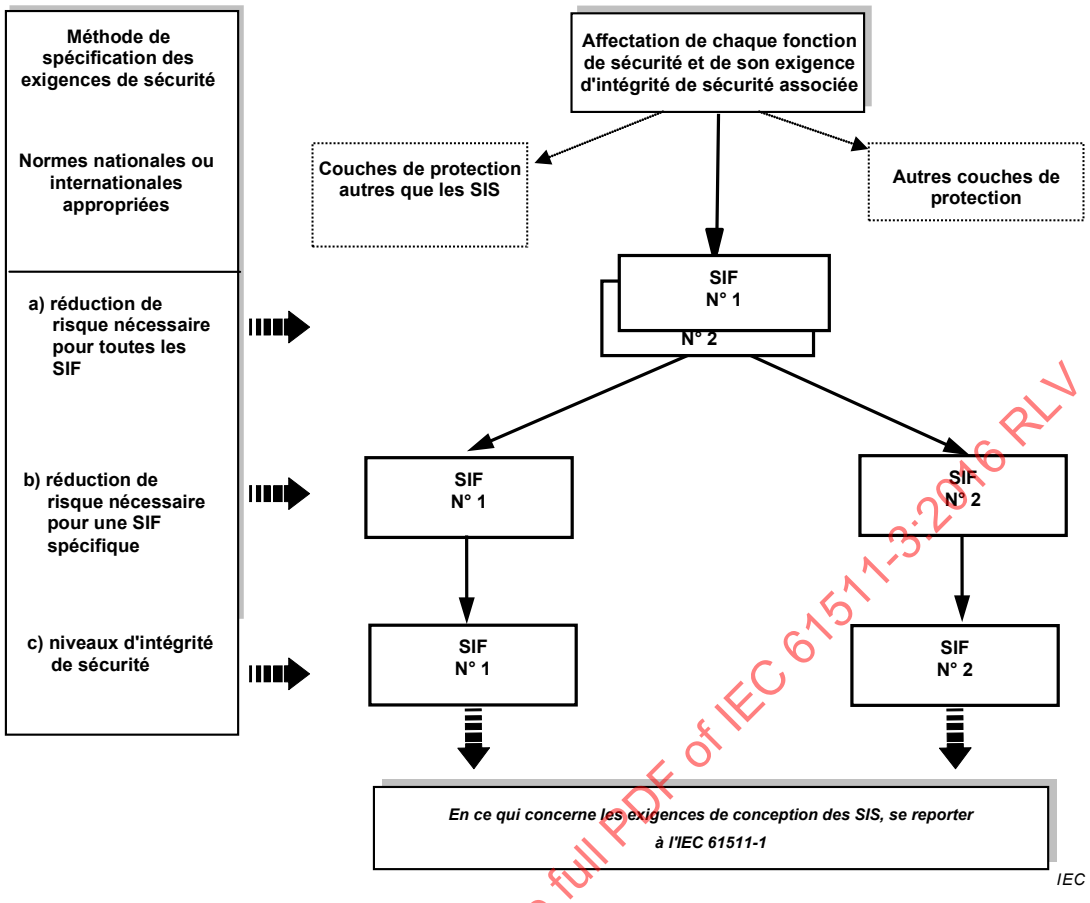
A.8 Choix de la méthode pour la détermination du niveau exigé d'intégrité de sécurité

Il existe plusieurs méthodes de détermination du niveau exigé d'intégrité de sécurité pour une application donnée. Les Annexes B à I fournissent des informations sur un certain nombre de méthodes utilisées. La méthode choisie pour une application spécifique dépendra de plusieurs facteurs, parmi lesquels:

– la complexité de l'application;
– les lignes directrices émanant des autorités compétentes;
– la nature du risque et la réduction de risque exigée;
– l'expérience et les compétences des personnes disponibles pour réaliser ce travail;
– les informations disponibles concernant les paramètres relatifs au risque (voir la Figure A.4);
– les informations disponibles sur les SIS actuellement utilisées dans les applications particulières, notamment celles décrites dans les normes et pratiques industrielles.

Dans certaines applications, plusieurs méthodes peuvent être utilisées. Une méthode qualitative peut être employée en tant que première approche pour déterminer le niveau d'intégrité de sécurité (SIL) exigé pour toutes les fonctions instrumentées de sécurité (SIF). Il convient que les applications auxquelles a été affecté un SIL 3 ou un SIL 4 par cette méthode fassent ensuite l'objet d'une étude plus détaillée en utilisant une méthode quantitative permettant de comprendre de manière plus rigoureuse leur intégrité de sécurité exigée.

Il est important de noter qu'il convient d'utiliser les critères de risque du site pour l'évaluation, quelles que soient les méthodes sélectionnées pour l'application.



NOTE Des exigences d'intégrité de sécurité sont associées à chaque SIF avant affectation (voir l'IEC 61511-1:2016, Article 9).

Figure A.4 – Affectation des exigences de sécurité aux couches de protection autres que les SIS et aux autres couches de protection

Annexe B
(informative)

Méthode semi-quantitative – analyse par arbre d'événement

B.1 Présentation

L'Annexe B décrit la manière dont les niveaux d'intégrité de sécurité (SIL) cibles peuvent être déterminés si une approche semi-quantitative est employée. Une approche semi-quantitative utilise à la fois des techniques qualitatives et quantitatives. Son utilisation est particulièrement intéressante lorsque le risque tolérable doit être spécifié sous une forme numérique (par exemple, lorsqu'il convient qu'une conséquence spécifiée ne se produise pas avec une fréquence supérieure à 1 fois tous les 100 ans).

L'Annexe B ne prétend pas fournir une description exhaustive de la méthode, mais est uniquement destinée à fournir un aperçu des principes généraux. Elle est fondée sur une méthode décrite de manière plus détaillée dans la référence suivante:

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures,* Third Edition, Wiley-Interscience, New York (2008) (disponible en anglais seulement).

B.2 Conformité à l'IEC 61511-1:2016

L'objectif général de la présente Annexe B est de décrire une procédure permettant d'identifier les fonctions instrumentées de sécurité (SIF) exigées et d'établir leurs niveaux d'intégrité de sécurité (SIL). Pour assurer la conformité, les étapes fondamentales exigées sont les suivantes:

a) Etablir l'objectif de sécurité (risque tolérable) pour le processus;

b) Procéder à une analyse de danger et de risque afin d'évaluer le risque existant pour chaque événement dangereux spécifique;

c) Identifier la/les fonction(s) de sécurité nécessaire(s) pour chaque événement dangereux spécifique;

d) Affecter la/les fonction(s) de sécurité aux couches de protection;

NOTE Il est pris pour hypothèse que les couches de protection sont indépendantes les unes des autres. Le processus d'affectation peut garantir que les défaillances de cause commune, de mode commun et systématiques soient suffisamment faibles par rapport aux exigences de réduction de risque globale.

e) Déterminer si une fonction instrumentée de sécurité (SIF) est exigée;

f) Déterminer le SIL exigé de la SIF.

L'étape a) établit la sécurité cible du processus. L'étape b) traite essentiellement de l'analyse de risque du processus, tandis que l'étape c) déduit, à partir de l'analyse de risque, les fonctions de sécurité qui sont exigées ainsi que la réduction de risque dont elles ont besoin pour satisfaire à la sécurité cible du processus. L'affectation de ces fonctions de sécurité aux couches de protection à l'étape d) permettra de voir clairement si une SIF est exigée (étape e)) ainsi que le SIL dont elle aura besoin pour satisfaire à la conformité (étape f)).

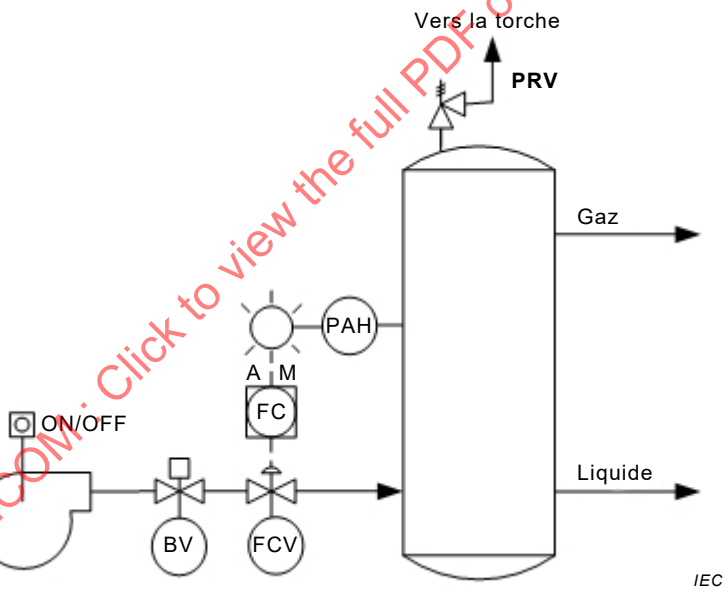
L'Annexe B propose d'utiliser une technique d'analyse de risque semi-quantitative pour satisfaire aux objectifs de l'IEC 61511-1:2016, Article 8. Une technique est représentée par un exemple simple.

B.3 Exemple

B.3.1 Généralités

Un processus est considéré comme utilisant un récipient sous pression avec alimentation par pompe et deux sorties (liquide et gaz) contenant un mélange de gaz et de liquide inflammable volatil et de l'instrumentation associée (voir Figure B.1). La commande du processus s'effectue à partir d'un système de commande de processus de base (BPCS) qui surveille le signal provenant du transmetteur de débit et commande l'actionnement d'une vanne. Les systèmes d'ingénierie disponibles sont les suivants: a) un transmetteur de pression indépendant qui déclenche une alarme de pression élevée et alerte l'opérateur afin qu'il mette en œuvre l'action appropriée pour arrêter la pénétration de matériau; et b) en l'absence de réponse de l'opérateur, une couche de protection non instrumentée (vanne de limitation de la pression) qui traite les dangers liés à la pression élevée à l'intérieur du récipient. Les dégagements par la vanne de limitation de la pression sont acheminés par un tuyau jusqu'à un réservoir de séparation qui libère les gaz dans un système de torche. Dans cet exemple, il est pris pour hypothèse que le système de torche est dûment homologué, conçu, installé et en exploitation; les défaillances potentielles du système de torche ne sont donc pas prises en considération dans cet exemple.

NOTE Le terme "systèmes d'ingénierie" se rapporte à tous les systèmes disponibles pour répondre à une sollicitation du processus, y compris d'autres systèmes de protection instrumentés, et à l'action/aux actions associée(s) de l'opérateur.



Légende
FC Contrôleur de flux
FCV Vanne de commande de flux
PAH Alarme de pression élevée
BV Vanne de sectionnement
PRV Vanne de limitation de la pression

Figure B.1 – Récipient sous pression avec systèmes de sécurité existants

B.3.2 Cible de sécurité du processus

Pour garantir la bonne gestion du risque industriel, une exigence fondamentale consiste à définir de façon claire et concise la sécurité cible du processus (ou risque tolérable) souhaitée. Cela peut être défini par l'utilisation de réglementations et de normes nationales et internationales, de politiques d'entreprise et la prise en considération des opinions des parties concernées telles que le public, la juridiction locale et les compagnies d'assurance, l'ensemble étant soutenu par la mise en œuvre de bonnes pratiques techniques. La sécurité cible du processus est propre à un processus, une société ou une industrie. Il convient donc

de ne pas généraliser sans que des réglementations et des normes justifient de telles généralisations. Pour cet exemple de présentation, partir de l'hypothèse que la sécurité cible du processus est établie à un taux de dégagement moyen de moins de 10^{-4} par an, en fonction des conséquences attendues du dégagement sur l'environnement.

B.3.3 Analyse de danger

Il convient d'effectuer une analyse de danger destinée à identifier les dangers, les écarts potentiels du processus et leurs causes, les systèmes d'ingénierie disponibles, les événements initiateurs ainsi que les événements dangereux potentiels (accidents) pouvant se produire. Pour cela, plusieurs techniques qualitatives peuvent être utilisées:

– revues de sécurité;
– listes de contrôle;
– analyse prédictive par simulation;
– étude HAZOP;
– analyse des modes de défaillance et de leurs effets;
– l'analyse cause-conséquence.

L'analyse HAZOP (HAZard and OPerability) est une technique qui est largement employée. L'analyse (ou l'étude) HAZOP permet d'identifier et d'évaluer les dangers dans une installation de processus, ainsi que les problèmes d'opérabilité non dangereux qui compromettent son aptitude à atteindre la productivité de calcul.

En guise de deuxième étape, une analyse HAZOP est effectuée pour l'exemple de présentation fourni à la Figure B.1. Le but de cette étude HAZOP est d'évaluer les événements dangereux qui peuvent entraîner le dégagement du matériau dans l'environnement. Une liste abrégée est énumérée au Tableau B.1 pour donner les résultats HAZOP.

Les résultats de l'étude HAZOP ont permis d'établir qu'une condition de surpression pourrait provoquer un dégagement du matériau inflammable dans l'environnement. La pression élevée est un écart de processus qui pourrait se transformer en événement dangereux menant à de multiples scénarios en fonction de la réponse fournie par les systèmes d'ingénierie disponibles. Si une étude HAZOP complète a déjà été effectuée pour le processus, d'autres événements initiateurs qui pourraient provoquer un dégagement de matériau dans l'environnement peuvent inclure des fuites dans les équipements du processus, une rupture totale de la canalisation et des événements externes (par exemple: incendie). Pour cet exemple de présentation, la condition de surpression est examinée.

Tableau B.1 – Résultats de l'analyse HAZOP

Elément	Ecarts	Causes	Conséquences	Protections	Action
Récipient	Flux élevé	Défaillance de la boucle de commande de flux	Un flux élevé provoque une pression élevée (voir Note ci-dessous)		
	Pression élevée	1) Défaillance de la boucle de commande de flux 2) Incendie externe	Endommagement du récipient et dégagement dans l'environnement	1) Alarme de pression élevée 2) Système déluge 3) Vanne de limitation de la pression	Evaluation des conditions de conception pour le dégagement par la vanne de limitation de la pression dans l'environnement
	Débit faible/ inexistant	Défaillance de la boucle de commande de flux	Aucune conséquence présentant un intérêt		
	Débit inversé		Aucune conséquence présentant un intérêt		

NOTE Pour cet exemple, il est pris pour hypothèse que le récipient peut présenter une pression élevée en raison de l'inaptitude de l'équipement en aval à gérer le flux de gaz total provenant du récipient lorsque le débit d'alimentation est trop élevé.

B.3.4 Technique d'analyse de risque semi-quantitative

Une estimation du risque de processus est effectuée par le biais d'une analyse de risque semi-quantitative, qui identifie et quantifie les risques associés aux accidents de processus ou aux événements dangereux potentiels. Les résultats peuvent être utilisés pour identifier les fonctions de sécurité nécessaires et leur niveau d'intégrité de sécurité (SIL) associé dans le but de réduire le risque de processus jusqu'à un niveau acceptable. L'évaluation du risque de processus au moyen de techniques semi-quantitatives peut être distinguée lors des étapes majeures suivantes. Les quatre premières étapes peuvent être exécutées au cours de l'étude HAZOP.

a) Identifier les dangers liés au processus;

b) Identifier les événements initiateurs;

c) Elaborer des scénarios d'événements dangereux pour chaque événement initiateur;

d) Identifier la composition de la couche de protection;

NOTE 1 Les fonctions de sécurité sont affectées aux couches de protection afin d'assurer la protection d'un processus. Elles incluent les SIS et d'autres moyens de réduction de risque (voir la Figure B.2).

NOTE 2 Cette étape s'applique à l'exemple ci-dessus, puisqu'il est question d'un processus existant doté de couches de protection existantes.

e) Vérifier la fréquence d'occurrence des événements initiateurs et la fiabilité des fonctions de sécurité existantes en utilisant des données historiques ou des techniques de modélisation (analyse par arbre d'événement, analyse des modes de défaillance et de leurs effets, analyse par arbre des défaillances, par exemple);

f) Quantifier la fréquence d'occurrence des événements dangereux significatifs;

g) Evaluer les conséquences de tous les événements dangereux significatifs;

h) Intégrer les résultats (conséquences et fréquence d'un accident) dans l'analyse de risque associée à chaque événement dangereux.

Les résultats significatifs présentant un intérêt sont les suivants:

– une compréhension plus fine et détaillée des dangers et des risques associés au processus;

– une connaissance du risque de processus;

– la contribution des fonctions de sécurité existantes à la réduction de risque globale;
– l'identification de chaque fonction de sécurité nécessaire pour réduire le risque de processus jusqu'à un niveau acceptable;
– une comparaison entre le risque de processus estimé et le risque cible.

La technique semi-quantitative nécessite des ressources considérables, mais offre des avantages autres que ceux offerts par les approches qualitatives. La technique s'appuie largement sur les compétences d'une équipe à identifier des dangers, fournit une approche explicite pour traiter les systèmes de sécurité existants utilisant d'autres technologies, utilise un cadre pour documenter toutes les activités qui ont conduit aux résultats énoncés et fournit un système pour la gestion du cycle de vie.

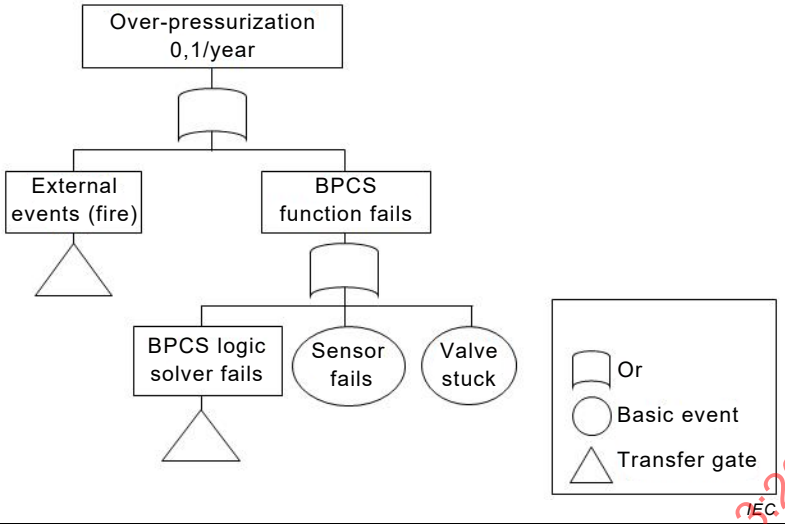
En ce qui concerne l'exemple de présentation, l'étude HAZOP a permis d'établir qu'un événement dangereux – la surpression – peut entraîner le dégagement de matériau dans l'environnement. Il convient de noter que l'approche utilisée en B.3.4 est la combinaison d'une analyse quantitative de la fréquence de l'événement dangereux et d'une évaluation qualitative des conséquences. Cette approche est utilisée pour présenter la procédure systématique qu'il convient de suivre afin d'identifier les événements dangereux et les fonctions instrumentées de sécurité (SIF).

B.3.5 Analyse de risque du processus existant

L'étape suivante consiste à identifier les facteurs qui peuvent contribuer au développement de l'événement initiateur. La Figure B.2 présente un arbre des défaillances simple, qui identifie un certain nombre d'événements qui contribuent au développement d'une condition de surpression à l'intérieur du récipient. L'événement de tête, à savoir la surpression interne du récipient, est provoqué par la défaillance du BPCS (p. ex.: boucle de commande de flux) ou par un incendie externe (voir le Tableau B.1).

Le but de l'arbre des défaillances est de mettre l'accent sur l'impact de la défaillance du BPCS sur le processus, et la fréquence d'un incendie externe est considérée comme négligeable en comparaison. Le BPCS n'accomplit aucune fonction de sécurité. Toutefois, sa défaillance contribue à solliciter encore plus l'intervention du système instrumenté de sécurité (SIS). De ce fait, un BPCS fiable réduirait la sollicitation d'intervention du système instrumenté de sécurité (SIS).

L'arbre des défaillances peut être quantifié et, pour cet exemple, la fréquence de la condition de surpression est, par hypothèse, de l'ordre de 10^{-1} fois par an. Il est à noter que chaque cause présentée à la Figure B.2 est par hypothèse indépendante (autrement dit qu'elle ne chevauche pas) des autres causes, avec un taux de défaillances exprimé en événements par année.



Anglais	Français
Over-pressurization	Surpression
0,1/year	0,1/an
External events	Evénements externes
(fire)	(incendie)
BPCS function fails	Défaillance d'une fonction du BPCS
BPCS logic solver fails	Défaillance du solveur logique du BPCS
Sensor fails	Défaillance du capteur
Valve stuck	Blocage de la vanne
OR	OR
Basic event	Evénement de base
Transfer gate	Porte de transfert

Figure B.2 – Arbre des défaillances pour la surpression du récipient

NOTE 1 La Figure B.2 présente l'arbre des défaillances sans tenir compte des mesures de protection.

Une fois que la fréquence d'occurrence de l'événement initiateur a été établie, l'aptitude des systèmes de sécurité à répondre ou non à la condition anormale est modélisée au moyen d'une analyse par arbre d'événement. Les données de fiabilité relatives aux performances des systèmes de sécurité peuvent être obtenues à partir de données acquises sur le terrain ou des bases de données publiées, voire être prédites en utilisant des techniques de modélisation de fiabilité.

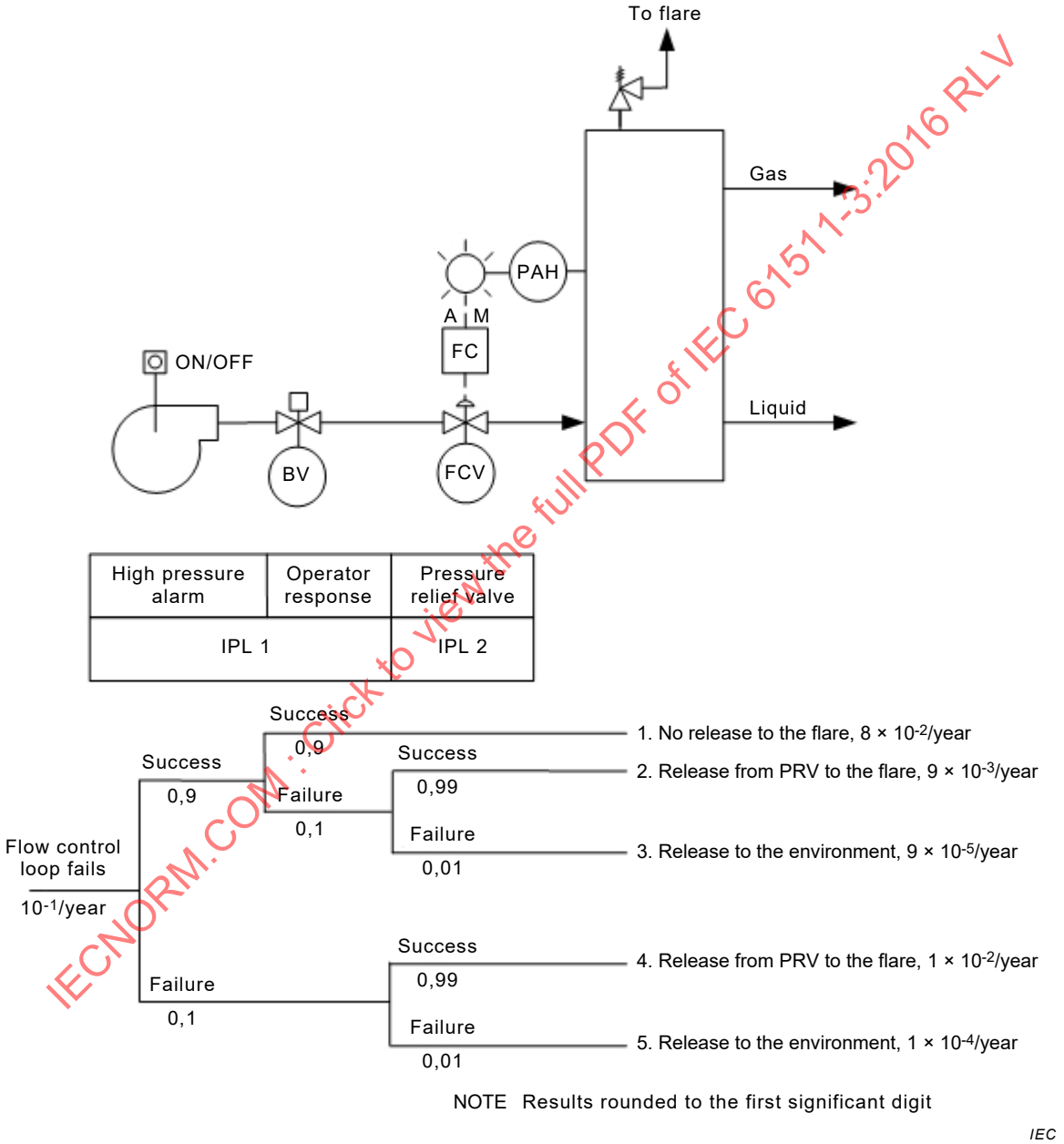
Dans cet exemple, les données de fiabilité relèvent de l'hypothèse et il convient de ne pas considérer qu'elles représentent les performances publiées ou prévues du système. La Figure B.3 présente les scénarios de résultat potentiels qui pourraient donner une condition de surpression. Les résultats de la modélisation d'événement sont: a) la fréquence d'occurrence de chaque séquence de l'événement, et b) les conséquences qualitatives en termes de résultats de l'événement.

A la Figure B.3, cinq scénarios de résultats sont identifiés, présentant chacun une fréquence d'occurrence et l'énoncé d'une conséquence qualitative. Le scénario de résultats n° 1 implique une réponse de l'opérateur à l'alarme de pression élevée, présente une fréquence d'occurrence de 8×10^{-2} par an et entraîne une réduction de la production sans dégagement. Il s'agit d'une condition de conception acceptable du processus, et l'opérateur est formé et soumis à l'essai par rapport à la réponse adéquate pour réaliser la réduction de risque.

Les scénarios de résultats n° 2 et 4 impliquent le dégagement de matériau dans la torche, présentent une fréquence combinée de $1{,}9 \times 10^{-2}$ par an ($9 \times 10^{-3} + 1 \times 10^{-2}$) et sont également considérés comme une condition de conception du processus. Les autres

scénarios de résultats (3 et 5) présentent une fréquence d'occurrence combinée de $1,9 \times 10^{-4}$ par an ($9 \times 10^{-5} + 1 \times 10^{-4}$) et entraînent l'endommagement du récipient, ainsi que le dégagement de matériau dans l'environnement (voir Note 2).

Il convient de noter que cette analyse ne tient pas compte du fait qu'il puisse avoir une défaillance de cause commune de l'alarme de pression élevée, ainsi qu'une défaillance du capteur de débit du système de commande de processus de base (BPCS). Une telle défaillance de cause commune pourrait entraîner une hausse significative de la fréquence d'occurrence pour les résultats n° 3 et donc une augmentation du risque global.



NOTE Results rounded to the first significant digit

IEC

Anglais	Français
To flare	Vers la torche
Gas	Gaz
Liquid	Liquide
High pressure alarm	Alarme de pression élevée
Operator response	Réponse de l'opérateur
Pressure relief valve	Vanne de limitation de la pression
Flow control loop fails	Défaillance de la boucle de commande de flux
10^{-1}/year	10^{-1}/an
Success	Réussite
Failure	Défaillance
No release to the flare	Pas de dégagement vers la torche
8×10^{-2}/year	8×10^{-2}/an
Release from PRV to the flare	Dégagement entre la vanne de limitation de la pression et la torche
9×10^{-3}/year	9×10^{-3}/an
Release to the environment	Dégagement dans l'environnement
9×10^{-5}/year	9×10^{-5}/an
1×10^{-2}/year	1×10^{-2}/an
1×10^{-4}/year	1×10^{-4}/an
NOTE	NOTE
Results rounded to the first significant digit	Résultats arrondis au premier chiffre significatif

Figure B.3 – Evénements dangereux avec des systèmes de sécurité existants

NOTE 2 Dans certaines applications, la fréquence et la probabilité de défaillance en cas de sollicitation ne peuvent pas être multipliées (voir la Figure B.3). Ce phénomène peut être dû à un chevauchement, une défaillance de cause commune et des dépendances holistiques entre les différentes couches de protection. Voir l'Annexe J.

NOTE 3 Chaque événement indiqué à la Figure B.3 est censé être indépendant des autres. De plus, les données indiquées sont approximatives; par conséquent, la somme des fréquences de tous les accidents s'approche de la fréquence de l'événement initiateur (0,1 par an).

B.3.6 Evénements ne satisfaisant pas à la sécurité cible du processus

Comme indiqué précédemment, des lignes directrices spécifiques à l'installation établissent la sécurité du processus comme suit: pas de dégagement de matériau dans l'environnement selon une fréquence d'occurrence supérieure à 10^{-4} par an. La fréquence globale des dégagements dans l'environnement est égale à $1{,}9 \times 10^{-5}$ (scénario n° 3) + $1{,}9 \times 10^{-4}$ (scénario n° 5) = $1{,}92 \times 10^{-4}$ par an, ce qui est supérieur à la sécurité cible du processus. Compte tenu de la fréquence d'occurrence des événements dangereux et des données relatives aux conséquences indiquées à la Figure B.3, une réduction de risque supplémentaire doit être réalisée pour que les scénarios de résultats n° 2, 3 et 5 se situent en dessous de la sécurité cible du processus.

B.3.7 Réduction de risque au moyen d'autres couches de protection

Il convient d'envisager les couches de protection utilisant d'autres technologies avant de définir le besoin d'une fonction instrumentée de sécurité (SIF) mise en œuvre dans un système instrumenté de sécurité (SIS). Un système déluge est cité comme une protection dans le Tableau B.1, mais il n'empêche ni l'endommagement du récipient ni le dégagement dans l'environnement.

L'objectif de l'analyse étant de minimiser le risque lié au dégagement de matériau dans l'environnement, il peut être pris pour hypothèse que le système déluge ne constitue pas un

plan de réduction de risque acceptable en ce qui concerne l'endommagement du récipient ou le dégagement dans l'environnement. Le système déluge réduit le risque pour le personnel et le transfert d'événements, qui ne sont pas évalués dans cet exemple.

B.3.8 Réduction de risque au moyen d'une fonction instrumentée de sécurité

La sécurité cible du processus ne peut pas être réalisée en utilisant des couches de protection utilisant d'autres technologies. Afin de réduire la fréquence globale des dégagements dans l'atmosphère, une nouvelle fonction instrumentée de sécurité (SIF) présentant un niveau d'intégrité de sécurité (SIL) 2 doit satisfaire à la sécurité cible du processus. La nouvelle SIF est montrée à la Figure B.4.

A ce stade, une conception détaillée de la SIF n'est pas nécessaire. Un concept général de conception de la SIF est suffisant. L'objectif de cette étape est de déterminer si une nouvelle SIF de SIL 2 apportera la réduction de risque exigée et permettra d'atteindre la sécurité cible du processus. La conception détaillée de la SIF interviendra après la détermination de la sécurité cible du processus. Pour cet exemple, la nouvelle SIF utilise des capteurs de pression jumelés, consacrés à la sécurité dans une configuration 1oo2 (non présentés dans la Figure B.4) qui transmettent des signaux à un solveur logique. La sortie du solveur logique commande la vanne d'arrêt et la pompe.

NOTE 1oo2 signifie que l'un ou l'autre des capteurs de pression peut déclencher l'arrêt du processus.

La nouvelle SIF de SIL 2 est utilisée pour minimiser la fréquence d'un dégagement provenant d'un récipient sous pression à cause d'une surpression. La Figure B.4 présente la nouvelle couche de protection et fournit tous les scénarios d'accidents potentiels. Comme l'indique cette figure, la fréquence d'un dégagement provenant de ce récipient peut être réduite à une valeur inférieure ou égale à 10^{-4} par an, et la sécurité cible du processus peut être satisfaite sous réserve de pouvoir établir que la SIF satisfait aux exigences du SIL 2.

Dans la Figure B.4, sept scénarios de résultats sont identifiés, présentant chacun une fréquence d'occurrence et une conséquence qualitative. La fréquence du scénario de résultats n° 1 est la même que celle susmentionnée. La réponse de l'opérateur entraîne une réduction de la production à une fréquence de 8×10^{-2} par an.

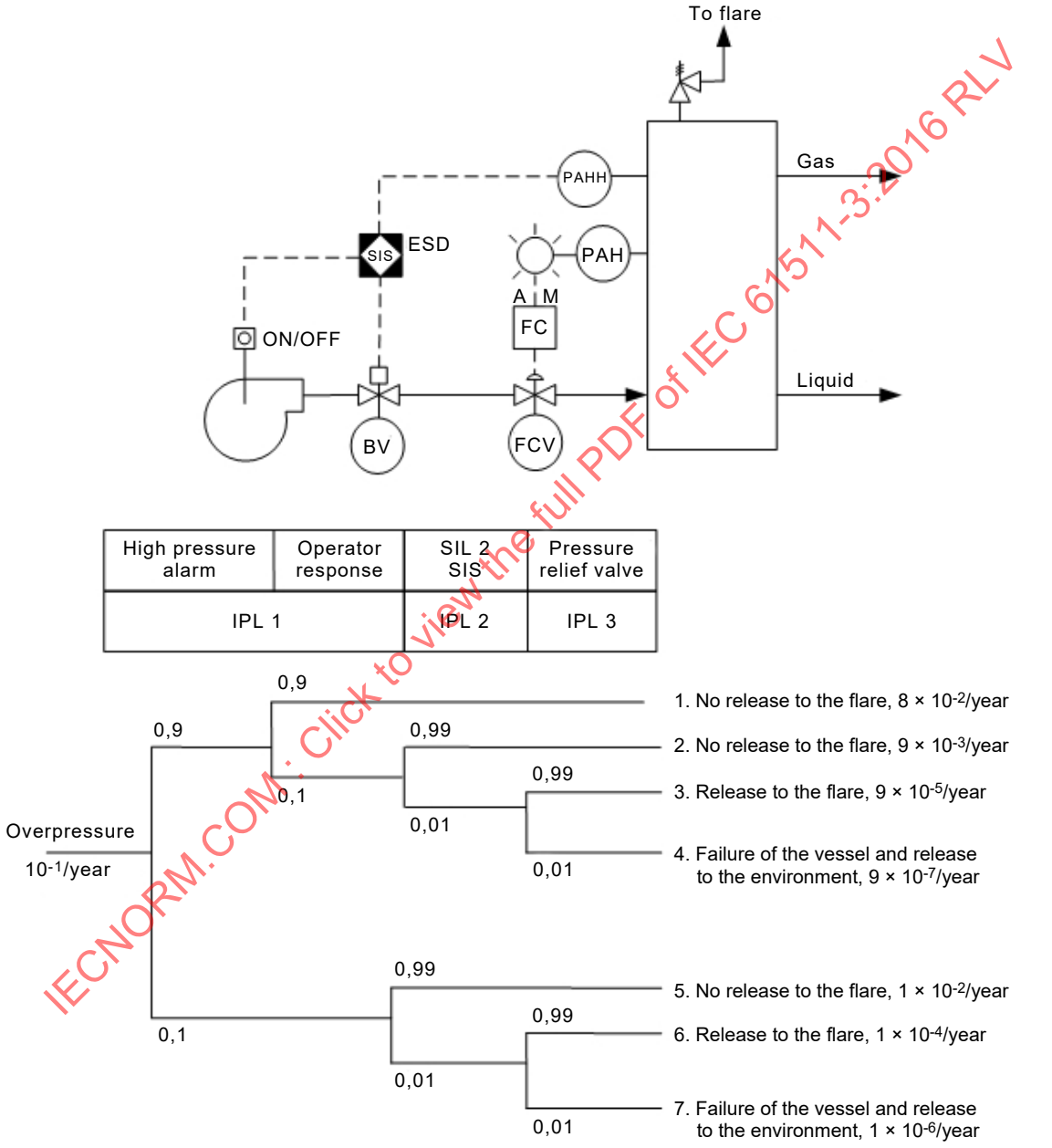
Dans ce cas de conception, l'exploitation réussie du système instrumenté de sécurité (SIS) mène à un arrêt du processus et présente une fréquence d'occurrence de $1{,}9 \times 10^{-2}$ par an. Le SIS réduit le taux de sollicitation du processus sur la vanne de limitation de la pression. La fréquence du scénario de résultats n° 3, qui implique le dégagement de la PRV (vanne de limitation de la pression) à la torche, est réduite de deux ordres de grandeur par rapport au cas précédent de 9×10^{-5} par an. Le scénario de résultats 4, c'est-à-dire l'événement dangereux avec dégagement de matériau dans l'environnement, présente une fréquence d'occurrence de 9×10^{-7} par an.

Le scénario de résultats n° 5 se traduit par une absence de dégagement en raison de l'arrêt du processus par le système instrumenté de sécurité (SIS) et présente une fréquence d'occurrence de 1×10^{-2} par an. En cas de défaillance du SIS, la vanne de limitation de la pression assure la prochaine fonction de sécurité (comme l'explique le scénario de résultats n° 6) et s'ouvre pour donner accès à la torche. La fréquence d'ouverture de la vanne de limitation de la pression est de 1×10^{-4} par an. La fréquence totale des dégagements dans la torche est déterminée par les scénarios 3 et 6. Leur fréquence globale d'occurrence est de $9 \times 10^{-5} + 1 \times 10^{-4}$ ou $1{,}9 \times 10^{-4}$. Les dégagements provenant de la torche sont une condition de conception acceptable pour le processus. Le scénario de résultats n° 7 traite de la défaillance de l'ensemble des fonctions de sécurité et présente une fréquence d'occurrence de 1×10^{-6} par an.

La fréquence totale de défaillance du récipient avec dégagement dans l'environnement (somme des fréquences des scénarios 4 et 7) a été réduite à $1{,}9 \times 10^{-6}$ par an, ce qui est inférieur à la sécurité cible du processus de 10^{-4} par an.

Il convient de noter que cette analyse par arbre d'événement ne tient pas compte de la possibilité de défaillance de cause commune et des dépendances holistiques entre l'alarme de pression élevée et la SIF de SIL 2. Il peut également exister une éventuelle défaillance de cause commune et des dépendances holistiques entre les fonctions de sécurité et la défaillance du capteur de débit du BPCS.

De telles défaillances de cause commune peuvent entraîner une augmentation significative de la probabilité de défaillance en cas de sollicitation des fonctions de protection et donc une augmentation substantielle du risque global.



NOTE Results rounded to the first significant digit

IEC

Anglais	Français
To flare	Vers la torche
Gas	Gaz
Liquid	Liquide
High pressure alarm	Alarme de pression élevée
Operator response	Réponse de l'opérateur
SIL 2 SIS	SIS de SIL 2
Pressure relief valve	Vanne de limitation de la pression
Overpressure	Surpression
No release to the flare	Pas de dégagement vers la torche
8×10^{-2}/year	8×10^{-2}/an
Release to the flare	Dégagement vers la torche
9×10^{-3}/year	9×10^{-3}/an
9×10^{-5}/year	9×10^{-5}/an
Failure of the vessel and release to the environment	Défaillance du récipient et dégagement dans l'environnement
9×10^{-7}/year	9×10^{-7}/an
1×10^{-2}/year	1×10^{-2}/an
1×10^{-4}/year	1×10^{-4}/an
NOTE	NOTE
Results rounded to the first significant digit	Résultats arrondis au premier chiffre significatif

Figure B.4 – Evénements dangereux avec fonction instrumentée de sécurité de SIL 2

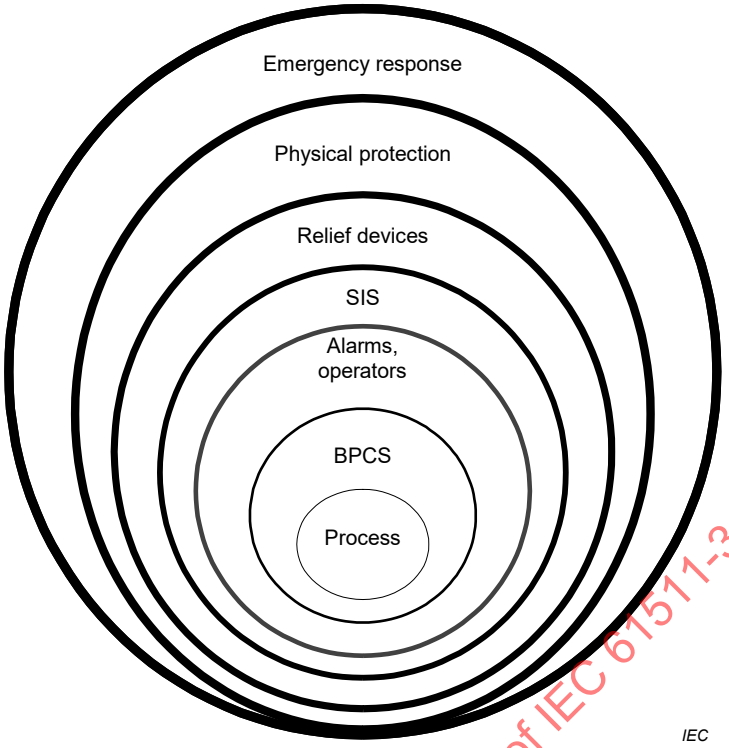
Annexe C
(informative)

Méthode de la matrice de couches de sécurité

C.1 Présentation

Dans chaque processus, il convient que la réduction de risque commence par les éléments les plus essentiels de la conception du processus: la sélection du processus lui-même, le choix du site et les décisions relatives aux stocks dangereux et à l'implantation de l'installation. La détention de stocks minimaux de produits chimiques dangereux, l'installation de canalisations et de systèmes échangeurs thermiques qui empêchent physiquement le mélange accidentel de produits chimiques réactifs, le choix de récipients à parois épaisses pouvant résister aux pressions maximales possibles du processus et le choix d'un fluide chauffant ayant une température maximale inférieure aux températures de décomposition des produits chimiques du processus constituent des décisions de conception du processus destinées à réduire les risques opérationnels. Le fait d'accorder une attention toute particulière à la réduction de risque en sélectionnant soigneusement les paramètres de conception et d'exploitation du processus constitue une étape clé dans la conception d'un processus de sécurité. Il est également recommandé de rechercher des moyens d'éliminer les dangers et d'appliquer des méthodes de conception à sécurité intrinsèque lors de la phase de développement du processus. Malheureusement, même si cette philosophie de conception a été mise en application dans son intégralité, des dangers peuvent demeurer et il convient d'appliquer des mesures de protection supplémentaires.

Dans le secteur des industries de transformation, plusieurs couches de protection sont utilisées pour assurer la protection d'un processus (voir Figure C.1). A la Figure C.1 ci-dessous, chaque couche de protection est composée d'équipements et/ou de commandes administratives qui fonctionnent de concert avec d'autres couches de protection pour contrôler ou atténuer le risque de processus.



Anglais	Français
Emergency response	Réponse d'urgence
Physical protection	Protection physique
Relief devices	Appareils de limitation
SIS	SIS
Alarms, operators	Alarmes, opérateurs
BPCS	BPCS
Process	Processus

Figure C.1 – Couches de protection

Le concept de couches de protection repose sur trois concepts de base:

a) Une couche de protection est composée d'un ensemble d'équipements et/ou de commandes administratives qui fonctionnent de concert avec d'autres couches de protection pour contrôler ou atténuer le risque de processus.

b) Une couche de protection satisfait aux critères suivants:
   – Elle réduit le risque identifié d'un facteur au moins égal à 10;
   – Elle présente les caractéristiques importantes suivantes:
     - Spécificité – Une couche de protection est conçue pour empêcher ou atténuer les conséquences d'un événement potentiellement dangereux. De nombreuses causes peuvent conduire au même événement dangereux et de nombreux scénarios d'événements peuvent donc initier une action de la part d'une couche de protection.
     - Indépendance – Une couche de protection est indépendante des autres couches de protection s'il peut être démontré qu'il n'existe aucun risque de défaillance de cause commune ni de défaillance de mode commun avec d'autres couches de protection revendiquées.
     - Sûreté de fonctionnement – Il peut être considéré avec certitude que la couche de protection remplit sa fonction prévue et traite aussi bien les défaillances aléatoires

que les défaillances systématiques que ce qui a été prévu au stade de sa conception.

- Aptitude aux contrôles – Une couche de protection est conçue pour faciliter la validation régulière des fonctions de protection.

c) La couche de protection d'un système instrumenté de sécurité (SIS) est une couche de protection qui satisfait à la définition d'un SIS au titre de l'Annexe C (le terme "SIS" était utilisé au moment de l'élaboration de la matrice de couches de sécurité).

Références:

– *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 (disponible en anglais seulement);

– *Layer of Protection Analysis-Simplified – Process risk assessment,* American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7 (disponible en anglais seulement);

– CCPS/AIChE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, Wiley-Interscience, New York (2007) (disponible en anglais seulement);

– ISA 84.91.01: *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industries*, The Instrumentation, Society of Automation, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA (disponible en anglais seulement);

– *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 (disponible en anglais seulement);

– FM Global Property Loss Prevention Data Sheet 7-45, "*Instrumentation and Control in Safety Applications*", 1998, FM Global, Johnston, RI, USA (disponible en anglais seulement).

C.2 Cible de sécurité du processus

Pour garantir la bonne gestion du risque industriel, une exigence fondamentale consiste à définir de façon claire et concise la sécurité cible du processus (ou risque tolérable) souhaitée qui peut être définie par l'utilisation de réglementations et de normes nationales et internationales, de politiques d'entreprise et la prise en considération des opinions des parties concernées telles que le public, la juridiction locale et les compagnies d'assurance, l'ensemble étant soutenu par la mise en œuvre de bonnes pratiques techniques. La sécurité cible du processus est propre à un processus, une société ou une industrie. Il convient donc de ne pas généraliser sans que des réglementations et des normes justifient de telles généralisations.

C.3 Analyse de danger

Il convient d'effectuer une analyse de danger destinée à identifier les dangers, les écarts potentiels du processus et leurs causes, les systèmes d'ingénierie disponibles, les événements initiateurs ainsi que les événements dangereux potentiels pouvant se produire. Pour cela, plusieurs techniques qualitatives peuvent être utilisées:

– revues de sécurité;

– listes de contrôle;

– analyse prédictive par simulation;

– étude HAZOP;

– analyse des modes de défaillance et de leurs effets;

– l'analyse cause-conséquence.

L'analyse HAZOP (HAZard and OPerability) est une technique qui est largement employée. L'analyse (ou l'étude) HAZOP permet d'identifier et d'évaluer les dangers dans une installation de processus, ainsi que les problèmes d'opérabilité non dangereux qui compromettent son aptitude à atteindre la productivité de conception.

L'analyse HAZOP est détaillée dans des normes telles que l'IEC 61882:2001. Elle exige une connaissance approfondie et une compréhension exhaustive de la conception, du fonctionnement et de la maintenance d'un processus. En général, un chef d'équipe expérimenté guide systématiquement l'équipe d'analyse pendant toute la phase de conception du processus en utilisant un ensemble approprié de mots-guides. Les mots-guides sont appliqués à des points ou à des étapes d'étude spécifiques du processus et sont associés à des paramètres spécifiques du processus dans le but d'identifier les écarts potentiels par rapport à l'exploitation prévue. Des listes de contrôle ou une expérience du processus sont également utilisées pour aider l'équipe à établir la liste nécessaire des écarts à prendre en compte lors de l'analyse. L'équipe s'entend sur les causes possibles des écarts de processus, sur les conséquences de ces écarts, ainsi que sur les systèmes de procédure et d'ingénierie exigés. Si les causes et les conséquences sont significatives et que les protections sont inadéquates, l'équipe peut recommander des mesures de sécurité supplémentaires ou des actions de suivi pour la prise en considération de la gestion.

Il arrive souvent que les données expérimentales et les résultats d'études HAZOP propres à un processus particulier puissent être généralisés de manière à pouvoir être appliqués à des processus similaires dans une société. Si une telle généralisation peut être faite, le déploiement de la méthode de la matrice de couches de sécurité avec des ressources limitées est faisable.

C.4 Technique d'analyse de risque

Une fois l'étude HAZOP effectuée, le risque associé à un processus peut être évalué en utilisant des techniques qualitatives ou quantitatives. Ces techniques reposent sur les compétences du personnel de l'installation et d'autres spécialistes en analyse de danger et de risque à identifier des événements dangereux potentiels et à en évaluer la probabilité d'occurrence, les conséquences et l'impact.

Une approche qualitative peut être utilisée pour évaluer le risque de processus. Une telle approche permet de définir un cheminement traçable de la manière dont l'événement dangereux se développe, ainsi que l'estimation de la probabilité (plage d'occurrence approximative) et de la gravité.

Le Tableau C.1 donne les lignes directrices types pour estimer la probabilité d'occurrence des événements dangereux sans tenir compte de l'impact des couches de protection existantes. Les données contenues dans ce tableau sont génériques et peuvent être utilisées si aucune donnée spécifique à l'installation ou au processus n'est disponible. Toutefois, si des données propres à une société sont disponibles, il convient de les utiliser pour établir la probabilité d'occurrence des événements dangereux.

De la même manière, le Tableau C.2 montre un moyen permettant de convertir la gravité de l'impact d'un événement dangereux en degrés de gravité en vue d'une évaluation relative. Là encore, ces classes sont données en guise de lignes directrices. La gravité de l'impact des événements dangereux et leur classement sont établis en se fondant sur les compétences et l'expérience propres à l'installation.

Tableau C.1 – Probabilité d'occurrence des événements dangereux (sans tenir compte des couches de protection)

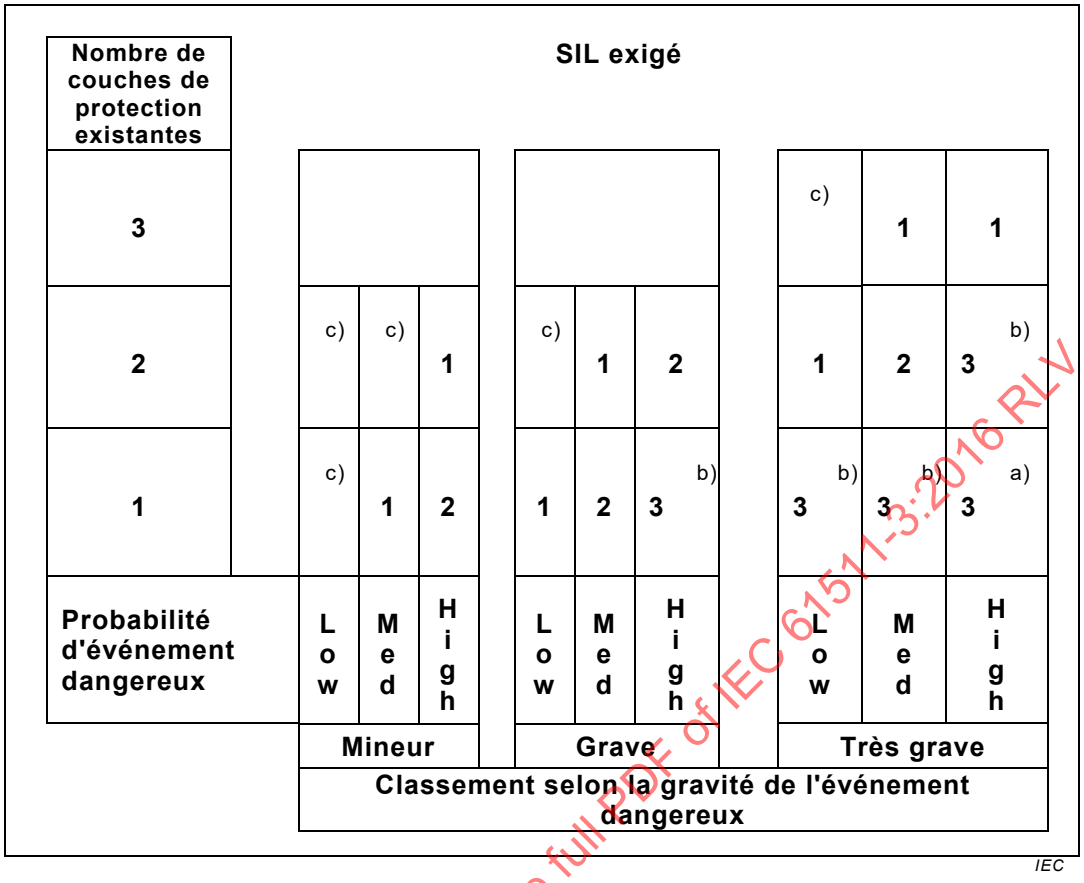
Type d'événements	Probabilité d'occurrence
	Classement qualitatif
Des événements tels que des défaillances multiples de divers instruments ou vannes, des erreurs humaines multiples dans un environnement sans contrainte ou des défaillances spontanées de récipients du processus.	Faible
Des événements tels que des défaillances simultanées d'instruments et de vannes ou des dégagements/importants dans des zones de chargement/déchargement.	Moyenne
Des événements tels que des fuites dans des circuits du processus, des défaillances d'instruments/de vannes ou des erreurs humaines qui entraînent de faibles dégagements de matériaux dangereux.	Elevée
NOTE Le système peut être conforme à l'IEC 61511-1:2016 lorsqu'une revendication est formulée selon laquelle la fréquence de défaillance d'une fonction de commande est inférieure à 10^{-1}.	

Tableau C.2 – Critères de classement de la gravité de l'impact des événements dangereux

Classement selon la gravité	Impact
Très grave	Endommagement à grande échelle des équipements. Arrêt d'un processus pour une période prolongée. Conséquence catastrophique pour le personnel et pour l'environnement.
Grave	Endommagement des équipements. Arrêt de courte durée du processus. Atteintes graves au personnel et à l'environnement.
Mineur	Endommagement mineur des équipements. Pas d'arrêt du processus. Lésions temporaires infligées au personnel et atteinte à l'environnement.

C.5 Matrice de couches de sécurité

Une matrice de risque peut être utilisée pour évaluer le risque en combinant la probabilité d'occurrence et le classement selon la gravité de l'impact des événements dangereux. Une approche similaire peut être utilisée pour développer une matrice, qui identifie la réduction de risque potentielle pouvant être associée à l'utilisation d'une couche de protection du SIS. Une telle matrice de risque est donnée à la Figure C.2. Dans la Figure C.2, la sécurité cible du processus a été intégrée à la matrice. En d'autres termes, la matrice repose sur l'expérience en exploitation et sur les critères de risque propres à la société, sur la philosophie de conception, d'exploitation et de protection de la société, ainsi que sur le niveau de sécurité que la société a défini comme sécurité cible du processus.



Anglais	Français
Low	Faible
Med	Moyenne
High	Elevée

a) A ce niveau de risque, une fonction instrumentée de sécurité (SIF) de SIL 3 ne garantit pas une réduction de risque suffisante. Des modifications supplémentaires sont exigées pour réduire le risque.

b) A ce niveau de risque, une SIF de SIL 3 peut ne pas assurer une réduction de risque suffisante. Une revue supplémentaire est exigée.

c) La couche de protection du SIS n'est probablement pas nécessaire.

NOTE 1 Nombre total de couches de protection – inclut toutes les couches de protection assurant la protection du processus, y compris le SIS en cours de classification (c'est-à-dire le nombre de couches de protection après analyse, y compris la nouvelle SIF (si exigée)).

NOTE 2 Probabilité d'occurrence des événements dangereux – probabilité que l'événement dangereux se produise alors qu'aucune des couches de protection n'est en service. Pour des lignes directrices, se reporter au Tableau C.1.

NOTE 3 Gravité d'un événement dangereux – impact associé à l'événement dangereux. Pour des lignes directrices, se reporter au Tableau C.2.

NOTE 4 Cette approche est considérée comme ne convenant pas pour le SIL 4.

Figure C.2 – Exemple de matrice de couches de sécurité

C.6 Procédure générale

a) Etablir la sécurité cible du processus.

b) Procéder à une identification du danger (étude HAZOP, par exemple) pour identifier tous les événements dangereux présentant un intérêt.

c) Etablir les scénarios d'événements dangereux et estimer la probabilité d'événement dangereux en utilisant les lignes directrices et les données propres à la société.

d) Etablir le classement selon la gravité des événements dangereux en utilisant les lignes directrices propres à la société.

e) Identifier les couches de protection existantes (Figure C.2). Il convient de réduire la probabilité estimée d'occurrence d'événements dangereux par un facteur de 10 pour chaque couche de protection.

f) Identifier la nécessité d'une couche de protection du SIS supplémentaire en comparant le risque restant à la sécurité cible du processus.

g) Identifier le SIL à l'aide de la Figure C.2.

h) Il convient que l'utilisateur se conforme à l'Article C.1 b).

Annexe D
(informative)

Méthode semi-qualitative: graphe de risque étalonné

D.1 Présentation

L'Annexe D s'appuie sur le schéma général de mise en œuvre du graphe de risque décrit à l'Article E.1 de l'IEC 61508-5:2010. L'Annexe D a été adaptée pour mieux répondre aux besoins de l'industrie de transformation.

Elle décrit la méthode du graphe de risque étalonné utilisée pour déterminer les niveaux d'intégrité de sécurité (SIL) des fonctions instrumentées de sécurité (SIF). Il s'agit d'une méthode semi-qualitative qui permet de déterminer le niveau d'intégrité de sécurité (SIL) d'une fonction instrumentée de sécurité (SIF) à partir du moment où les facteurs de risque associés au processus et au système de commande de processus de base (BPCS) sont connus.

L'approche utilise un certain nombre de paramètres, qui décrivent ensemble la nature de la situation dangereuse en cas de défaillance ou d'indisponibilité d'un système instrumenté de sécurité (SIS). Un paramètre est choisi dans chacun des quatre ensembles, puis les paramètres sélectionnés sont combinés pour choisir le SIL affecté à la SIF. Ces paramètres:

– permettent une évaluation nuancée des risques; et
– représentent les facteurs clés de l'évaluation du risque.

L'approche du graphe de risque peut également être utilisée pour déterminer la nécessité d'une réduction de risque lorsque les conséquences incluent une dégradation importante de l'environnement ou une perte de biens. L'Annexe D a pour objet de donner des lignes directrices concernant les problèmes ci-dessus.

L'Annexe D commence par la protection contre les dangers menaçant le personnel. Elle permet d'envisager l'application du graphe de risque général donné à la Figure E.1 de l'IEC 61508-5:2010 aux industries de transformation. Enfin, elle indique les applications du graphe de risque à la protection de l'environnement et à la protection des biens.

D.2 Synthèse du graphe de risque

Un risque est défini comme une combinaison de la probabilité d'occurrence d'un dommage et de la gravité du dommage en question (voir l'Article 3 de l'IEC 61511-1:2016). Habituellement, dans le secteur des industries de transformation, le risque dépend des quatre paramètres suivants:

– la conséquence de l'événement dangereux (C);
– l'occupation (probabilité que la zone exposée soit occupée) (F);
– la probabilité que la situation dangereuse soit évitée (P);
– le taux de sollicitation (nombre de fois par an où la situation dangereuse se produirait en l'absence de la SIF à l'étude) (W).

Lorsqu'un graphe de risque est utilisé pour déterminer le niveau d'intégrité de sécurité (SIL) d'une fonction de sécurité opérant en mode continu, la modification des paramètres utilisés dans le graphe de risque devra être envisagée. Il convient que les paramètres (voir Tableau D.1) représentent les facteurs de risque qui se rapportent le mieux aux caractéristiques de l'application concernée. Le mapping des SIL par rapport aux résultats des décisions relatives aux paramètres devra également être envisagé, car un certain ajustement

peut se révéler nécessaire pour garantir la réduction de risque à des niveaux tolérables. A titre d'exemple, le paramètre W peut être redéfini comme le pourcentage de vie du système durant lequel le système est en service. De ce fait, le paramètre W1 serait sélectionné lorsque le danger n'est pas présent en permanence et que la période par année durant laquelle une défaillance engendrerait un danger est courte. Dans cet exemple, les autres paramètres devraient également être envisagés en ce qui concerne les critères de décision concernés et les résultats relatifs aux niveaux d'intégrité passés en revue pour garantir un risque tolérable.

Tableau D.1 – Descriptions des paramètres du graphe de risque pour les industries de transformation

Paramètre		Description
Conséquence	C	Nombre d'accidents mortels et/ou de lésions graves susceptibles de se produire suite à l'occurrence de l'événement dangereux. Ce paramètre est déterminé en calculant les nombres dans la zone exposée lorsque la zone est occupée en tenant compte de la vulnérabilité à l'événement dangereux.
Occupation	F	Probabilité que la zone exposée soit occupée au moment où l'événement dangereux se produit. Ce paramètre est déterminé en calculant la fraction de temps durant laquelle la zone est occupée au moment où se produit l'événement dangereux. Cela peut tenir compte de la possibilité d'avoir une augmentation de la probabilité que des personnes soient présentes dans la zone exposée, afin de déterminer les situations anormales qui peuvent exister au moment de l'apparition de l'événement dangereux (vérifier aussi si cela modifie le paramètre C).
Probabilité que le danger soit évité	P	Probabilité que des personnes exposées puissent éviter la situation dangereuse qui existe en cas de défaillance de la fonction instrumentée de sécurité (SIF) sur sollicitation. Cela dépend de la présence de méthodes indépendantes utilisées pour avertir les personnes exposées au danger avant que le danger ne se produise, ainsi que de la présence de méthodes d'évacuation.
Taux de sollicitation	W	Nombre de fois par an où l'événement dangereux se produirait en l'absence de la SIF à l'étude. Ce paramètre peut être déterminé en tenant compte de toutes les défaillances pouvant provoquer l'événement dangereux et en évaluant le taux global d'occurrence. Il convient d'inclure d'autres couches de protection à l'étude.

D.3 Etalonnage

Les objectifs de la procédure d'étalonnage sont les suivants:

a) Décrire tous les paramètres de manière à permettre à l'équipe chargée d'évaluer le SIL de porter des jugements objectifs fondés sur les caractéristiques de l'application.

b) Garantir que le SIL choisi pour une application satisfait aux critères de risque définis par la société et tient compte des risques provenant d'autres sources.

c) Permettre de vérifier le processus de sélection des paramètres.

L'étalonnage du graphe de risque est le processus qui consiste à attribuer des valeurs numériques aux paramètres du graphe de risque. Cela constitue la base pour l'évaluation du risque de processus qui existe et permet de déterminer l'intégrité exigée de la SIF à l'étude. A chacun des paramètres est attribuée une plage de valeurs de sorte que, lorsque ces paramètres sont combinés, ils permettent d'effectuer une évaluation nuancée du risque qui existe en l'absence de la fonction de sécurité. De ce fait, une mesure du degré de confiance à attribuer à la SIF est déterminée. Le graphe de risque se rapporte à des combinaisons particulières de paramètres de risque et de niveaux d'intégrité de sécurité (SIL). La relation entre les combinaisons de paramètres de risque et de niveaux d'intégrité de sécurité (SIL) est établie en prenant en considération le risque tolérable associé à des dangers spécifiques. Pour une description du processus d'étalonnage, se reporter à l'Annexe I (Paragraphes I.2 et I.4.7).

Lorsque le sujet de l'étalonnage des graphes de risque est abordé, il est important de tenir compte des exigences en matière de risques provenant des attentes des exploitants et des

exigences des autorités compétentes. Les risques pour la vie peuvent être considérés dans les deux en-têtes suivants:

– Risque pour les individus – défini comme le risque par année pour l'individu le plus exposé. Il s'agit normalement de la valeur maximale qui peut être tolérée. La valeur maximale provient normalement de toutes les sources de danger.
– Risque sociétal – défini comme le risque total par année encouru par un groupe d'individus exposés. L'exigence est normalement la réduction de risque sociétal jusqu'à au moins une valeur maximale qui peut être tolérée par la société et jusqu'à ce qu'une autre réduction de risque soit disproportionnée par rapport aux coûts relatifs à une telle réduction de risque.

Si le risque pour les individus doit être réduit jusqu'à une valeur maximale spécifiée, il ne peut alors pas être retenu pour hypothèse que l'ensemble de cette réduction de risque puisse être affecté à un seul système instrumenté de sécurité (SIS). Les personnes exposées sont soumises à une grande plage de risques issus d'autres sources (par exemple: risques de chute, d'incendie et d'explosion).

Lorsqu'elle étudie l'étendue de la réduction de risque exigée, une organisation peut avoir des critères concernant le coût différentiel pour la prévention des accidents mortels. Ce coût différentiel peut être calculé en divisant le coût annualisé relatif au matériel supplémentaire et à l'ingénierie associée à un niveau d'intégrité supérieur par la réduction de risque différentielle. Un niveau d'intégrité supplémentaire est justifié si le coût différentiel pour la prévention d'un accident mortel est inférieur à un montant prédéterminé.

Un critère largement utilisé applicable au risque sociétal est fondé sur la probabilité, *F*, que *N* accidents mortels ou plus se produisent. Les critères de risque sociétal acceptable se présentent sous la forme d'une ligne ou d'un ensemble de lignes sur un graphe bilogarithmique représentant le nombre d'accidents mortels en fonction de la fréquence des accidents. Pour vérifier que les lignes directrices relatives au risque sociétal n'ont pas été enfreintes, la courbe de la fréquence cumulée est tracée en fonction des conséquences des accidents pour tous les accidents (c'est-à-dire la courbe *F-N*), en garantissant que la courbe *F-N* ne coupe pas la courbe de risque tolérable. Les lignes directrices relatives à l'élaboration de critères de risque entraînant des problèmes sociétaux sont données dans la publication "*Reducing Risks, Protecting People*", HSE, Royaume-Uni, ISBN 0 7176 2151 0 (disponible en anglais seulement).

Les quatre paramètres de risque auxquels l'Article D.2 fait référence font partie d'un arbre de décision dont la forme est représentée à la Figure D.1. Les points susmentionnés doivent être étudiés avant de pouvoir spécifier les valeurs de chacun des paramètres. Une plage est affectée à la plupart des paramètres (par exemple, si le taux de sollicitation attendu d'un processus particulier se trouve dans les limites d'une plage de décade de sollicitations spécifique par an, le paramètre W3 peut être utilisé). De la même manière, le paramètre W2 s'appliquerait pour des sollicitations dans la plage de décade inférieure et le paramètre W1 s'applique pour des sollicitations dans la plage de décade inférieure suivante. Le fait d'affecter une plage spécifique à chaque paramètre aide l'équipe à prendre des décisions sur la valeur du paramètre à sélectionner pour une application spécifique. Pour étalonner le graphe de risque, des valeurs ou des plages de valeurs sont attribuées à chaque paramètre. Le risque associé à chacune des combinaisons de paramètres est alors évalué en termes individuels et sociétaux. La réduction de risque exigée pour satisfaire au critère de risque déterminé (risque tolérable ou moins) peut alors être établie. Grâce à cette méthode, les niveaux d'intégrité de sécurité (SIL) associés à chaque combinaison de paramètres peuvent être déterminés. Cette procédure d'étalonnage ne doit pas être effectuée chaque fois que le niveau d'intégrité de sécurité (SIL) d'une application spécifique doit être déterminé. Normalement, cette procédure d'étalonnage est uniquement nécessaire pour permettre aux organisations d'exécuter le travail une seule fois pour des dangers similaires. Un ajustement peut être nécessaire pour des projets spécifiques si les hypothèses initiales énoncées au cours de l'étalonnage s'avèrent invalides pour tout autre projet spécifique.

Lorsque les allocations des paramètres sont effectuées, il convient que des informations soient disponibles pour indiquer la manière dont les valeurs ont été déduites.

Il est important que cette procédure d'étalonnage soit validée à un niveau hiérarchique élevé au sein de l'organisation chargée de la sécurité. Les décisions prises déterminent la sécurité globale obtenue.

En général, il sera difficile à partir d'un graphe de risque de considérer le fait qu'il puisse avoir une défaillance dépendante entre les sources de sollicitation et le système instrumenté de sécurité (SIS). Cela peut donc conduire à une surestimation de l'efficacité du SIS.

D.4 Composition et organisation de l'équipe chargée d'évaluer le niveau d'intégrité de sécurité (SIL)

Il est improbable qu'une seule personne réunisse toutes les compétences et l'expérience nécessaires pour prendre des décisions à propos des paramètres concernés. Cette tâche est normalement confiée à une équipe constituée dans le but spécifique de déterminer les niveaux d'intégrité de sécurité (SIL). L'équipe sera probablement composée des membres suivants:

– un spécialiste du processus;
– un ingénieur spécialisé dans la commande de processus;
– un gestionnaire des opérations;
– un spécialiste de la sécurité;
– un opérateur expérimenté ayant déjà exploité le processus à l'étude.

Habituellement, l'équipe traite chaque fonction instrumentée de sécurité (SIF) à tour de rôle. L'équipe aura besoin d'informations complètes sur le processus et sur le nombre probable de personnes exposées au risque. Il convient que l'équipe compte un opérateur expérimenté ayant déjà utilisé la méthode du graphe de risque et qui comprenne les concepts de base sur lesquels repose la méthode. Il convient que le responsable s'assure que chaque membre se sent libre d'exprimer ses interrogations et son point de vue.

D.5 Documents relatifs aux résultats de la détermination du niveau d'intégrité de sécurité (SIL)

Il est important que toutes les décisions prises lors de la détermination du SIL soient consignées dans des documents soumis à la gestion de configuration. Il convient que la documentation indique clairement les raisons pour lesquelles l'équipe a sélectionné les paramètres spécifiques associés à une fonction de sécurité. Il convient de regrouper dans un même dossier les formulaires utilisés pour enregistrer les résultats de la détermination du SIL de chaque fonction de sécurité, ainsi que les hypothèses de départ. S'il est établi que plusieurs systèmes exécutent des fonctions de sécurité dans une zone desservie par une seule équipe d'exploitation, il peut alors être nécessaire de passer en revue la validité des hypothèses d'étalonnage. Il convient que le dossier contienne également les informations supplémentaires suivantes:

– le graphe de risque utilisé avec les descriptions de toutes les plages de paramètres;
– le numéro du dessin et le numéro de révision de tous les documents utilisés;
– les références aux hypothèses relatives aux effectifs et aux éventuelles études de conséquences qui ont été utilisées pour évaluer les paramètres;
– les références aux défaillances qui conduisent à des sollicitations et à d'éventuels modèles de propagation des défaillances quand ils ont été utilisés pour déterminer les taux de sollicitation;
– les références aux sources de données utilisées pour déterminer les taux de sollicitation.

D.6 Exemple d'étalonnage fondé sur des critères types

Le Tableau D.2, qui fournit des descriptions et des plages de paramètres pour chaque paramètre, a été élaboré dans le but de satisfaire à des critères spécifiques types pour les processus chimiques tels que décrits précédemment. Avant d'utiliser cette méthode dans le cadre d'un projet, il est important de confirmer qu'elle satisfait aux besoins des responsables de la sécurité.

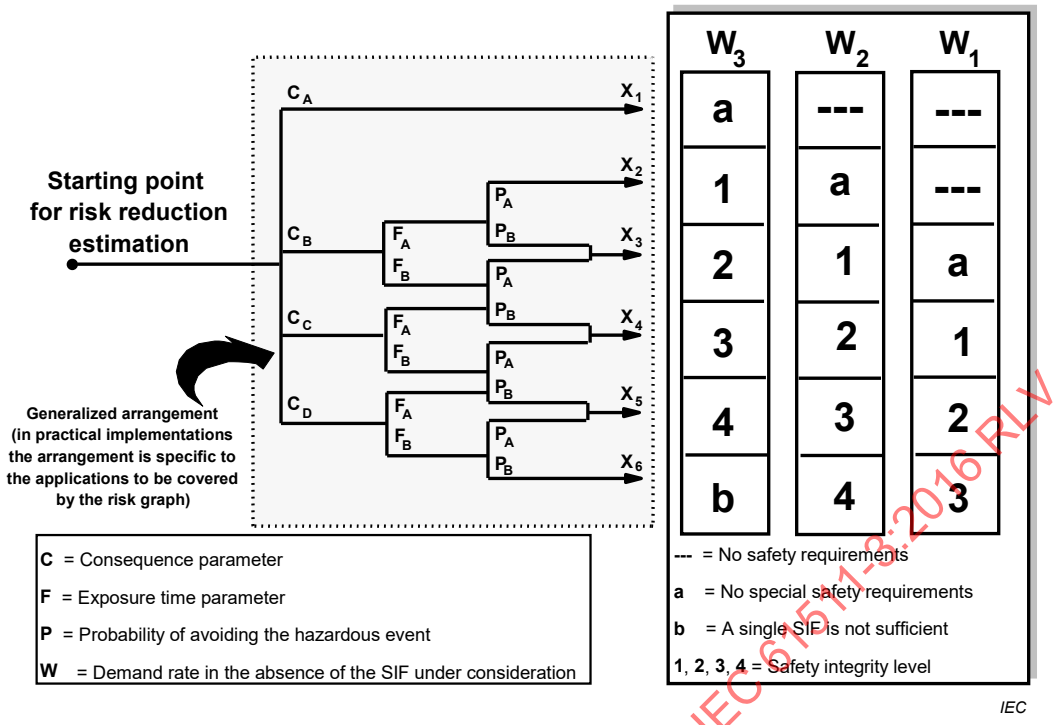
Le concept de vulnérabilité a été introduit dans le but de modifier le paramètre de conséquence. En effet, dans de nombreux cas, une défaillance ne provoque pas un accident mortel immédiat. La vulnérabilité d'un récepteur constitue un point important à prendre en considération dans l'analyse de risque parce que la dose reçue par un sujet ne suffit parfois pas à provoquer le décès. La vulnérabilité d'un récepteur à une conséquence est une fonction de la concentration du danger auquel il a été exposé, ainsi que de la durée de l'exposition. A titre d'exemple, il est pris pour hypothèse qu'une défaillance provoque une surpression supérieure à la pression de calcul d'un appareil, mais que la surpression n'augmentera pas jusqu'à une valeur supérieure à la pression d'essai de l'équipement. Le résultat probable de cette défaillance se limitera normalement à une fuite à travers des joints d'étanchéité de bride. En pareil cas, le taux de progression est susceptible d'être lent et le personnel d'exploitation pourra normalement éviter les conséquences. Même en cas de fuite importante de matériau liquide, le temps de progression sera suffisamment lent pour qu'il existe une forte probabilité que le personnel d'exploitation puisse être capable d'éviter le danger. Il existe évidemment des cas où une défaillance pourrait provoquer une rupture des canalisations ou des récipients où la vulnérabilité du personnel d'exploitation peut être élevée.

Le nombre croissant de personnes se trouvant à proximité de l'événement dangereux suite à une étude des symptômes apparaissant lors du développement de l'événement sera pris en considération. Il convient d'envisager le cas le plus défavorable.

Il est important de bien comprendre la différence entre la "vulnérabilité" (V) et la "probabilité d'éviter un événement dangereux" (P) afin de ne pas prendre en compte deux fois l'allocation pour le même facteur. La vulnérabilité est une mesure qui se rapporte à la vitesse de progression après l'apparition du danger et à la probabilité d'un accident mortel si l'événement dangereux survient, alors que le paramètre P est une mesure qui se rapporte à la prévention de l'événement dangereux. Il convient d'utiliser le paramètre P_A uniquement si l'opérateur, après avoir pris conscience de la défaillance du SIS, peut entreprendre une action pour éliminer le danger.

Certaines restrictions ont été posées sur la manière dont les paramètres d'occupation sont sélectionnés. L'exigence consiste à sélectionner le facteur d'occupation en se basant sur la personne la plus exposée plutôt que sur une moyenne calculée sur l'ensemble du personnel. Cela permet de s'assurer que la personne la plus exposée n'est pas soumise à un risque élevé, qui est ensuite intégré à la moyenne pour toutes les personnes exposées à ce risque.

Si un paramètre ne tombe pas dans les limites d'une des plages spécifiées, les exigences de réduction de risque doivent être déterminées par d'autres méthodes ou le graphe de risque (Figure D.1) doit être réétalonné via les méthodes décrites ci-dessus.



Anglais	Français
Starting point for risk reduction estimation	Point de départ pour l'estimation de la réduction de risque
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)	Disposition généralisée (dans des mises en œuvre pratiques, la disposition est propre aux applications devant être couvertes par le graphe de risque)
C = Consequence parameter	C = Paramètre de conséquence
F = Exposure time parameter	F = Paramètre du temps d'exposition
P = Probability of avoiding the hazardous event	P = Probabilité d'éviter l'événement dangereux
W = Demand rate in the absence of the SIF under consideration	W = Taux de sollicitation en l'absence de la SIF à l'étude
--- = No safety requirements	--- = Pas d'exigence de sécurité
a = No special safety requirements	a = Pas d'exigence de sécurité spéciale
b = A single SIF is not sufficient	b = Une seule SIF n'est pas suffisante
1, 2, 3, 4 = Safety integrity level	1, 2, 3, 4 = niveau d'intégrité de sécurité

Figure D.1 – Graphe de risque: schéma général

Il convient de ne pas utiliser la Figure D.1 sans nouvel étalonnage pour le faire correspondre avec les critères de risque du site. Il convient qu'un site sans critère de risque approprié ne cherche pas à adopter cette méthode. La façon de procéder pour l'étalonnage dépendra de celle dont les critères de risque tolérable sont exprimés. Il convient d'ajuster les descriptions de paramètres afin qu'elles correspondent avec la plage d'application prévue et avec la tolérance au risque. Les valeurs C, F, P ou W peuvent être modifiées. Le Tableau D.2 est un exemple d'étalonnage où la valeur W est ajustée par un facteur d'étalonnage D pour correspondre aux critères de risque spécifiés.

Tableau D.2 – Exemple d'étalonnage du graphe de risque général

Paramètre de risque		Classification	Commentaires
Conséquence (C) Nombre d'accidents mortels Ce paramètre peut être calculé en déterminant le nombre de personnes présentes lorsque la zone exposée au danger est occupée et en le multipliant par la vulnérabilité au danger identifié. La vulnérabilité est déterminée par la nature du danger contre lequel la protection est assurée. Les facteurs suivants peuvent être utilisés: V = 0,01 Faible dégagement de matériau inflammable ou toxique V = 0,1 Important dégagement de matériau inflammable ou toxique V = 0,5 Comme ci-dessus, mais aussi une haute probabilité d'incendie ou matériau très toxique V = 1 Rupture ou explosion	CA CB CC CD	Lésion mineure Plage de 0,01 à 0,1 Plage de > 0,1 à 1,0 Plage > 1,0	a) Le système de classification a été établi pour traiter les blessures infligées aux personnes ou les décès. b) Pour l'interprétation de CA, CB, CC et CD, il convient de tenir compte des conséquences de l'accident et du rétablissement normal.
Occupation (F) Ce paramètre est calculé en déterminant la durée proportionnelle pendant laquelle la zone exposée au danger est occupée pendant une période normale de travail. NOTE 1 Si le temps passé dans la zone dangereuse est différent selon l'équipe d'exploitation, il convient alors de choisir le temps maximal. NOTE 2 L'utilisation du paramètre FA n'est appropriée que s'il peut être démontré que le taux de sollicitation est aléatoire et qu'il n'est pas lié à la période durant laquelle l'occupation pourrait être supérieure à la normale. Ce dernier cas se retrouve habituellement avec des sollicitations qui se produisent au moment du démarrage des équipements ou pendant la recherche d'anomalies.	FA FB	Exposition rare à plus fréquente dans la zone dangereuse. L'occupation est inférieure à 0,1. Exposition fréquente à permanente dans la zone dangereuse	c) Voir le commentaire a) ci-dessus.
Probabilité que l'événement dangereux soit évité (P) en cas de défaillance du système de protection.	PA PB	Adoptée si toutes les conditions de la colonne 4 sont satisfaites Adoptée si une seule des conditions n'est pas satisfaite	d) Il convient de choisir le paramètre PA uniquement si toutes les conditions suivantes sont vraies: – des moyens sont prévus pour signaler la défaillance du SIS à l'opérateur; – des moyens indépendants sont prévus pour arrêter le processus afin de pouvoir éviter le danger ou de permettre l'évacuation de toutes les personnes vers une zone de sécurité; – il s'écoule plus de 1 h ou un temps tout à fait suffisant entre le moment où l'opérateur est averti et le moment où un événement dangereux se produit pour entreprendre les actions nécessaires.

Paramètre de risque		Classification	Commentaires
Taux de sollicitation (W). Le nombre de fois par an où l'événement dangereux se produirait en l'absence de la SIF à l'étude.	W1	Taux de sollicitation inférieur à 0,1 D par an	e) Le facteur W a pour objet d'estimer la fréquence du danger qui apparaît en l'absence du SIS.
Pour déterminer le taux de sollicitation, toutes les sources de défaillance qui peuvent provoquer un événement dangereux doivent être considérées. Lors de la détermination du taux de sollicitation, une confiance limitée peut être accordée aux performances et à l'intervention du système de commande. Les performances, qui peuvent être revendiquées si le système de commande ne doit pas être conçu et entretenu conformément à l'IEC 61511:-, sont limitées à des valeurs inférieures aux plages de performances associées au SIL1. Le taux de sollicitation (W) est égal au taux de sollicitation relatif à la SIF à l'étude.	W2 W3	Taux de sollicitation entre 0,1 D et D par an Taux de sollicitation entre D et 10 D par an Pour des taux de sollicitation supérieurs à 10 D par an, une intégrité plus élevée doit être exigée.	Si le taux de sollicitation est très élevé, le niveau d'intégrité de sécurité (SIL) doit être déterminé par une autre méthode ou le graphe de risque doit être étalonné une nouvelle fois. Il convient de noter que les méthodes utilisant des graphes de risque peuvent ne pas constituer la meilleure approche dans le cas d'applications fonctionnant en mode continu. Voir 3.2.39.2 de l'IEC 61511-1:2016. f) Il convient de déterminer la valeur du facteur d'étalonnage D afin que le graphe de risque donne un niveau de risque résiduel tolérable, en tenant compte d'autres risques auxquels les personnes exposées sont confrontées et des critères propres à la société. Il convient de déduire les valeurs numériques devant être utilisées par rapport à chaque valeur W dans le tableau par étalonnage du graphe de risque, tel que décrit à l'Article D.3 ou l'Annexe I.
NOTE Il s'agit d'un exemple destiné à présenter l'application des principes pour la conception des graphes de risque. Les graphes de risque relatifs à des applications particulières et à des dangers particuliers peuvent faire l'objet d'un accord entre les parties concernées, en tenant compte du risque tolérable (voir les Articles D.1 à D.6).			

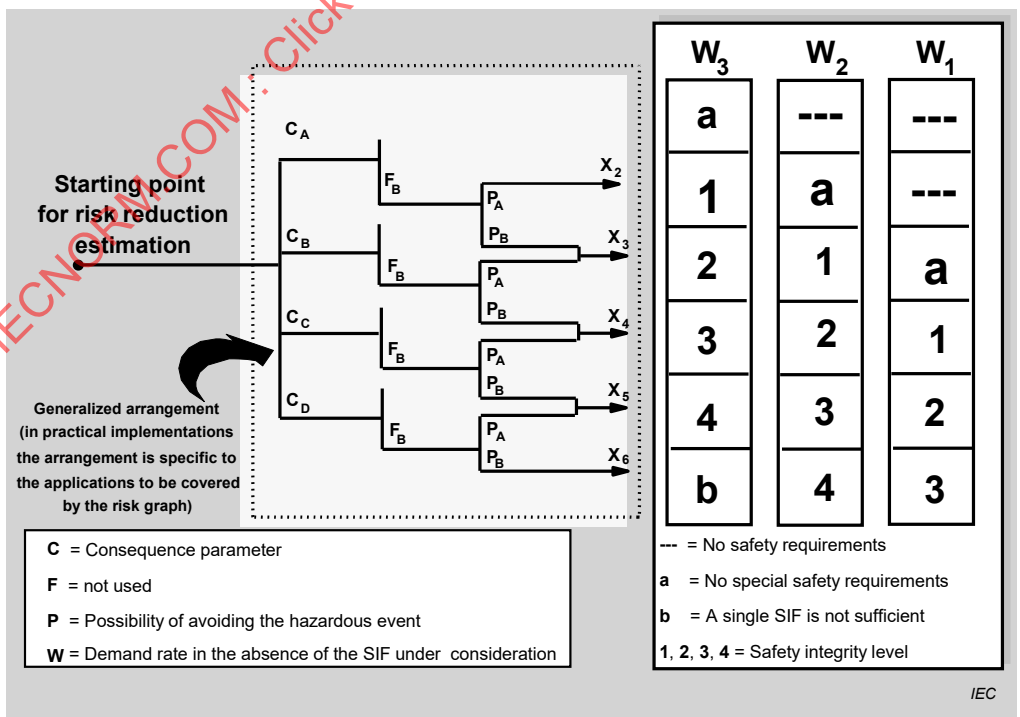
D.7 Utilisation des graphes de risque lorsque les conséquences sont une atteinte à l'environnement

L'approche des graphes de risque peut également être utilisée pour déterminer les exigences relatives au niveau d'intégrité lorsque les conséquences d'une défaillance comprennent une atteinte grave à l'environnement. Le niveau exigé d'intégrité dépend des caractéristiques de la substance dégagée et de la sensibilité de l'environnement. Le Tableau D.3 indique les conséquences en termes d'environnement. Chaque site d'installation de processus individuelle peut avoir une quantité définie associée à des substances spécifiques au-delà desquelles les autorités compétentes locales doivent être alertées. Les projets doivent déterminer ce qui peut être accepté dans un lieu spécifique.

Tableau D.3 – Conséquences générales sur l'environnement

Paramètre de risque		Classification	Commentaires
Conséquence (C)	CA	Un dégagement entraînant un dommage mineur qui n'est pas très grave, mais qui est assez important pour être signalé à la direction de l'installation	Une fuite modérée à travers une bride ou une vanne Déversement de liquide à faible échelle Pollution du sol à faible échelle sans altération de la nappe phréatique
	CB	Dégagement dans les limites du site du processus entraînant un dommage significatif	Un nuage de vapeur malsaine se déplaçant au-delà de l'appareil suite à la rupture d'un joint de bride ou la défaillance d'un joint de compresseur
	CC	Dégagement hors des limites du site du processus entraînant un dommage grave qui peut être nettoyé rapidement sans conséquence significative durable	Un dégagement de vapeur ou de brouillard avec ou sans retombée liquide qui porte temporairement atteinte à la flore ou à la faune
	CD	Dégagement hors des limites de l'installation de processus, avec un dommage important, qui ne peut pas être nettoyé rapidement ou qui a des conséquences durables	Déversement dans une rivière ou dans la mer Un dégagement de vapeur ou de brouillard avec ou sans retombée liquide qui porte temporairement atteinte à la flore ou à la faune Retombées solides (poussières, catalyseurs, suie, cendres) Déversement de liquide qui pourrait affecter la nappe phréatique

Les conséquences mentionnées ci-dessus peuvent être utilisées conjointement avec le modèle spécial de graphe de risque donné à la Figure D.2. Il convient de noter que le paramètre F n'est pas utilisé dans ce graphe de risque, car le concept d'occupation ne s'applique pas. D'autres paramètres P et W s'appliquent, et les définitions peuvent être identiques à celles appliquées ci-dessus aux conséquences sur la sécurité bien que la valeur du facteur d'étalonnage D puisse devoir être modifiée pour correspondre aux critères de risque liés à l'environnement.



Anglais	Français
Starting point for risk reduction estimation	Point de départ pour l'estimation de la réduction de risque
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)	Disposition généralisée (dans des mises en œuvre pratiques, la disposition est propre aux applications devant être couvertes par le graphe de risque)
C = Consequence parameter	C = Paramètre de conséquence
F = not used	F = non utilisé
P = Possibility of avoiding the hazardous event	P = Possibilité d'éviter l'événement dangereux
W = Demand rate in the absence of the SIF under consideration	W = Taux de sollicitation en l'absence de la SIF à l'étude
--- = No safety requirements	--- = Pas d'exigence de sécurité
a = No special safety requirements	a = Pas d'exigence de sécurité spéciale
b = A single SIF is not sufficient	b = Une seule SIF n'est pas suffisante
1, 2, 3, 4 = Safety integrity level	1, 2, 3, 4 = Niveau d'intégrité de sécurité

Figure D.2 – Graphe de risque: atteinte à l'environnement

D.8 Utilisation de graphes de risque quand les conséquences sont une perte de biens

L'approche des graphes de risque peut également être utilisée pour déterminer les exigences relatives au niveau d'intégrité lorsque les conséquences d'une défaillance comprennent une perte de biens. Une perte de biens est la perte économique totale associée à la défaillance du fonctionnement sur sollicitation. Elle inclut les coûts de reconstruction en cas d'endommagement et les coûts relatifs à la perte d'exploitation. Le niveau d'intégrité justifié pour toute conséquence d'une perte peut être calculé en utilisant une analyse coûts-avantages. L'utilisation du graphe de risque pour les pertes de biens présente des avantages si elle sert à déterminer les niveaux d'intégrité associés aux conséquences sur la sécurité et sur l'environnement. Si cette méthode est utilisée pour déterminer le niveau d'intégrité associé aux pertes de biens, les paramètres de conséquence C_A à C_D doivent être définis. Ces paramètres peuvent varier très largement d'une société à l'autre.

Un graphe de risque similaire à celui utilisé pour la protection de l'environnement peut être élaboré pour la perte de biens. Il convient de noter qu'il convienne de ne pas utiliser le paramètre F, car le concept d'occupation ne s'applique pas. D'autres paramètres P et W s'appliquent, et les définitions peuvent être identiques à celles appliquées ci-dessus aux conséquences sur la sécurité bien que la valeur du facteur d'étalonnage D puisse devoir être modifiée pour correspondre aux critères de risque liés au bien.

D.9 Détermination du niveau d'intégrité d'une fonction instrumentée de sécurité lorsque les conséquences d'une défaillance impliquent plusieurs types de pertes

Dans de nombreux cas, les conséquences d'une défaillance de fonctionnement sur sollicitation impliquent plus d'une catégorie de pertes. Lorsque ce cas se présente, il convient de déterminer séparément les exigences de niveau d'intégrité associées à chaque catégorie de pertes. Différentes méthodes peuvent être utilisées pour chacun des risques distincts identifiés. Il convient que le niveau d'intégrité spécifié pour la fonction tienne compte du total cumulé de tous les risques concernés en cas de défaillance de la fonction sur sollicitation.

Annexe E
(informative)

Méthode qualitative: graphe de risque

E.1 Généralités

L'Annexe E décrit la méthode du graphe de risque utilisée pour déterminer les niveaux d'intégrité de sécurité (SIL) des fonctions instrumentées de sécurité (SIF). Il s'agit d'une méthode qualitative qui permet de déterminer le SIL d'une SIF à partir du moment où les facteurs de risque associés au processus et au système de commande de processus de base (BPCS) sont connus.

L'approche utilise un certain nombre de paramètres, qui décrivent ensemble la nature de la situation dangereuse en cas de défaillance ou d'indisponibilité d'un ou de plusieurs SIS. Un paramètre est choisi dans chacun des quatre ensembles, puis les paramètres sélectionnés sont combinés pour choisir le SIL affecté à la SIF. Ces paramètres:

– permettent une évaluation nuancée des risques; et
– représentent les facteurs clés de l'évaluation du risque.

L'approche du graphe de risque peut également être utilisée pour déterminer la nécessité d'une réduction de risque lorsque les conséquences incluent une dégradation importante de l'environnement ou une perte de biens.

La méthode de l'Annexe E est présentée de façon plus détaillée dans la norme VDI/VDE 2180 (2015).

E.2 Mise en œuvre type de fonctions instrumentées

La protection des installations de processus utilisant des moyens de commande de processus fait clairement la distinction entre les tâches se rapportant à la sécurité et les exigences d'exploitation. Par conséquent, les systèmes de commande de processus sont classés comme suit:

– BPCS;
– systèmes de surveillance de processus;
– SIS.

Le but de cette classification est de disposer d'exigences adéquates applicables à chaque type de système afin de satisfaire aux exigences générales de l'installation, à des coûts raisonnables du point de vue économique. La classification permet une délimitation claire lors de la planification, de l'installation et de l'exploitation, ainsi que lors de modifications ultérieures des systèmes de commande de processus.

Les BPCS sont utilisés pour assurer un fonctionnement correct de l'installation dans sa plage d'exploitation normale. Cela inclut le mesurage, la commande et/ou l'enregistrement de toutes les variables concernées du processus. Les BPCS fonctionnent en continu ou sont fréquemment sollicités pour intervenir avant que la réaction d'un SIS ne soit nécessaire (en principe, les BPCS ne doivent pas être mis en œuvre conformément aux exigences de l'IEC 61511-1:2016).

Les systèmes de surveillance de processus interviennent pendant l'exploitation spécifiée d'une installation de processus au cas où une ou plusieurs variables du processus se situeraient hors des limites de la plage d'exploitation normale. Les systèmes de surveillance

de processus déclenchent une alarme d'état de défaillance admissible de l'installation de processus pour avertir le personnel d'exploitation ou induire des interventions manuelles (en principe, les systèmes de surveillance de processus ne nécessitent pas d'être mis en œuvre conformément aux exigences de l'IEC 61511-1:2016).

Le SIS empêche l'apparition d'un état de défaillance dangereux de l'installation de processus ("système de protection") ou réduit les conséquences d'un événement dangereux.

S'il n'y a aucun SIS, un événement dangereux peut porter atteinte à la sécurité du personnel.

Contrairement aux fonctions d'un BPCS, les fonctions d'un SIS présentent normalement un faible taux de sollicitation. Cela est principalement dû à la faible probabilité d'occurrence de l'événement dangereux. En outre, il y a normalement des BPCS et des systèmes de surveillance qui fonctionnent en continu et réduisent le taux de sollicitation du SIS.

E.3 Synthèse du graphe de risque

Le graphe de risque est fondé sur le principe selon lequel le risque est proportionnel à la conséquence et à la fréquence de l'événement dangereux. Il commence en prenant pour hypothèse qu'il n'existe aucun SIS malgré la présence de systèmes types tels que des BPCS et des systèmes de surveillance, qui ne sont pas des SIS.

Les conséquences sont relatives au dommage associé à la santé et à la sécurité, ou également aux dommages associés à l'environnement.

La fréquence est la combinaison entre:

– la fréquence de présence dans la zone dangereuse et le temps d'exposition potentiel;
– la possibilité d'éviter l'événement dangereux; et
– la probabilité que l'événement dangereux se produise en l'absence d'un SIS (mais tous les autres moyens de réduction de risque étant en fonctionnement) – cela est indiqué sous le terme "probabilité d'occurrence intempestive".

Cela engendre les quatre paramètres de risque suivants:

– la conséquence de l'événement dangereux (S);
– la fréquence de présence dans la zone dangereuse multipliée par le temps d'exposition (A);
– la possibilité d'éviter les conséquences de l'événement dangereux (G);
– la probabilité de l'occurrence intempestive (W).

Lorsqu'un graphe de risque est utilisé pour déterminer le SIL d'une SIF agissant en mode continu, la modification des paramètres utilisés dans le graphe de risque devra être envisagée. Il convient que les paramètres représentent les facteurs de risque qui se rapportent le mieux aux caractéristiques de l'application concernée. Le mapping des SIL par rapport aux résultats des décisions relatives aux paramètres devra également être envisagé, car un certain ajustement peut se révéler nécessaire pour garantir la réduction de risque à des niveaux tolérables. A titre d'exemple, le paramètre W peut être redéfini comme le pourcentage de vie du système durant lequel le système est en service. De ce fait, le paramètre W1 serait sélectionné lorsque le danger n'est pas présent en permanence et que la période par année durant laquelle une défaillance engendrerait un danger est courte. Dans cet exemple, les autres paramètres devraient également être envisagés en ce qui concerne les critères de décision concernés et passer en revue les résultats relatifs aux niveaux d'intégrité pour garantir un risque tolérable.

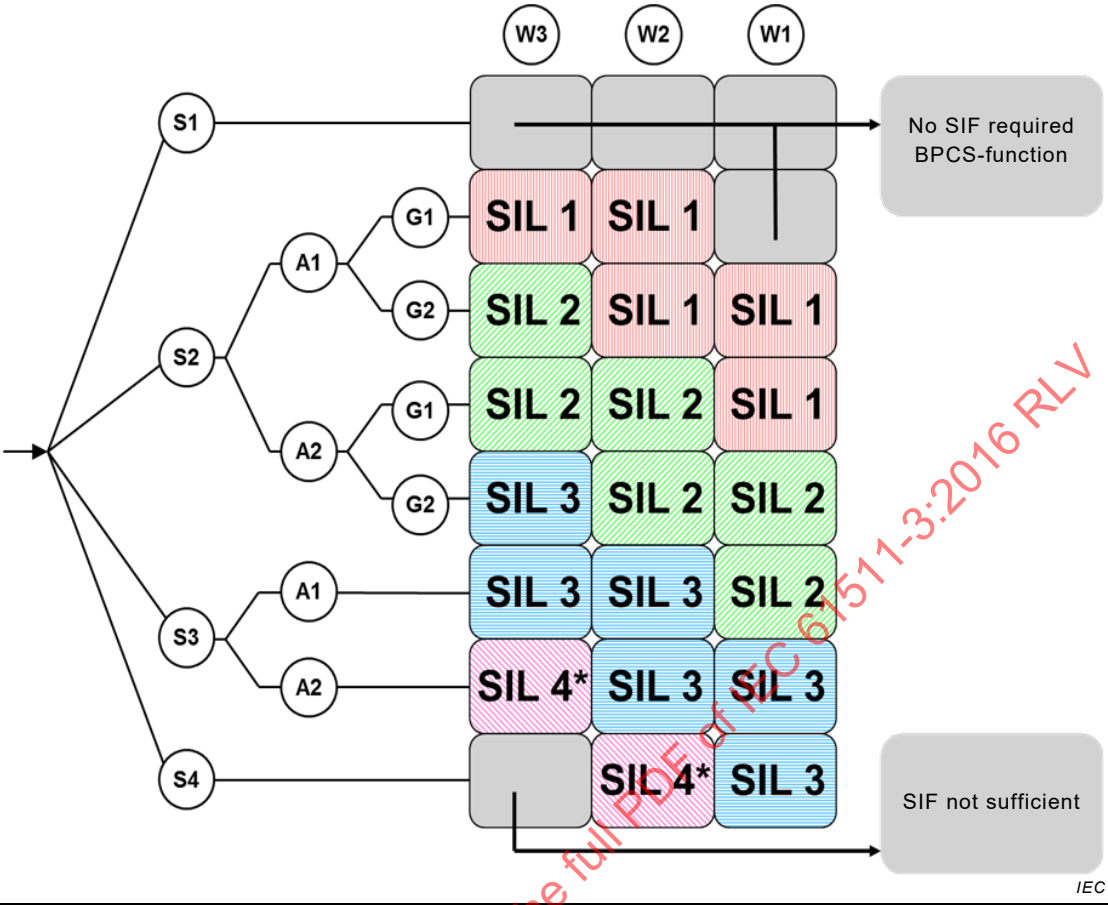
E.4 Mise en œuvre du graphe de risque: protection individuelle

La combinaison des paramètres de risque décrits plus haut permet d'obtenir un graphe de risque tel que donné à la Figure E.1. Des indices de paramètre plus élevés indiquent un risque plus important ($S_1 < S_2 < S_3 < S_4$; $A_1 < A_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$). La classification correspondante des paramètres de la Figure E.1 est donnée dans le Tableau E.1. Le graphique est utilisé séparément pour chaque fonction de sécurité afin de déterminer le SIL exigé pour la fonction en question.

Lors de la détermination du risque devant être évité par les SIS, le risque sans l'existence du SIS à l'étude doit être considéré. Les principaux points de cette revue sont le type et l'étendue des effets et la fréquence prévue de l'état dangereux de l'installation de processus.

Le risque peut être déterminé de manière systématique et vérifiable en utilisant la méthode détaillée dans la norme VDI/VDE 2180, qui permet de déterminer les classes d'exigences à partir de paramètres établis. Selon la règle, plus le nombre ordinal d'une classe d'exigences sera élevé, plus la partie du risque devant être couverte par le SIS sera grande et plus les exigences et les mesures résultantes, de façon générale, seront donc sévères.

En ce qui concerne les industries de transformation, le SIL 4 n'est pas couvert par le SIS seul. Des mesures autres que des mesures de commande de processus doivent être prises pour réduire le risque à SIL 3 au moins.



Anglais	Français
No SIF required	Pas de SIF exigée
BPCS function	Fonction du BPCS
SIF not sufficient	SIF pas suffisante

Légende: * = SIF non recommandée

NOTE Des couleurs différentes sont utilisées pour faciliter l'identification des différentes valeurs du SIL.

Figure E.1 – Graphe de risque de la norme VDI/VDE 2180 – Protection individuelle et relations avec les SIL

Tableau E.1 – Données relatives au graphe de risque (voir Figure E.1)

Paramètre de risque		Classification	Commentaires
Gravité (S)	S1	Blessures légères infligées à des personnes	1) Ce système de classification a été établi pour traiter les blessures et les décès. D'autres méthodes de classification devraient être élaborées pour les atteintes à l'environnement ou aux biens.
	S2	Blessures graves permanentes infligées à une ou plusieurs personnes; décès d'une personne	
	S3	Décès de plusieurs personnes	
	S4	Effet catastrophique, de très nombreuses personnes tuées	
Fréquence de présence dans la zone dangereuse multipliée par le temps d'exposition (A)	A1	Exposition rare à plus fréquente dans la zone dangereuse	2) Voir commentaire 1 ci-dessus.
	A2	Exposition fréquente à permanente dans la zone dangereuse	
Possibilité d'éviter les conséquences de l'événement dangereux (G)	G1	Possible sous certaines conditions	3) Ce paramètre tient compte des éléments suivants: – l'exploitation d'un processus supervisé (c'est-à-dire exploité par des personnes qualifiées ou non qualifiées) ou non supervisé; – le taux de développement de l'événement dangereux (par exemple: soudainement, rapidement ou lentement); – la facilité de reconnaissance du danger (par exemple: perçu immédiatement, détecté par des mesures techniques ou détecté sans mesure technique); – la prévention de l'événement dangereux (par exemple: itinéraires d'évacuation possibles, non possibles ou possibles sous certaines conditions); – l'expérience réelle en matière de sécurité (une telle expérience peut exister pour un processus identique ou similaire ou peut ne pas exister).
	G2	Pratiquement impossible	
Probabilité de l'occurrence intempestive (W)	W1	Une très faible probabilité que les occurrences intempestives soient effectives et seulement quelques occurrences intempestives sont probables	4) L'objectif du facteur W est d'estimer la fréquence de l'occurrence intempestive qui apparaît sans l'ajout d'un SIS (E/E/PE ou autre technologie), mais qui tient compte des installations externes de réduction de risque.
	W2	Une faible probabilité que les occurrences intempestives soient effectives et quelques occurrences intempestives sont probables	
	W3	Une probabilité relativement élevée que les occurrences intempestives soient effectives et des occurrences intempestives fréquentes sont probables	

E.5 Points à considérer lors de l'application de graphes de risque

Lorsque la méthode du graphe de risque est appliquée, il est important de considérer les exigences liées au risque spécifiées par l'exploitant et par les autorités compétentes concernées.

Il convient de décrire et de documenter l'interprétation et l'évaluation de chaque branche du graphe de risque en termes clairs et compréhensibles pour garantir une application cohérente de la méthode.

Il est important que le graphe de risque et son étalonnage soient validés à un niveau hiérarchique élevé au sein de l'organisation chargée de la sécurité.

Annexe F
(informative)

Analyse des couches de protection (LOPA)

F.1 Présentation

L'Annexe F décrit un outil d'analyse de danger lié au processus appelé "analyse des couches de protection" (LOPA, *Layer Of Protection Analysis*). La méthode débute par les données élaborées au cours de l'identification du danger et tient compte de chaque danger identifié en documentant la cause initiatrice et les couches de protection qui évitent ou atténuent le danger. La réduction de risque totale peut alors être déterminée, et la nécessité d'une réduction de risque supplémentaire peut être analysée. Si une réduction de risque supplémentaire est exigée et si elle doit être fournie sous la forme d'une SIF, la méthodologie LOPA permet de déterminer le SIL approprié pour la SIF.

L'Annexe F ne prétend pas fournir une description exhaustive de la méthode. Elle est uniquement destinée à en présenter les principes généraux. Elle est fondée sur une méthode décrite de manière plus détaillée dans la référence suivante:

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 (disponible en anglais seulement)

Voir également l'IEC 61511-2:-, Article F.11 pour obtenir des exemples d'application de la méthode LOPA.

Il convient de ne pas utiliser les valeurs données dans l'Annexe F comme des valeurs génériques, mais dans des applications spécifiques d'analyse des couches de protection.

Le cycle de vie de sécurité du SIS défini dans l'IEC 61511-1:2016 exige de déterminer un SIL pour la conception d'une fonction instrumentée de sécurité. La méthode LOPA décrite ici est une méthode qui peut être appliquée à une installation existante par une équipe pluridisciplinaire pour établir le SIL de la SIF. Il convient que l'équipe soit composée des membres suivants:

– un opérateur expérimenté, capable d'exploiter le processus à l'étude;
– un ingénieur ayant une parfaite maîtrise du processus;
– un gestionnaire de la fabrication;
– un ingénieur spécialisé dans la commande de processus;
– un technicien d'entretien des instruments et de maintenance électrique, ayant une bonne connaissance du processus à l'étude;
– un spécialiste de l'analyse de risque.

Il convient qu'un membre de l'équipe reçoive une formation sur la méthodologie LOPA.

Les informations exigées pour la méthode LOPA figurent parmi les données recueillies et élaborées au cours du processus d'identification du danger. Le Tableau F.1 montre la relation entre les données exigées pour l'analyse des couches de protection (LOPA) et les données élaborées au cours du processus d'identification du danger (étude HAZOP pour cet exemple). La Figure F.1 donne un exemple caractéristique de feuille de calcul qui peut être utilisée pour la méthode LOPA.

La méthode LOPA analyse les dangers afin de déterminer si des SIF sont exigées; le cas échéant, elle permet de déterminer le SIL exigé pour chaque SIF.

F.2 Evénement à impact

En utilisant la Figure F.1, chaque description d'un événement à impact (conséquence) déterminée à partir de l'étude HAZOP est reportée dans la colonne 1.

F.3 Degré de gravité

Les degrés de gravité Mineur (M), Grave (S) ou Très grave (E) sont ensuite sélectionnés pour l'événement à impact conformément au Tableau F.2 et reportés dans la colonne 2 de la Figure F.1.

Tableau F.1 – Données élaborées au cours de l'étude HAZOP pour la méthode LOPA

Informations exigées pour la méthode LOPA	Informations élaborées au cours de l'étude HAZOP
Evénement à impact	Conséquence
Degré de gravité	Gravité de la conséquence
Cause initiatrice	Cause
Probabilité d'occurrence d'une cause initiatrice	Fréquence de la cause
Couches de protection	Protections existantes
Atténuation supplémentaire exigée	Nouvelles protections recommandées