

Guidance on safety integrity level determination for safety instrumented systems in support of IEC 61511



This is a preview. [Click here to purchase the full publication.](#)

GUIDANCE ON SAFETY INTEGRITY LEVEL DETERMINATION
FOR SAFETY INSTRUMENTED SYSTEMS IN SUPPORT OF IEC 61511

First edition

January 2020

Published by

Energy Institute, London

The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

This is a preview. [Click here to purchase the full publication.](#)

The Energy Institute (EI) is the chartered professional membership body for the energy industry, supporting over 20 000 individuals working in or studying energy and 200 energy companies worldwide. The EI provides learning and networking opportunities to support professional development, as well as professional recognition and technical and scientific knowledge resources on energy in all its forms and applications.

The EI's purpose is to develop and disseminate knowledge, skills and good practice towards a safe, secure and sustainable energy system. In fulfilling this mission, the EI addresses the depth and breadth of the energy sector, from fuels and fuels distribution to health and safety, sustainability and the environment. It also informs policy by providing a platform for debate and scientifically-sound information on energy issues.

The EI is licensed by:

- the Engineering Council to award Chartered, Incorporated and Engineering Technician status, and
- the Society for the Environment to award Chartered Environmentalist status.

It also offers its own Chartered Energy Engineer, Chartered Petroleum Engineer, and Chartered Energy Manager titles.

A registered charity, the EI serves society with independence, professionalism and a wealth of expertise in all energy matters.

This publication has been produced as a result of work carried out within the Technical Team of the EI, funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit <http://www.energyinst.org>

The EI gratefully acknowledges the financial contributions towards the scientific and technical programme from the following companies:

BP Exploration Operating Co Ltd	Qatar Petroleum
BP Oil UK Ltd	Repsol Sinopec
Centrica	RWE npower
Chevron North Sea Ltd	Saudi Aramco
Chevron Products Company	Scottish Power
Chrysaor	SGS
CLH	Shell UK Oil Products Limited
ConocoPhillips Ltd	Shell U.K. Exploration and Production Ltd
DCC Energy	SSE
EDF Energy	TAQA Bratani
ENI	Total E&P UK Limited
E.ON UK	Total UK Limited
Equinor	Tullow Oil
ExxonMobil International Ltd	Uniper
Innogy	Valero
Kuwait Petroleum International Ltd	Vattenfall
Nexen CNOOC	Vitol Energy
Ørsted	Woodside
Perenco	World Fuel Services
Phillips 66	

However, it should be noted that the above organisations have not all been directly involved in the development of this publication, nor do they necessarily endorse its content.

Copyright © 2019 by the Energy Institute, London.

The Energy Institute is a professional membership body incorporated by Royal Charter 2003.

Registered charity number 1097899, England

All rights reserved

No part of this book may be reproduced by any means, or transmitted or translated into a machine language without the written permission of the publisher.

ISBN 978 1 78725 106 9

Published by the Energy Institute

The information contained in this publication is provided for general information purposes only. Whilst the Energy Institute and the contributors have applied reasonable care in developing this publication, no representations or warranties, express or implied, are made by the Energy Institute or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the Energy Institute and the contributors accept no responsibility whatsoever for the use of this information. Neither the Energy Institute nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

Hard copy and electronic access to EI and IP publications is available via our website, <https://publishing.energyinst.org>.

Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.

For more information, contact the EI Publications Team.

e: pubs@energyinst.org

This is a preview. [Click here to purchase the full publication.](#)

CONTENTS

	Page
Foreword	8
Acknowledgements	10
1 Introduction, scope and application	12
1.1 Introduction	12
1.2 Industry context	13
1.3 Scope	13
1.4 Meeting safety and environmental legal requirements	14
1.5 Risk types and criteria	14
1.6 Application	14
2 Basic introduction to safety integrity level (SIL) determination	17
2.1 Introduction	17
2.2 Safety instrumented systems (SISs) and safety instrumented functions (SIFs)	17
2.3 SIF functionality and performance (safety integrity)	19
2.3.1 Key attributes of a SIF	20
2.3.2 Safety integrity and reliability	20
2.4 Hazard, risk and safety-related terms	21
2.4.1 Hazard-related terms	21
2.4.2 Risk and safety-related terms	22
2.4.3 Protection layers (PLs) (prevention/mitigation)	22
2.5 Risk reduction concepts	24
2.6 Example: risk reduction achieved by a SIF	26
2.7 Modes of operation and SIF target failure measures	28
2.8 Summary of key points	31
3 SIL determination process	33
3.1 Introduction	33
3.2 The key steps of SIL determination	33
3.3 Step 1: Preliminary activities required before undertaking safety integrity level determination	34
3.3.1 Selecting target harmful event frequencies	34
3.3.2 Specify team competence, constitution and members	36
3.3.3 Required information available to the SIL determination workshop team	38
3.3.4 Hazard analysis	39
3.4 Step 2: SIL determination method	40
3.4.1 Risk graph method	41
3.4.2 Layers of protection analysis (LOPA) method	42
3.4.3 Fault tree analysis (FTA) method	42
3.4.4 Quantitative risk assessment (QRA) method	43
3.4.5 Criteria for SIL determination method selection	43
3.5 Step 3: Undertaking the SIL determination	45
3.5.1 Step 3.1: Select specific hazardous event	46
3.5.2 Step 3.2: Identify all initiating events (IEs), enabling events and conditions, and estimate the IE frequencies	46
3.5.3 Step 3.3: Identify PLs (prevention)	47
3.5.4 Step 3.4: Identify PLs (mitigation)	48

Contents continued

	Page
3.5.5 Step 3.5: Determine the conditional modifiers (CMs)	49
3.5.6 Step 3.6: Conduct a risk analysis to determine the intermediate harmful event frequency	49
3.5.7 Step 3.7: Compare the intermediate harmful event frequency with the initial target risk frequency and establish a provisional SIL	50
3.5.8 Step 3.8: Development of the SIF functionality	52
3.5.9 Step 4: Sensitivity analysis	52
3.6 Step 5: As low as reasonably practicable (ALARP) demonstration	53
3.7 Step 6: Completion of analysis for all hazardous events	54
3.8 Step 7: Review completed SIL determination/develop SIL determination report	55
3.9 Step 8: Management of change (MoC) and periodic review	55
4 Key questions for senior managers	57
Annexes	
Annex A Glossaries of terms, acronyms and abbreviations, and symbols	61
A.1 Introduction	61
A.2 Glossary of terms	61
A.3 Glossary of acronyms and abbreviations	74
A.4 Glossary of symbols	77
Annex B References and bibliography	78
Annex C Detailed guidance on SIL determination	81
C.1 Introduction	81
C.2 What SIL determination achieves	81
C.3 Determining hazardous events	83
C.3.1 Example – Concept of sufficient independence between the specified PL and the IE that it is designed to protect against	85
C.4 Risk reduction concepts	85
C.4.1 SIF functionality and performance (safety integrity)	85
C.4.2 Overall risk reduction model	86
C.5 SILs and modes of operation	88
C.5.1 Design strategy to achieve a specified SIL	88
C.5.2 Modes of operation	90
C.6 Common cause failures	96
C.7 Basic process control system dangerous failures that place a demand on a PL	96
C.8 Basic process control system protection function implemented as a PL and a person in the SIF loop	97
C.9 Conditional modifiers	101
C.9.1 Example: Conditional modifiers (CMs) independent of initiating events (IEs)	103
C.10 SIL determination examples: overall risk model examples	103
C.11 Ongoing management and auditability of risk reduction measures (RRMs) and risk reduction parameters	105
C.12 As low as reasonably practicable (ALARP) framework	106

Contents continued

	Page
C.12.1 The ALARP concept	106
C.12.2 ALARP demonstration	108
C.12.3 Cost benefit analysis (CBA).	109
C.13 Human failures and human error probabilities (HEPs)	115
C.14 Walk-through example of the SIL determination process.	116
C.15 Generalised risk graph	117
Annex D Selecting target harmful event frequencies for SIL determination	122
D.1 Introduction	122
D.2 Corporate risk policy	122
D.3 Selecting target harmful event frequencies: general considerations.	123
D.4 Specified harmful event frequencies: safety risks – general	124
D.4.1 Specified harmful event frequencies: all safety risks (process and non-process risks).	126
D.4.2 Specified harmful event frequencies: risk allowance for non-process risks	126
D.4.3 Specified harmful event frequencies: process risks – individual risk for exposure to multiple hazardous events	127
D.5 Specified harmful event frequencies: environmental risks	129
D.6 Specified harmful event frequencies: asset risks	131
Annex E Worked examples.	132
E.1 Example 1: Low liquid level in sour gas suction scrubber.	132
E.1.1 Overview	132
E.1.2 IEs	133
E.1.3 CMs.	134
E.1.4 PLs	134
E.1.5 Application of SIL determination methods	134
E.1.6 ALARP demonstration	135
E.1.7 SIF characteristics	136
E.2 Example 2: Overfill of above-ground storage tank containing a petroleum fuel	138
E.2.1 Overview	138
E.2.2 Event tree analysis	141
E.2.3 SIF safety integrity requirements.	142
Annex F Common shortfalls found in LOPA studies.	143

LIST OF FIGURES AND TABLES

	Page
Figures	
Figure 1 Overall structure of this technical publication	16
Figure 2 Safety instrumented system (SIS)	18
Figure 3 A SIS carrying out several SIFs	19
Figure 4 Example of a SIF loop	19
Figure 5 Interrelationship of the key hazard– and harm-related terms	21
Figure 6 The concept of risk	22
Figure 7 PLs (prevention) and PLs (mitigation) illustrated through a bow-tie diagram	23
Figure 8 Illustrative RRM found in the process industry sectors	24
Figure 9 Basic risk model to illustrate terminology	24
Figure 10 Illustration of the risk reduction achieved by reducing the harmful event frequency	27
Figure 11 Illustration of risk reduction concepts and relationship of the SIL to the risk reduction achieved	30
Figure 12 SIL determination process flowchart	35
Figure 13 SIL determination method selection (the qualitative-quantitative continuum)	43
Figure C.1 PLs (prevention) and PLs (mitigation) illustrated through a bow-tie diagram	83
Figure C.2 Determination of the SIFs from knowledge of the specific IEs and hazardous event scenario	84
Figure C.3 Overall risk model: key risk reduction methods and risk parameter terminology	87
Figure C.4 IEC 61511: Design requirements to achieve a specified SIL for the specified SIF	89
Figure C.5 Overall risk model applied to SIL determination for SIF operating in low demand mode	92
Figure C.6 Overall risk model applied to SIL determination for SIF operating in high demand or continuous mode	94
Figure C.7 Concept of implementing a BPCS protection function as a PL in the BPCS	98
Figure C.8 Concept of implementing a BPCS protection function as a PL in the BPCS: Process Operator implements part of the BPCS control function.	99
Figure C.9 Concept of implementing a BPCS protection function as a PL in the BPCS: Process Operator A implements part of the BPCS control function and Process Operator B implements part of the BPCS protection function.	99
Figure C.10 Low demand mode: Role of the CM, ORRMs and the SIS carrying out the specified SIF, in the risk reduction process	104
Figure C.11 High demand or continuous mode: Role of the CM, ORRMs and the SIS carrying out the specified SIF, in the risk reduction process	105
Figure C.12 The ALARP model	107
Figure C.13 The ALARP model: individual fatality rates for workers and members of the public	108
Figure C.14 The ALARP model and CBA illustrating use of DFs	110
Figure C.15 DFs and target harmful event frequencies	111
Figure C.16 Examples of potential human failures on a hazardous event sequence	115
Figure C.17 Risk model for use in walk-through SIL determination example	116
Figure C.18 Generalised risk graph	118
Figure D.1 Target harmful event frequencies for all safety risks where the consequence is an individual worker fatality	123
Figure D.2 Target harmful event frequencies for all safety risks where the consequence is an individual worker fatality	126
Figure D.3 Target harmful event frequencies for process risks for a hypothetical person with a risk profile factor (N) = 1, where the consequence is an individual fatality	127
Figure D.4 Target harmful event frequencies for process risks for a hypothetical person with a risk profile factor = N, where the consequence is an individual fatality	128

List of figures and tables continued

	Page
Figure E.1	Example 1: Schematic of system under analysis 133
Figure E.2	Example 1: FTA for example 1 138
Figure E.3	Example 2: Conceptual model of a bulk fuels storage facility showing source, pathways and environmental receptors 139
Figure E.4	Example 2: Event tree for AST CTF and overtop of secondary and tertiary containment with environmental impact consequences using base CTF incident frequency for worldwide CTFs 140

Tables

Table 1	Target failure measures for a SIF operating in low demand mode versus SIL of the SIF 28
Table 2	SIL determination workshop team: Typical roles and responsibilities when undertaking the SIL determination workshop. 37
Table 3	Comparison between qualitative and quantitative risk assessment methods. 44
Table 4	Key questions for senior managers 58
Table C.1	Target failure measures for a SIF operating in demand mode versus SIL of the SIF. . . 91
Table C.2	Target failure measures for a SIF operating in demand mode or continuous mode versus SIL of the SIF 91
Table C.3	Valuations of preventing health and safety effects on persons 114
Table C.4	Walk-through of SIL determination process using a simplified LOPA approach . . . 119
Table D.1	Illustrative ranges of target harmful event frequencies for specified consequences: individual risk for an hypothetical person (an individual worker). 125
Table D.2	Illustrative ranges of target harmful event frequencies for specified consequences: group risk for workers or members of the public 125
Table D.3	Illustrative target harmful event frequencies for specified consequences: environmental risk per receptor from all hazardous events at the whole establishment 130
Table D.4	Illustrative ranges of target harmful event frequencies for specified consequences: asset risk 131
Table E.1	Reliability analysis for Example 1 133
Table E.2	LOPA worksheet for Example 1 137
Table E.3	Harmful event frequencies for specified consequences (with respect to Figure E.4) 141

1 INTRODUCTION, SCOPE AND APPLICATION

1.1 INTRODUCTION

Most process plants are controlled by complex process control systems; there is increasing dependence on safety instrumented systems (SISs) to carry out safety instrumented functions (SIFs).

After applying inherently safer design (ISD) principles to the fundamental process plant design to eliminate hazards as the first priority, residual process plant hazards should be properly controlled and have effective risk reduction measures (RRMs) in place to achieve target risk levels. Equipment on the process plant and the process control system may provide some risk reduction, but these do not usually provide sufficient control for all the identified hazardous events. Consequently, to achieve target risk levels, and as part of a balanced approach to risk reduction, additional RRMs may be necessary. Such RRMs could include SISs to carry out SIFs. These are protection layers (PLs) that are intended to detect abnormal conditions on the process plant and prevent the hazardous event (PL(prevention)), or to mitigate the consequences of the hazardous event (PL(mitigation)). SISs comprise electrical, electronic or programmable electronic systems.

To achieve target risk levels, the approach should involve (in order of priority):

- Applying ISD principles (also in order of priority):
 - elimination of hazards, and
 - control and minimisation of risk at source using physical engineering controls (e.g. by increasing separation distances).
- Providing PLs (prevention) that reduce the specific hazardous event frequency (HEF). These may include systems and functions that are intended to detect abnormal conditions on the process plant and prevent the hazardous event.
- Providing PLs (mitigation) that mitigate the consequence of the specific hazardous event. These may include systems and functions that are intended to mitigate the consequences of the hazardous event.

For a specific hazardous event, the objective of SIL determination is to:

- Determine whether it is necessary to employ a SIS to carry out a specific SIF, where there is a shortfall in the risk reduction already achieved by RRMs to meet a target risk.
- Determine the SIL of the SIF where it has been determined that there is a shortfall in the risk reduction needed to meet the target risk.

An example of a hazardous event is 'Rupture of pressure vessel and release of flammable gas at high pressure leading to an extensive gas cloud.'

Whilst the guidance provided in this technical publication relates to the required performance of the SIFs to be implemented by PLs to prevent hazardous events or to mitigate the consequences of hazardous events, selecting SIFs and determining their performance requirements should be part of a balanced approach to risk reduction.

1.2 INDUSTRY CONTEXT

There is increasing dependence on SISs to carry out SIFs to achieve target risk levels (e.g. tolerable). Recent process industry incidents such as those occurring at petroleum refineries and bulk storage facilities have focused attention on several issues related to the design and maintenance of functional safety of SISs if the target risk levels are to be achieved.

1.3 SCOPE

This technical publication supports practical application of the following clauses of IEC 61511-1:

- clause 8 Process H&RA, and
- clause 9 Allocation of safety functions to protection layers.

It does so by providing guidance on:

- SIL determination of SIFs associated with SISs within the scope of IEC 61511.
- Identifying the SIFs to be carried out by one or more SISs.
- Illustrating several SIL determination methods available for ensuring that an appropriate SIL is selected for each SIF.
- The team-based workshop methodology.

Guidance is provided on some key principles and requirements for effective functional safety management (FSM), including:

- Setting a target risk comprising target harmful event frequencies for the specified consequences (e.g. safety and environment).
- Justifying the basis on which the target harmful event frequencies for specified consequences are set.
- Having a rational basis for claims made for the risk levels that are achieved.
- Ensuring that the assumptions relating to the risk reduction parameters that impact on the amount of risk reduction that is being claimed for a particular PL are based on robust evidence and are managed throughout the life of the process plant.

This technical publication focuses on quantitative and semi quantitative SIL determination techniques. It is, however, acknowledged that a qualitative approach to SIL determination may be appropriate, such as where there is available authoritative guidance on SIL determination that provides a rational basis for its target risk criteria. For more severe harmful event consequences, a quantitative and semi quantitative approach to SIL determination should be used.

Worked examples are provided to illustrate key points.

Excluded from the scope is guidance on other key steps of the SIS safety life cycle, from SIS design and engineering through installation and commissioning to decommissioning; for guidance, see *IEC 61511-2: Guidance on achievement, operation and maintenance of functional safety employing safety instrumented systems in support of IEC 61511*.