

AMERICAN NATIONAL STANDARD
ANSI/ISA-61511-3-2018 / IEC 61511-3:2016

**Functional Safety – Safety Instrumented
Systems for the Process Industry Sector –
Part 3: Guidelines for the determination
of the required safety integrity levels
(IEC 61511-3:2016, IDT)**

Approved 11 July 2018

ANSI/ISA-61511-3-2018 / IEC 61511-3:2016, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the determination of the required safety integrity levels (IEC 61511-3:2016, IDT)

ISBN: 978-1-945541-97-1

Copyright © 2016 IEC. Copyright © 2018 ISA. These materials are subject to copyright claims of IEC and ISA. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ISA. All requests pertaining to the ANSI/ISA-61511-3-2018 / IEC 61511-3:2016 Standard should be submitted to ISA.

ISA
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709
E-mail: standards@isa.org

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

Preface

This preface is included for information purposes only and is not part of ANSI/ISA-61511-3-2018 / IEC 61511-3:2016.

This standard has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of automation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, 67 T.W. Alexander Drive; P.O. Box 12277; Research Triangle Park, NC 277099; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards, recommended practices, and technical reports. The Department is further aware of the benefits of USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, the Department will endeavor to introduce SI and acceptable metric units in all new and revised standards to the greatest extent possible. The Metric Practice Guide, which has been published by the Institute of Electrical and Electronics Engineers (IEEE) as ANSI/IEEE Std. 268-1992, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all interested individuals in the development of ISA standards. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER. ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE

APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

CONTENTS

FOREWORD	11
INTRODUCTION	13
1 Scope	17
2 Normative references	18
3 Terms, definitions and abbreviations	19
Annex A (informative) Risk and safety integrity – general guidance	21
A.1 General	21
A.2 Necessary risk reduction	21
A.3 Role of safety instrumented systems	21
A.4 Risk and safety integrity	23
A.5 Allocation of safety requirements	24
A.6 Hazardous event, hazardous situation and harmful event	24
A.7 Safety integrity levels	25
A.8 Selection of the method for determining the required safety integrity level	25
Annex B (informative) Semi-quantitative method – event tree analysis	27
B.1 Overview	27
B.2 Compliance with IEC 61511-1:2016	27
B.3 Example	28
B.3.1 General	28
B.3.2 Process safety target	28
B.3.3 Hazard analysis	29
B.3.4 Semi-quantitative risk analysis technique	30
B.3.5 Risk analysis of existing process	31
B.3.6 Events that do not meet the process safety target	33
B.3.7 Risk reduction using other protection layers	34
B.3.8 Risk reduction using a safety instrumented function	34
Annex C (informative) The safety layer matrix method	37
C.1 Overview	37
C.2 Process safety target	39
C.3 Hazard analysis	39
C.4 Risk analysis technique	40
C.5 Safety layer matrix	41
C.6 General procedure	42
Annex D (informative) A semi-qualitative method: calibrated risk graph	45
D.1 Overview	45
D.2 Risk graph synthesis	45
D.3 Calibration	46
D.4 Membership and organization of the team undertaking the SIL assessment	48
D.5 Documentation of results of SIL determination	48
D.6 Example calibration based on typical criteria	48
D.7 Using risk graphs where the consequences are environmental damage	52

D.8	Using risk graphs where the consequences are asset loss.....	53
D.9	Determining the integrity level of instrument protection function where the consequences of failure involve more than one type of loss	54
Annex E (informative)	A qualitative method: risk graph	55
E.1	General	55
E.2	Typical implementation of instrumented functions	55
E.3	Risk graph synthesis	56
E.4	Risk graph implementation: personnel protection	57
E.5	Relevant issues to be considered during application of risk graphs	58
Annex F (informative)	Layer of protection analysis (LOPA)	61
F.1	Overview	61
F.2	Impact event.....	62
F.3	Severity level.....	62
F.4	Initiating cause	64
F.5	Initiation likelihood.....	64
F.6	Protection layers	65
F.7	Additional mitigation	65
F.8	Independent protection layers (IPL)	66
F.9	Intermediate event likelihood	66
F.10	SIF integrity level.....	67
F.11	Mitigated event likelihood	67
F.12	Total risk	67
F.13	Example	67
F.13.1	General.....	67
F.13.2	Impact event and severity level	67
F.13.3	Initiating cause	68
F.13.4	Initiating likelihood	68
F.13.5	General process design.....	68
F.13.6	BPCS	68
F.13.7	Alarms.....	68
F.13.8	Additional mitigation	68
F.13.9	Independent protection layer(s) (IPL)	69
F.13.10	Intermediate event likelihood.....	69
F.13.11	SIS.....	69
F.13.12	Next SIF.....	69
Annex G (informative)	Layer of protection analysis using a risk matrix	71
G.1	Overview	71
G.2	Procedure.....	73
G.2.1	General.....	73
G.2.2	Step 1: General Information and node definition	73
G.2.3	Step 2: Describe hazardous event	75
G.2.4	Step 3: Evaluate initiating event frequency	78
G.2.5	Step 4: Determine hazardous event consequence severity and risk reduction factor	79

G.2.6	Step 5: Identify independent protection layers and risk reduction factor	80
G.2.7	Step 6: Identify consequence mitigation systems and risk reduction factor	81
G.2.8	Step 7: Determine CMS risk gap	82
G.2.9	Step 8: Determine scenario risk gap	86
G.2.10	Step 9: Make recommendations when needed	86
Annex H (informative) A qualitative approach for risk estimation & safety integrity level (SIL) assignment		89
H.1	Overview	89
H.2	Risk estimation and SIL assignment	91
H.2.1	General	91
H.2.2	Hazard identification/indication	91
H.2.3	Risk estimation	91
H.2.4	Consequence parameter selection (C) (Table H.2)	92
H.2.5	Probability of occurrence of that harm	93
H.2.6	Estimating probability of harm	95
H.2.7	SIL assignment	95
Annex I (informative) Designing & calibrating a risk graph		99
I.1	Overview	99
I.2	Steps involved in risk graph design and calibration	99
I.3	Risk graph development	100
I.4	The risk graph parameters	100
I.4.1	Choosing parameters	100
I.4.2	Number of parameters	100
I.4.3	Parameter value	100
I.4.4	Parameter definition	101
I.4.5	Risk graph	101
I.4.6	Tolerable event frequencies (Tef) for each consequence	101
I.4.7	Calibration	102
I.4.8	Completion of the risk graph	103
Annex J (informative) Multiple safety systems		105
J.1	Overview	105
J.2	Notion of systemic dependencies	105
J.3	Semi-quantitative approaches	109
J.4	Boolean approaches	110
J.5	State-transition approach	113
Annex K (informative) As low as reasonably practicable (ALARP) and tolerable risk concepts		117
K.1	General	117
K.2	ALARP model	117
K.2.1	Overview	117
K.2.2	Tolerable risk target	118
Bibliography		120
Figure 1 – Overall framework of the IEC 61511 series		15

Figure 2 – Typical protection layers and risk reduction means	18
Figure A.1 – Risk reduction: general concepts	23
Figure A.2 – Risk and safety integrity concepts	24
Figure A.3 – Harmful event progression.....	25
Figure A.4 – Allocation of safety requirements to the non-SIS protection layers and other protection layers.....	26
Figure B.1 – Pressurized vessel with existing safety systems	28
Figure B.2 – Fault tree for overpressure of the vessel.....	31
Figure B.3 –Hazardous events with existing safety systems	33
Figure B.4 – Hazardous events with SIL 2 safety instrumented function	36
Figure C.1 – Protection layers	38
Figure C.2 – Example of safety layer matrix	42
Figure D.1 – Risk graph: general scheme	50
Figure D.2 – Risk graph: environmental loss.....	53
Figure E.1 – VDI/VDE 2180 Risk graph – personnel protection and relationship to SILs	57
Figure F.1 – Layer of protection analysis (LOPA) report	63
Figure G.1 – Layer of protection graphic highlighting proactive and reactive IPL	72
Figure G.2 – Work process used for Annex G	74
Figure G.3 – Example process node boundary for selected scenario	75
Figure G.4 – Acceptable secondary consequence risk	83
Figure G.6 – Managed secondary consequence risk	86
Figure G.5 – Unacceptable secondary consequence risk	83
Figure H.1 – Workflow of SIL assignment process	90
Figure H.2 – Parameters used in risk estimation.....	92
Figure I.1 – Risk graph parameters to consider	100
Figure I.2 – Illustration of a risk graph with parameters from Figure I.1	101
Figure J.1 – Conventional calculations	105
Figure J.2 – Accurate calculations	106
Figure J.3 – Redundant SIS.....	108
Figure J.4 – Corrective coefficients for hazardous event frequency calculations when the proof tests are performed at the same time	109
Figure J.5 – Expansion of the simple example	110
Figure J.6 – Fault tree modelling of the multi SIS presented in Figure J.5.....	111
Figure J.7 – Modelling CCF between SIS ₁ and SIS ₂	112
Figure J.8 – Effect of tests staggering	112
Figure J.9 – Effect of partial stroking	113
Figure J.10 – Modelling of repair resource mobilisation	114
Figure J.11 – Example of output from Monte Carlo simulation	115
Figure J.12 – Impact of repairs due to shared repair resources	116
Figure K.1 – Tolerable risk and ALARP	118

Table B.1 – HAZOP study results	30
Table C.1 – Frequency of hazardous event likelihood (without considering PLs)	40
Table C.2 – Criteria for rating the severity of impact of hazardous events	41
Table D.1 – Descriptions of process industry risk graph parameters	46
Table D.2 – Example calibration of the general purpose risk graph	51
Table D.3 – General environmental consequences	52
Table E.1– Data relating to risk graph (see Figure E.1)	58
Table F.1 – HAZOP developed data for LOPA	63
Table F.2 – Impact event severity levels	64
Table F.3 – Initiation likelihood	64
Table F.4 – Typical protection layers (prevention and mitigation) PFD_{avg}	65
Table G.1 – Selected scenario from HAZOP worksheet	76
Table G.2 – Selected scenario from LOPA worksheet	77
Table G.3 – Example initiating causes and associated frequency	79
Table G.4 – Consequence severity decision table.....	80
Table G.5 – Risk reduction factor matrix	80
Table G.6 – Examples of independent protection layers (IPL) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	82
Table G.7 – Examples of consequence mitigation system (CMS) with associated risk reduction factors (RRF) and probability of failure on demand (PFD)	82
Table G.8 – Step 7 LOPA worksheet (1 of 2)	85
Table G.9 – Step 8 LOPA worksheet (1 of 2)	87
Table H.1 – List of SIFs and hazardous events to be assessed	91
Table H.2 – Consequence parameter/severity level	92
Table H.3 – Occupancy parameter/Exposure probability (F)	93
Table H.4 – Avoidance parameter/avoidance probability	94
Table H.5 – Demand rate parameter (W)	95
Table H.6 – Risk graph matrix (SIL assignment form for safety instrumented functions)	96
Table H.7 – Example of consequence categories.....	96
Table K.1 – Example of risk classification of incidents	119
Table K.2 – Interpretation of risk classes	119

This page intentionally left blank.

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.