

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.110; 25.040.01

ISBN 978-2-8322-3212-5

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

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	12
2 Normative references	13
3 Terms, definitions and abbreviations	13
Annex A (informative) Risk and safety integrity – general guidance	14
A.1 General.....	14
A.2 Necessary risk reduction	14
A.3 Role of safety instrumented systems.....	14
A.4 Risk and safety integrity	16
A.5 Allocation of safety requirements	17
A.6 Hazardous event, hazardous situation and harmful event	17
A.7 Safety integrity levels	18
A.8 Selection of the method for determining the required safety integrity level	18
Annex B (informative) Semi-quantitative method – event tree analysis	20
B.1 Overview	20
B.2 Compliance with IEC 61511-1:2016	20
B.3 Example	20
B.3.1 General	20
B.3.2 Process safety target	21
B.3.3 Hazard analysis	21
B.3.4 Semi-quantitative risk analysis technique.....	22
B.3.5 Risk analysis of existing process	23
B.3.6 Events that do not meet the process safety target.....	25
B.3.7 Risk reduction using other protection layers.....	26
B.3.8 Risk reduction using a safety instrumented function	26
Annex C (informative) The safety layer matrix method	28
C.1 Overview	28
C.2 Process safety target	29
C.3 Hazard analysis	29
C.4 Risk analysis technique	30
C.5 Safety layer matrix	31
C.6 General procedure	32
Annex D (informative) A semi-qualitative method: calibrated risk graph	34
D.1 Overview	34
D.2 Risk graph synthesis	34
D.3 Calibration	35
D.4 Membership and organization of the team undertaking the SIL assessment	36
D.5 Documentation of results of SIL determination	37
D.6 Example calibration based on typical criteria.....	37
D.7 Using risk graphs where the consequences are environmental damage	40
D.8 Using risk graphs where the consequences are asset loss	41
D.9 Determining the integrity level of instrument protection function where the consequences of failure involve more than one type of loss.....	41
Annex E (informative) A qualitative method: risk graph	42

E.1	General.....	42
E.2	Typical implementation of instrumented functions	42
E.3	Risk graph synthesis	43
E.4	Risk graph implementation: personnel protection	43
E.5	Relevant issues to be considered during application of risk graphs.....	45
Annex F	(informative) Layer of protection analysis (LOPA)	47
F.1	Overview	47
F.2	Impact event	48
F.3	Severity level	48
F.4	Initiating cause.....	49
F.5	Initiation likelihood	50
F.6	Protection layers	50
F.7	Additional mitigation.....	51
F.8	Independent protection layers (IPL)	51
F.9	Intermediate event likelihood	52
F.10	SIF integrity level	52
F.11	Mitigated event likelihood	52
F.12	Total risk.....	52
F.13	Example	53
F.13.1	General	53
F.13.2	Impact event and severity level	53
F.13.3	Initiating cause	53
F.13.4	Initiating likelihood	53
F.13.5	General process design.....	53
F.13.6	BPCS	53
F.13.7	Alarms	53
F.13.8	Additional mitigation.....	54
F.13.9	Independent protection layer(s) (IPL).....	54
F.13.10	Intermediate event likelihood.....	54
F.13.11	SIS	54
F.13.12	Next SIF	54
Annex G	(informative) Layer of protection analysis using a risk matrix	56
G.1	Overview	56
G.2	Procedure.....	58
G.2.1	General	58
G.2.2	Step 1: General Information and node definition	58
G.2.3	Step 2: Describe hazardous event	59
G.2.4	Step 3: Evaluate initiating event frequency	62
G.2.5	Step 4: Determine hazardous event consequence severity and risk reduction factor.....	63
G.2.6	Step 5: Identify independent protection layers and risk reduction factor	64
G.2.7	Step 6: Identify consequence mitigation systems and risk reduction factor.....	65
G.2.8	Step 7: Determine CMS risk gap.....	66
G.2.9	Step 8: Determine scenario risk gap	69
G.2.10	Step 9: Make recommendations when needed	69
Annex H	(informative) A qualitative approach for risk estimation & safety integrity level (SIL) assignment	71
H.1	Overview	71

H.2	Risk estimation and SIL assignment	73
H.2.1	General	73
H.2.2	Hazard identification/indication	73
H.2.3	Risk estimation	73
H.2.4	Consequence parameter selection (C) (Table H.2)	74
H.2.5	Probability of occurrence of that harm	75
H.2.6	Estimating probability of harm	77
H.2.7	SIL assignment	77
Annex I (informative)	Designing & calibrating a risk graph	80
I.1	Overview	80
I.2	Steps involved in risk graph design and calibration	80
I.3	Risk graph development	80
I.4	The risk graph parameters	81
I.4.1	Choosing parameters	81
I.4.2	Number of parameters	81
I.4.3	Parameter value	81
I.4.4	Parameter definition	81
I.4.5	Risk graph	82
I.4.6	Tolerable event frequencies (Tef) for each consequence	82
I.4.7	Calibration	83
I.4.8	Completion of the risk graph	84
Annex J (informative)	Multiple safety systems	85
J.1	Overview	85
J.2	Notion of systemic dependencies	85
J.3	Semi-quantitative approaches	88
J.4	Boolean approaches	89
J.5	State-transition approach	92
Annex K (informative)	As low as reasonably practicable (ALARP) and tolerable risk concepts	96
K.1	General	96
K.2	ALARP model	96
K.2.1	Overview	96
K.2.2	Tolerable risk target	97
Bibliography		99
Figure 1	Overall framework of the IEC 61511 series	11
Figure 2	Typical protection layers and risk reduction means	13
Figure A.1	Risk reduction: general concepts	16
Figure A.2	Risk and safety integrity concepts	17
Figure A.3	Harmful event progression	18
Figure A.4	Allocation of safety requirements to the non-SIS protection layers and other protection layers	19
Figure B.1	Pressurized vessel with existing safety systems	21
Figure B.2	Fault tree for overpressure of the vessel	24
Figure B.3	Hazardous events with existing safety systems	25
Figure B.4	Hazardous events with SIL 2 safety instrumented function	27
Figure C.1	Protection layers	28

Figure C.2 – Example of safety layer matrix.....	32
Figure D.1 – Risk graph: general scheme	38
Figure D.2 – Risk graph: environmental loss.....	41
Figure E.1 – VDI/VDE 2180 Risk graph – personnel protection and relationship to SILs.....	44
Figure F.1 – Layer of protection analysis (LOPA) report.....	49
Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL.....	56
Figure G.2 – Work process used for Annex G	58
Figure G.3 – Example process node boundary for selected scenario	59
Figure G.4 – Acceptable secondary consequence risk	67
Figure G.5 – Unacceptable secondary consequence risk	67
Figure G.6 – Managed secondary consequence risk	69
Figure H.1 – Workflow of SIL assignment process	72
Figure H.2 – Parameters used in risk estimation.....	74
Figure I.1 – Risk graph parameters to consider.....	81
Figure I.2 – Illustration of a risk graph with parameters from Figure I.1.....	82
Figure J.1 – Conventional calculations	85
Figure J.2 – Accurate calculations.....	86
Figure J.3 – Redundant SIS	88
Figure J.4 – Corrective coefficients for hazardous event frequency calculations when the proof tests are performed at the same time.....	89
Figure J.5 – Expansion of the simple example	89
Figure J.6 – Fault tree modelling of the multi SIS presented in Figure J.5.....	90
Figure J.7 – Modelling CCF between SIS ₁ and SIS ₂	91
Figure J.8 – Effect of tests staggering	91
Figure J.9 – Effect of partial stroking	92
Figure J.10 – Modelling of repair resource mobilisation.....	93
Figure J.11 – Example of output from Monte Carlo simulation	94
Figure J.12 – Impact of repairs due to shared repair resources	95
Figure K.1 – Tolerable risk and ALARP	97
Table B.1 – HAZOP study results	22
Table C.1 – Frequency of hazardous event likelihood (without considering PLs).....	31
Table C.2 – Criteria for rating the severity of impact of hazardous events.....	31
Table D.1 – Descriptions of process industry risk graph parameters.....	35
Table D.2 – Example calibration of the general purpose risk graph	39
Table D.3 – General environmental consequences	40
Table E.1 – Data relating to risk graph (see Figure E.1).....	45
Table F.1 – HAZOP developed data for LOPA	48
Table F.2 – Impact event severity levels.....	49
Table F.3 – Initiation likelihood.....	50
Table F.4 – Typical protection layers (prevention and mitigation) PFD _{avg}	51
Table G.1 – Selected scenario from HAZOP worksheet.....	59
Table G.2 – Selected scenario from LOPA worksheet	61

Table G.3 – Example initiating causes and associated frequency	63
Table G.4 – Consequence severity decision table	64
Table G.5 – Risk reduction factor matrix.....	64
Table G.6 – Examples of independent protection layers (IPL) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	66
Table G.7 – Examples of consequence mitigation system (CMS) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	66
Table G.8 – Step 7 LOPA worksheet (1 of 2)	68
Table G.9 – Step 8 LOPA worksheet (1 of 2)	70
Table H.1 – List of SIFs and hazardous events to be assessed	73
Table H.2 – Consequence parameter/severity level	74
Table H.3 – Occupancy parameter/Exposure probability (F).....	75
Table H.4 – Avoidance parameter/avoidance probability	76
Table H.5 – Demand rate parameter (W)	77
Table H.6 – Risk graph matrix (SIL assignment form for safety instrumented functions).....	78
Table H.7 – Example of consequence categories	78
Table K.1 – Example of risk classification of incidents	98
Table K.2 – Interpretation of risk classes	98

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 61511-1:2016 should 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.

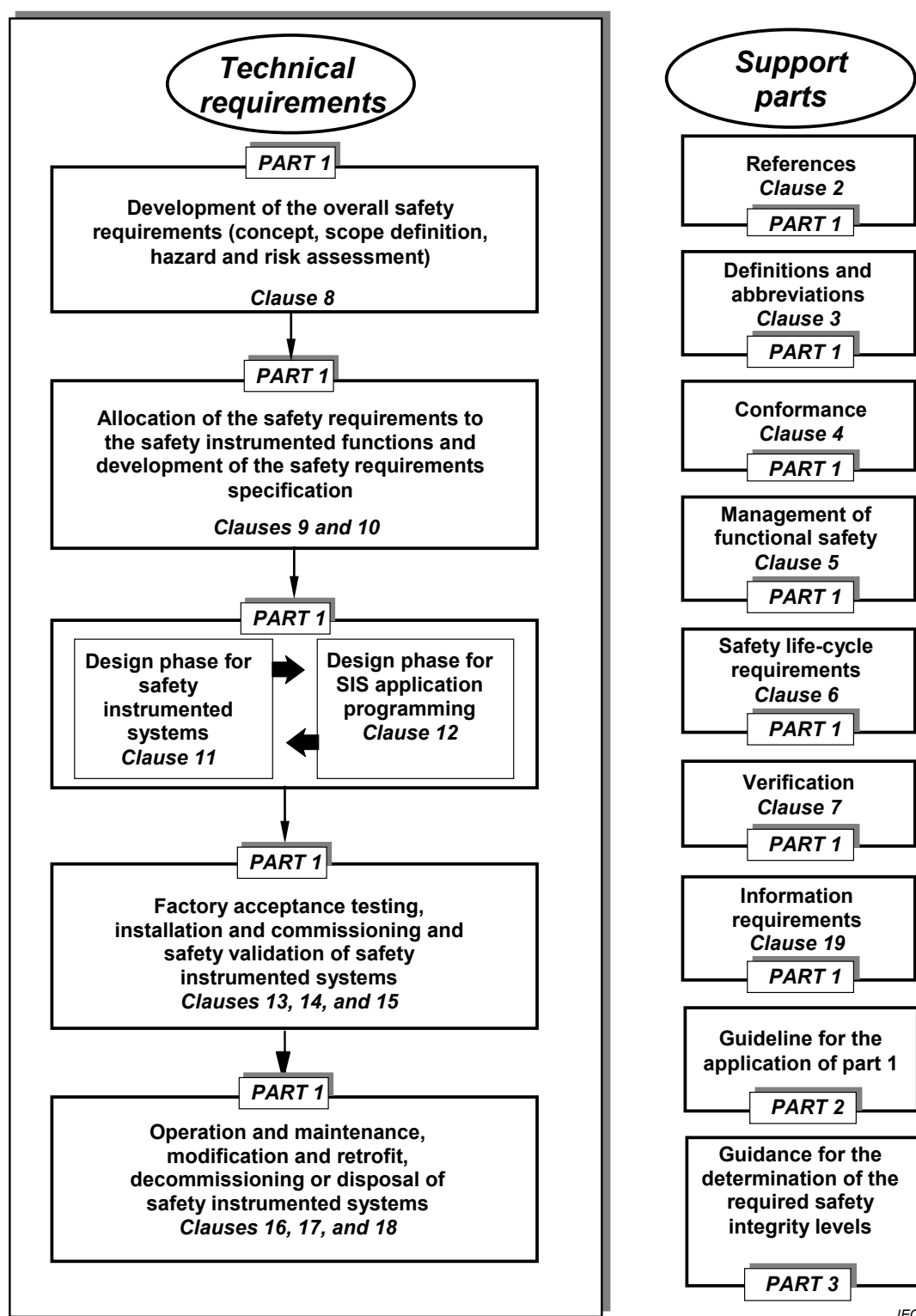


Figure 1 – Overall framework of the IEC 61511 series

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.

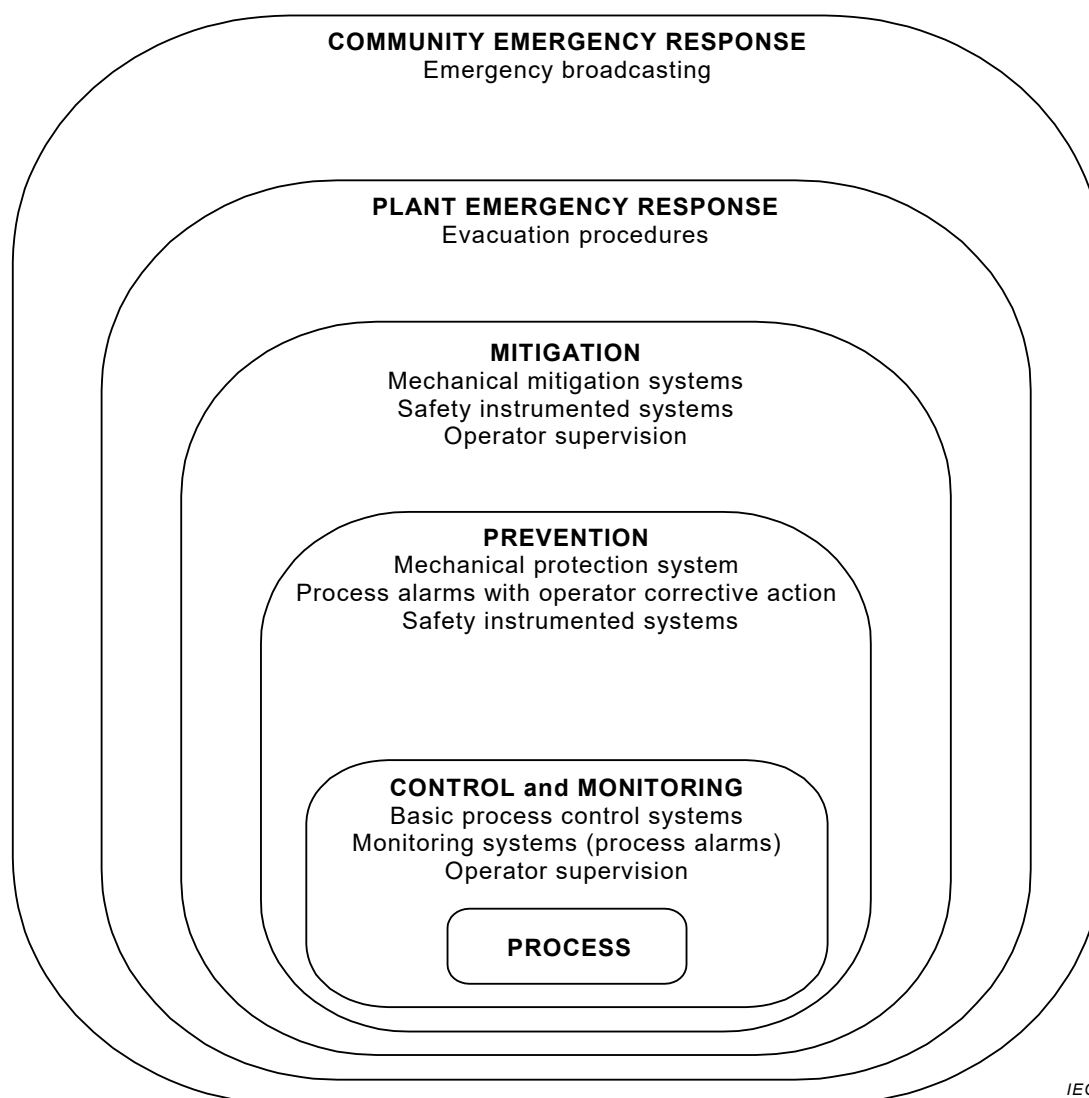


Figure 2 – Typical protection layers and risk reduction means

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 61511-1:2016 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 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.

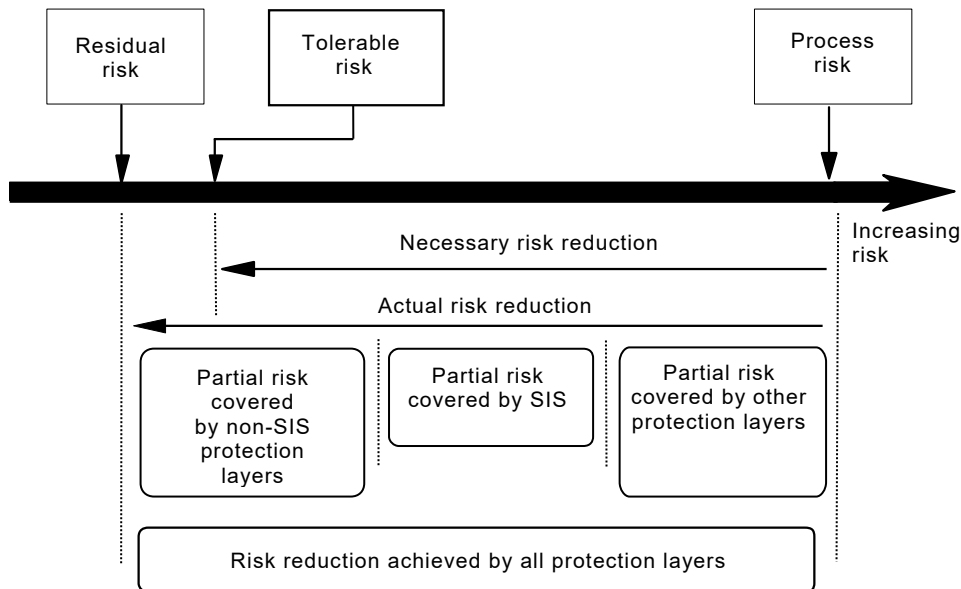
The various risks indicated in Figures A.1 and A.2 are as follows:

- 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.



IEC

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.

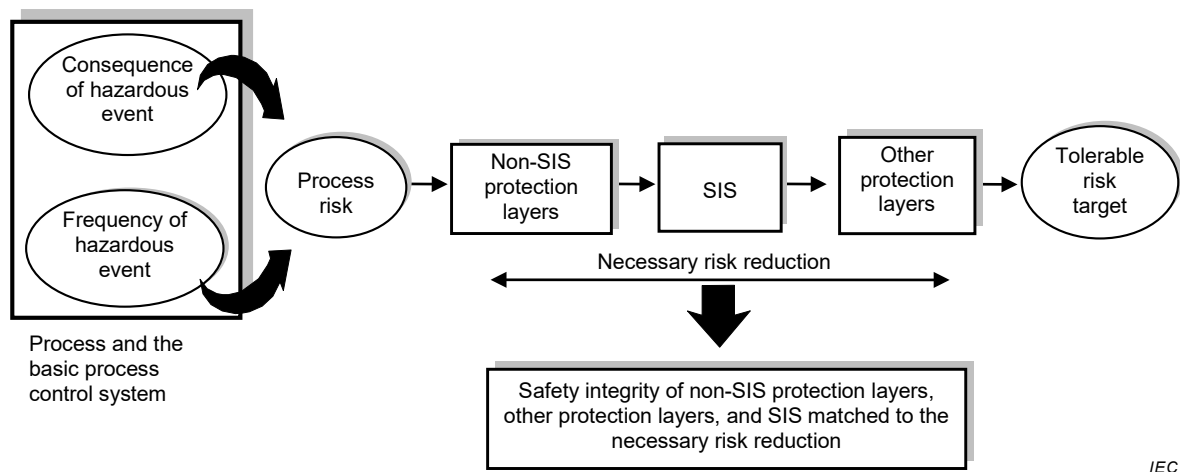


Figure A.2 – Risk and safety integrity concepts

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.

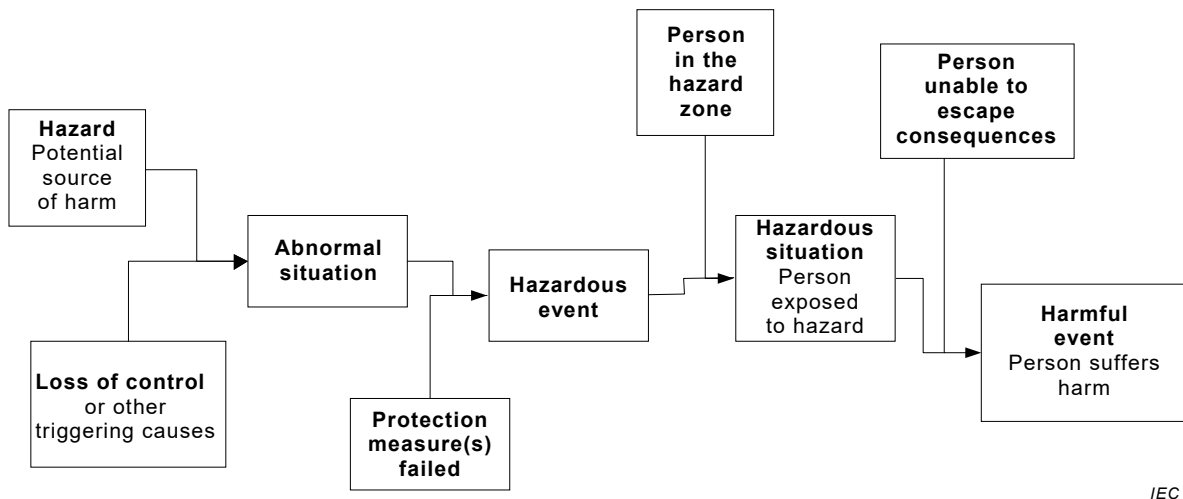


Figure A.3 – Harmful event progression

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.

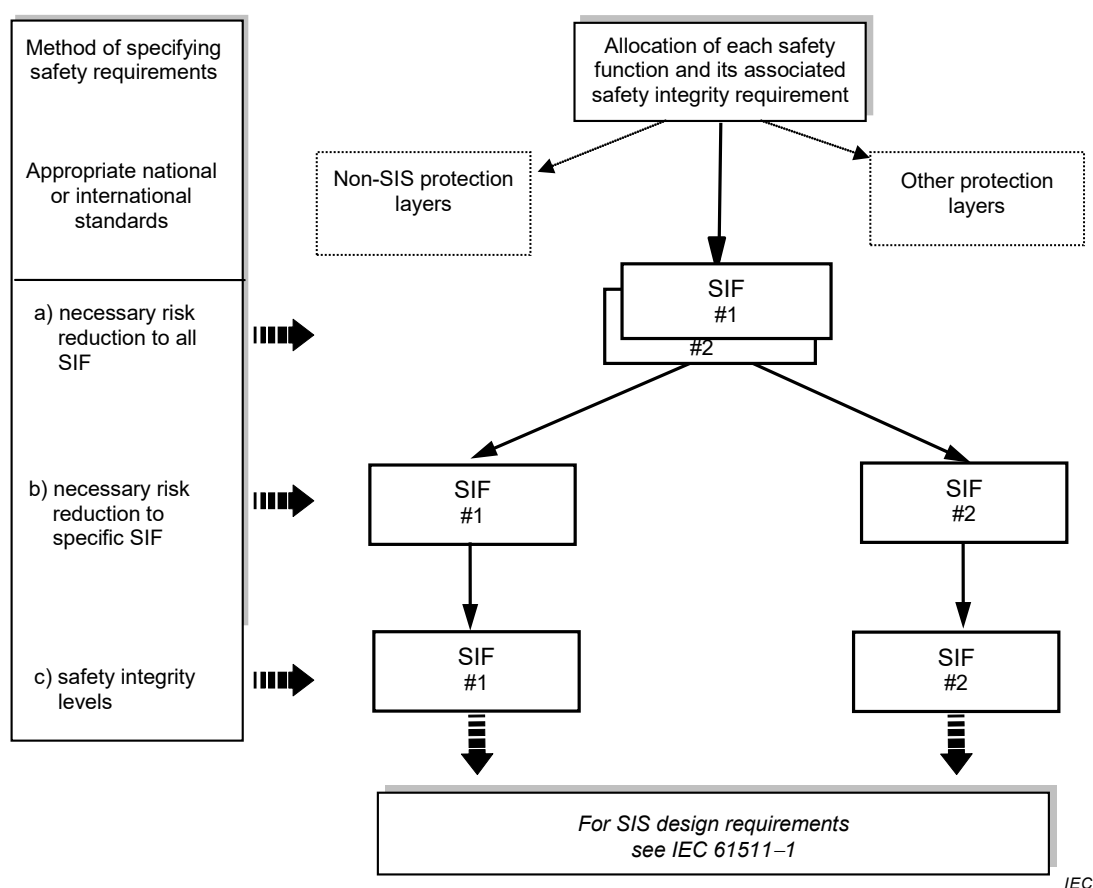
A.8 Selection of the method for determining the required safety integrity level

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.

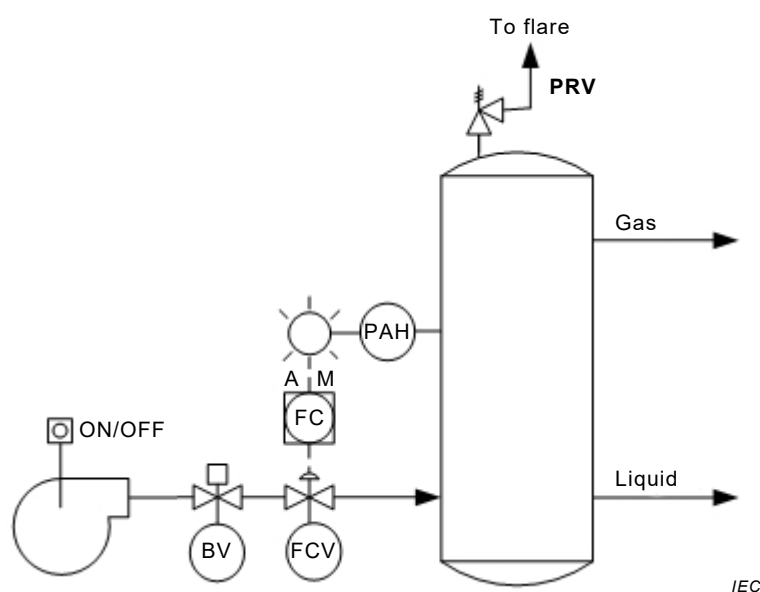
B.3 Example

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.

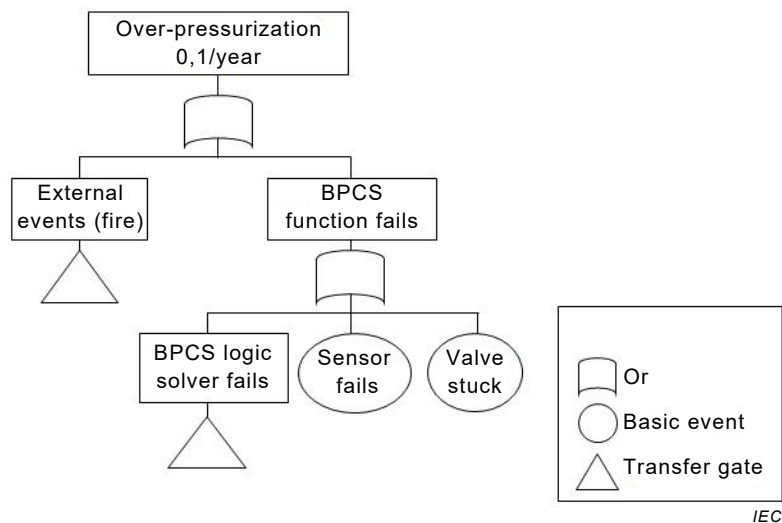


Figure B.2 – Fault tree for overpressure of the vessel

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

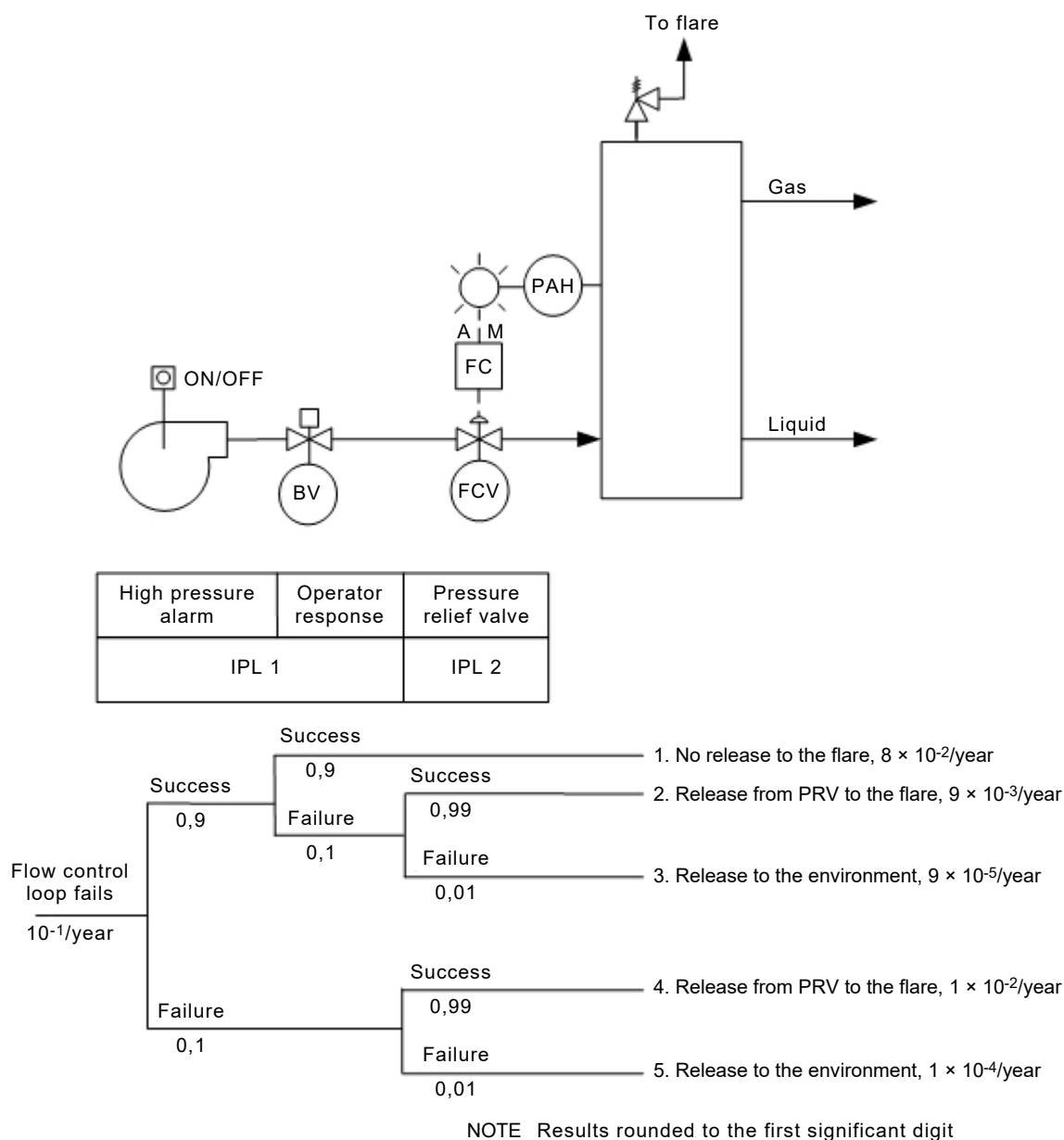
Once the frequency of occurrence of the initiating event has been established, the success or failure of the safety systems to respond to the abnormal condition is modelled using event tree analysis. The reliability data for the performance of the safety systems can be taken from field data, published 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.



IEC

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 × 10⁻⁴ (scenario 5) = 1,9 × 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.

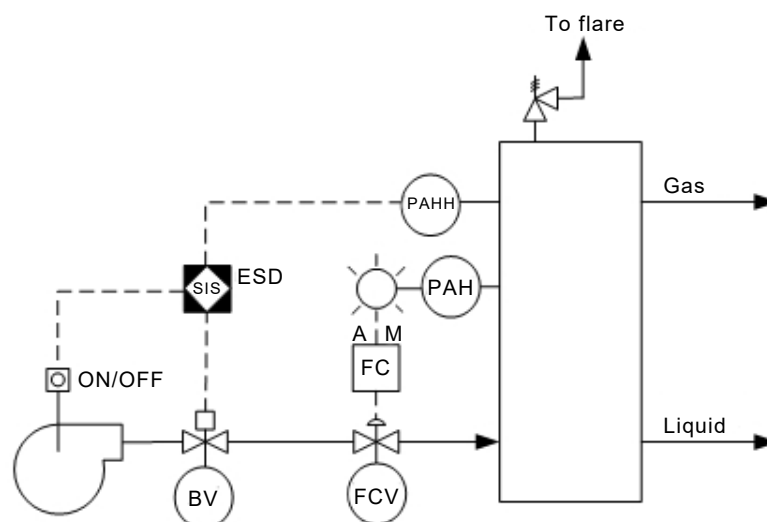
In this design case, successful operation of the SIS results in a shutdown of the process and occurs at a frequency of $1,9 \times 10^{-2}$ per year. The SIS reduces the process demand rate on the pressure relief valve. The frequency of scenario outcome 3 involving release from the PRV to the flare is 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.

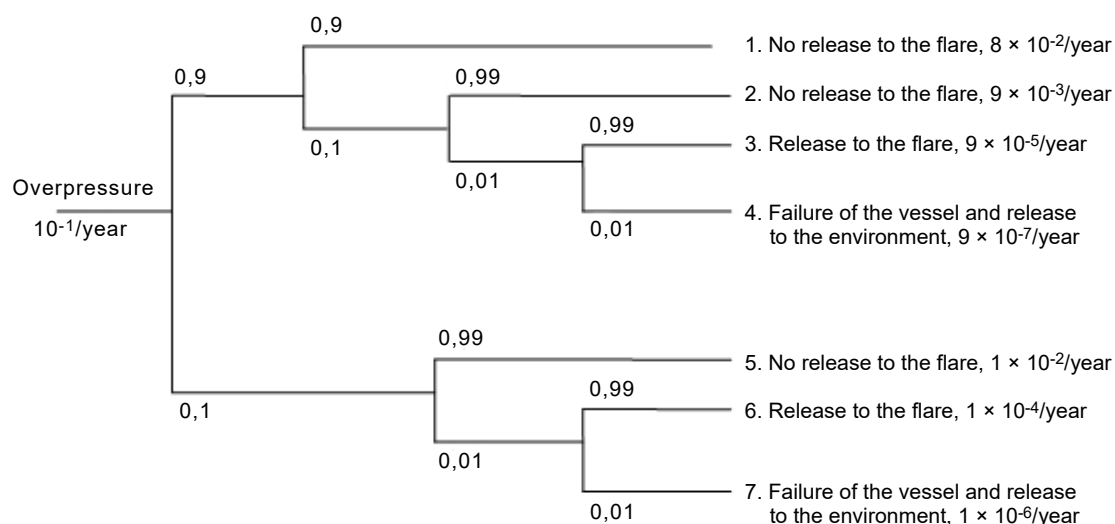
The total frequency of vessel failure with release to the environment (sum of frequencies of scenarios 4 and 7) has been reduced to $1,9 \times 10^{-6}$ per year, below the process safety target of 10^{-4} per year.

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.



High pressure alarm	Operator response	SIL 2 SIS	Pressure relief valve
IPL 1		IPL 2	IPL 3



NOTE Results rounded to the first significant digit

IEC

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

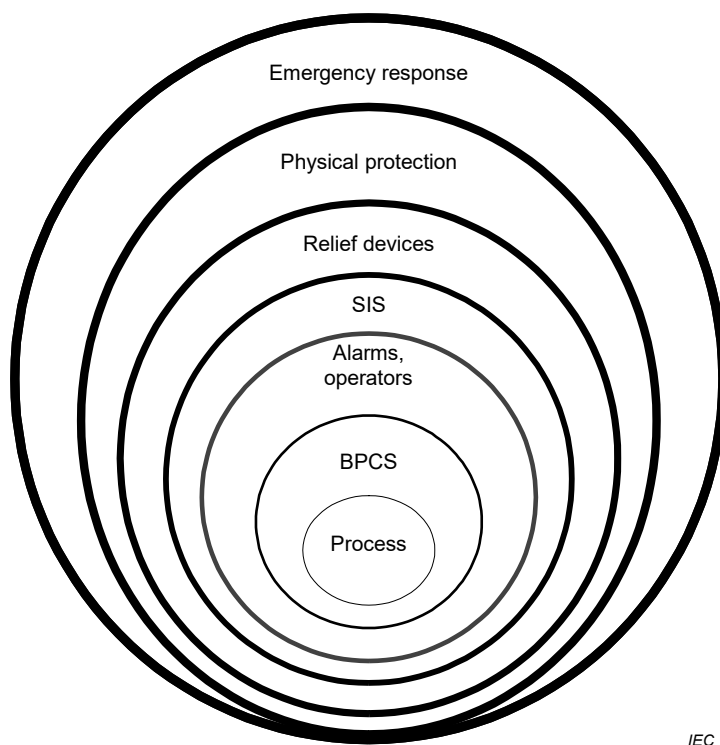
Annex C (informative)

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.



IEC

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.

Number of existing PLs	Required SIL								
							c)	1	1
	c)	c)	1	c)	1	2	1	2	b)
	c)	1	2	1	2	3	b)	b)	a)
Hazardous event likelihood	L o w	M e d	H i g h	L o w	M e d	H i g h	L o w	M e d	H i g h
Minor			Serious			Extensive			
Hazardous event severity rating									

IEC

- 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

- Establish the process safety target.
- Perform a hazard identification (for example, HAZOP studies) to identify all hazardous events of interest.
- Establish the hazardous event scenarios and estimate the hazardous event likelihood using company specific guidelines and data.
- Establish the severity rating of the hazardous events using company specific guidelines.
- 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:

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

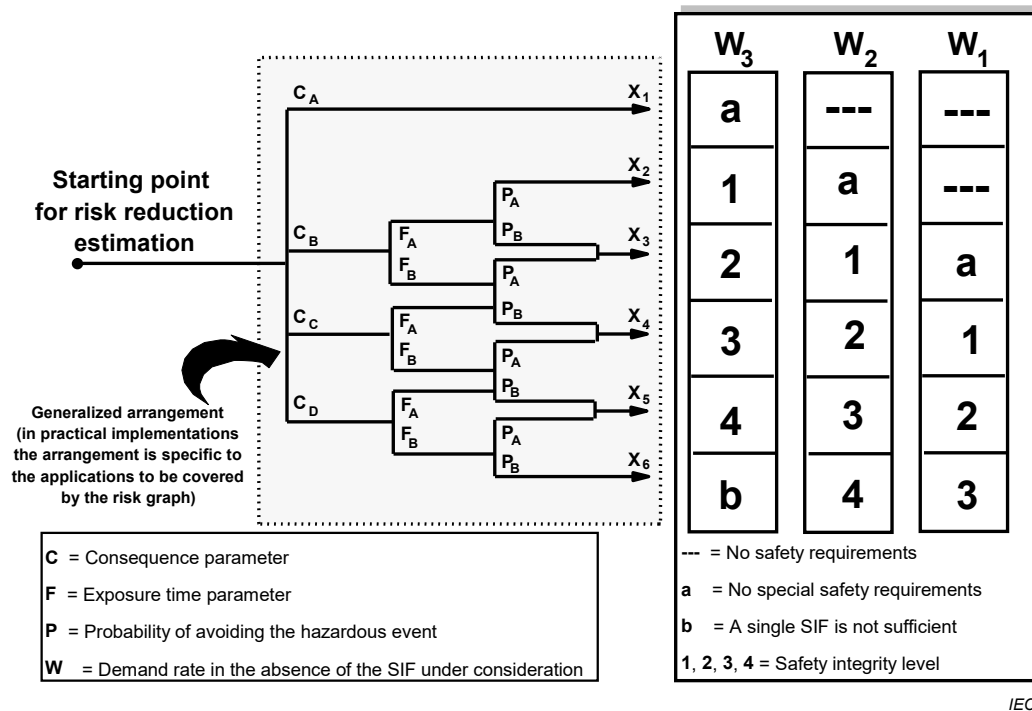


Figure D.1 – Risk graph: general scheme

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	Minor injury	a) The classification system has been developed to deal with injury and death to people.
	CB	Range 0,01 to 0,1	b) For the interpretation of CA, CB, CC and CD, the consequences of the accident and normal healing should be taken into account.
	CC	Range >0,1 to 1,0	
	CD	Range >1,0	
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	Rare to more frequent exposure in the hazardous zone. Occupancy less than 0,1	c) See comment a) above.
	FB	Frequent to permanent exposure in the hazardous zone	
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	PA	Adopted if all conditions in column 4 are 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.
	PB	Adopted if any one of the conditions are not satisfied	
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	Demand rate between 0,1 D and D per year	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.
	W3	Demand rate between D and 10 D per year	
		For demand rates higher than 10 D per year higher integrity shall be needed	
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.

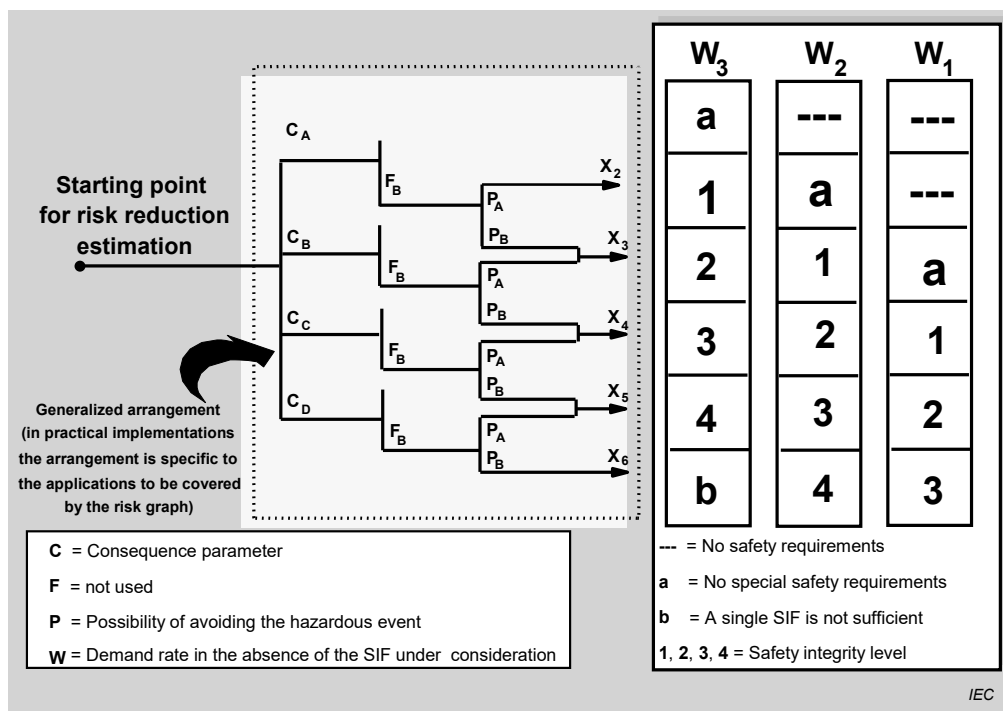


Figure D.2 – Risk graph: environmental loss

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.

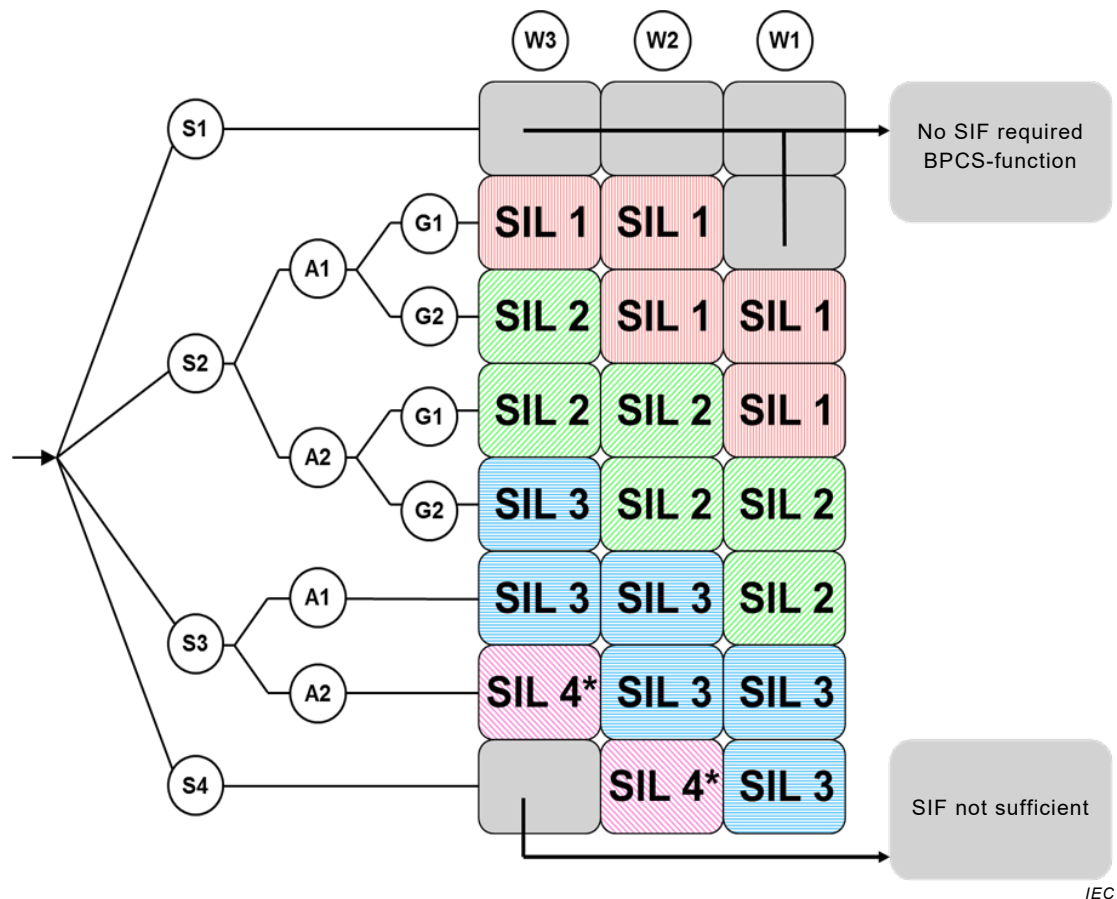
E.4 Risk graph implementation: personnel protection

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