



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.04-2020, Part 1

Guidelines for the Implementation of ANSI/ISA-61511-1:2018

Approved 17 April 2020

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

ISA-TR84.00.04-2020, Part 1

Guidelines for the Implementation of ANSI/ISA-61511-1-2018

ISBN: 978-1-64331-102-9

Copyright © 2020 by the International Society of Automation (ISA). All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.04-2020, Part 1.

This document has been prepared as part of the service of the International Society of Automation (ISA) toward a goal of uniformity in the field of instrumentation and 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 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. 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 DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NONDISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NONDISCRIMINATORY.

ISA REQUESTS 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.

The following served as leaders and voting members of ISA84 in the development of this technical report, which was prepared by ISA84 Working Group 4.

NAME	AFFILIATION
Angela Summers, WG4 Co-Chair	SIS-TECH Solutions
David Bennett, WG4 Co-Chair	Worley
Rahul Bhojani, ISA84 Co-Chair	BP
Paul Gruhn, ISA84 Co-Chair	aeSolutions
Nicholas Sands, ISA84 Co-Mgr Director	DuPont
Dennis Zetterberg, ISA84 Co-Mgr Director	Chevron
Richard Dunn, ISA84 Vice Chair	DuPont
Nagappan Muthiah, ISA84 Secretary	Phillips 66
Tadaaki Ando	Yokogawa
Murli Balsubramanian	ExxonMobil
David Blackburn	Phillips 66
Iwan van Beurden	exida
Harry Cheddie	Cteris
Raju Chittilapilly	ONGC
KV Gandhi	KBR
Luis Garcia	Siemens
Ian Gibson	Consultant
James Harris	UOP
Farshad Hendi	Schneider Electric
Janardhanan Kallambettu	Bechtel
Palaniappan Kannan	Petroleum Development of Oman
Len Laskowski	Emerson
Donald Lyons	Valero
Edward Marszal	Kenexis
Marcelo Mollicone	SYM PCS
Ramon Morillo	Motiva Enterprises
Scott Mourier	Dow Chemical
Donatus Ogwude	Creative Systems International
Bhagyashree Pataskar	Covestro
Richard Roberts	Consultant
Michael Scott	aeSolutions
Peter Skipp	Rockwell Automation
William Vogtmann	Enterprise Products Partners
Arthur Woltman	Consultant

This technical report was approved for publication by the ISA Standards and Practices Board on 17 April 2020.

NAME	AFFILIATION
C. Monchinski, Vice President	Automated Control Concepts Inc
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc
E. Cosman	OIT Concepts, LLC

D. Dunn
J. Federlein
B. Fitzpatrick
J-P Hauet
D. Lee
G. Lehmann
T. McAviney
V. Mezzano
G. Nasby
D. Reed
N. Sands
H. Sasajima
H. Storey
I. Verhappen
D. Visnich
W. Weidman
J. Weiss
M. Wilkins
D. Zetterberg

WS Nelson
Federlein & Assoc LLC
Wood PLC
Hauet.Com
Emerson Automation Solutions
AECOM
Consultant
Fluor Corporation
City of Guelph Water Services
Rockwell Automation
DuPont Company
Fieldcomm Group Inc. Asia-Pacific
Herman Storey Consulting
Industrial Automation Networks
Burns & McDonnell
Consultant
Applied Control Solutions LLC
Yokogawa UK Ltd
Chevron Energy Technology Company

This page intentionally left blank.

Foreword

ANSI/ISA-61511-2018 Part 1 gives requirements for specification, design, installation, operation, maintenance, modification, and decommissioning. These requirements are presented in the standard using the safety lifecycle shown in ANSI/ISA-61511-2018 Part 1 Figure 7 and described in ANSI/ISA-61511:2018 Part 1 Table 2.

The ISA84 committee has developed a series of complementary technical reports to provide guidance, as well as practical examples of implementation, on various topics and applications. Three of these technical reports, ISA-TR84.00.02, ISA-TR84.00.03, and ISA-TR84.00.04, provide informative guidance related to specific phases of the safety instrumented system (SIS) lifecycle. Figure 7 and Table 2 have been adapted for this foreword as shown in ISA-TR84.00.04 Figure 1.1 and Table 1.1, respectively. A brief overview of each technical report is given below, including the report's relationship to the life-cycle requirements and the intended scope of each report's guidance.

ISA-TR84.00.02—Safety Integrity Level (SIL) Verification of Safety Instrumented Functions—

Life-cycle phase 4 requires verification that the intended or installed SIS meets its specified SIL. To support the calculation of the average probability of failure on demand as required by ANSI/ISA-61511 Clause 11.9, ISA-TR84.00.02 provides guidance on the following: a) assessing random and systematic failures, failure modes, and failure rates; b) understanding the impact of diagnostics and automation asset integrity (AAI) activities on the SIL and reliability; c) identifying sources of common cause, common mode, and systematic failures; and d) using quantitative methodologies to verify the SIL and spurious trip rate. The approaches outlined in this document are performance-based; consequently, the reader is cautioned to understand that the examples provided do not represent prescriptive architectural configurations or AAI requirements for any given SIL. Once a SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured AAI program as described in ISA-TR84.00.03.

ISA-TR84.00.03—Automation Asset Integrity of Safety Instrumented Systems (SIS)—

Life-cycle phases 5 and 6 involve the installation and testing of the SIS, the validation that the SIS meets the safety requirements specification, and the assurance that functional safety is maintained during long-term operation and maintenance. An important aspect of achieving and maintaining the SIS integrity and its specified SIL is the implementation of an AAI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective AAI program that demonstrates through traceable and auditable documentation that the SIS and its equipment are maintained in compliance with the safety requirements specification. The technical report addresses the identification of personnel roles and responsibilities when establishing a plan, important considerations in establishing an effective AAI program, and detailed examples to illustrate user work processes used to support various activities of the AAI program. Data and information collected as part of the AAI program can be used to validate the SIL verification calculations as discussed in ISA-TR84.00.02 and the selection and continued use of devices as discussed in Annex L in this technical report.

ISA-TR84.00.04—Guidelines for the Implementation of ANSI/ISA-61511—

Life-cycle phases 2, 4, 9, and 10 address the management of functional safety, allocation of safety functions to protection layers, SIS design and engineering, and SIS verification. This technical report is divided into two parts. Part 1 provides an overview of the SIS lifecycle with references to annexes containing more detailed guidance on various subjects. Part 2 provides an end-user example of “how to” implement ANSI/ISA-61511. This report covers many aspects of the safety lifecycle, including such topics as: “grandfathering” existing SISs (Clause 3 and Annex A); operator-initiated functions (Annex B), separation of the basic process control system (BPCS) and SIS (Annex F), field device and logic solver selection (Annex L), manual shutdown considerations (Annex P), and design/installation considerations (e.g., wiring, power, relationship to BPCS, common mode impacts, fault tolerance, etc. – Annex N). ISA-TR84.00.02 expands Annex G in this technical

report, which only provides a brief introduction to the topic of failure calculations. ISA-TR84.00.04 does not address the AAI program, which is discussed in ISA-TR84.00.03.

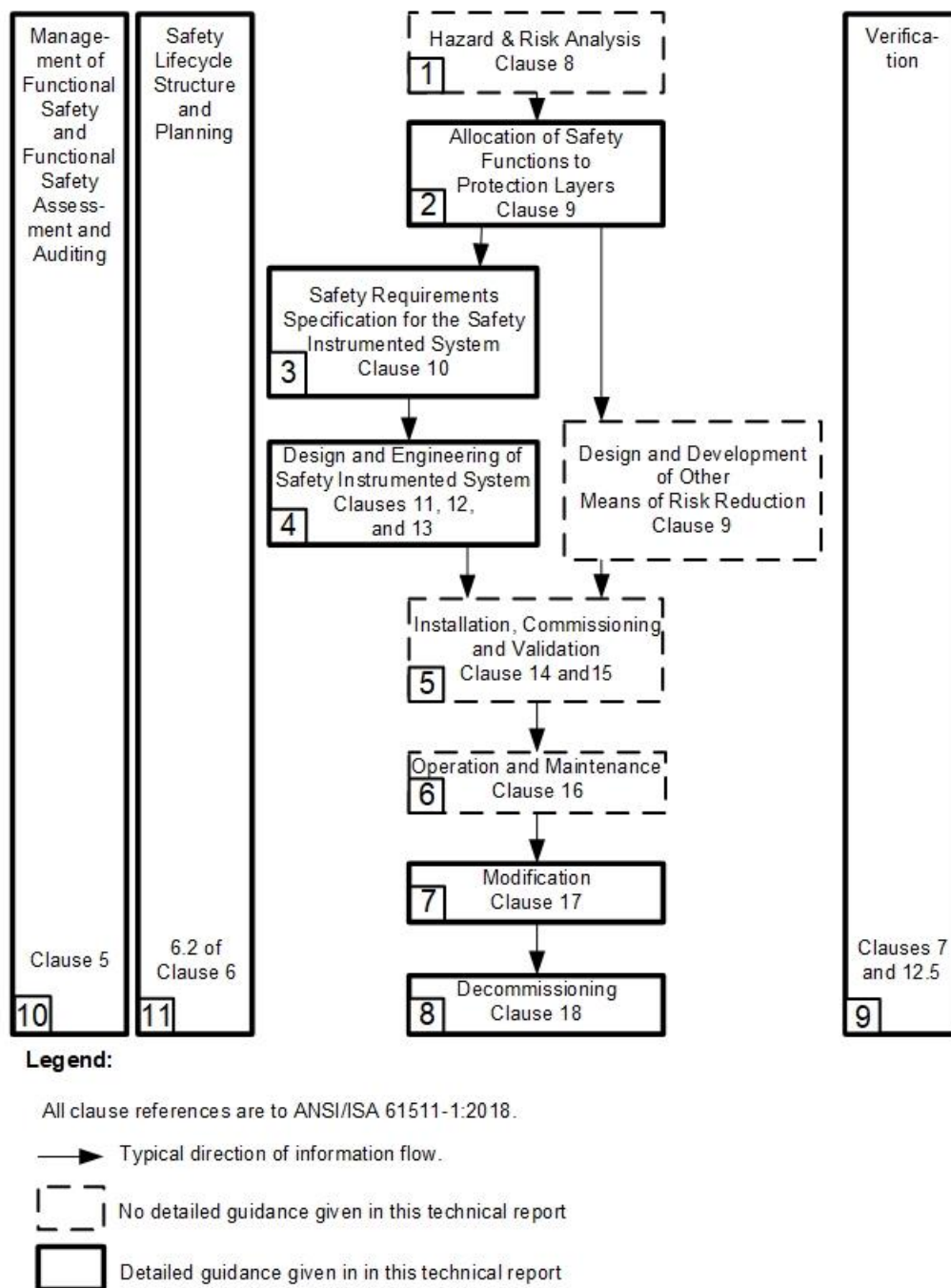


Figure 1.1 – SIS safety lifecycle (modified ANSI/ISA-61511-1:2018 Figure 7)

Table 1-1– SIS Safety Life Cycle overview (modified ANSI/ISA-61511-1:2018 Table 2)

(1 of 2)

Safety Life-cycle Phase or Activity		Objectives	ANSI/ISA-61511:2018 Requirements Clause	ISA84 Technical Report Reference
Figure 7 box number	Title			
1	Hazards and Risk Assessment (H&RA)	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	None
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	9	ISA-TR84.00.04 Annexes B, F, and J
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	10	No specific guidance on documenting the SRS. An example is shown in ISA-TR84.00.04 Part 2. All three technical reports (ISA-TR84.00.02, 03, and 04) provide fundamental considerations for SRS development.
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	11, 12	ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q ISA-TR84.00.02
5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and their associated safety integrity	14, 15	ISA-TR84.00.03
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	ISA-TR84.00.03

(Table 1 continued from previous page)

(2 of 2)

Safety Life-cycle Phase or Activity		Objectives	ANSI/ISA-61511:2018 Requirements Clause	ISA84 Technical Report Reference
Figure 7 box number	Title			
7	SIS modification	To make corrections, enhancements, or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	17	Apply appropriate safety life-cycle phase during management of change activity
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remains appropriate	18	Apply appropriate safety life-cycle phase during project execution
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.5	ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02
10	SIS FSA	To investigate and arrive at a judgement on the functional safety achieved by the SIS	5	ISA-TR84.00.04 Clause 3 and Annexes A, C, D, E, and S
11	Safety life-cycle structure and planning	To establish how the life-cycle steps are accomplished	6.2	ISA-TR84.00.04 Annex C

CONTENTS

1	Purpose	15
2	Introduction	15
3	Existing SIS	16
4	Overview	17
4.1	Life-cycle approach	18
4.2	Define a risk-management strategy	18
4.3	Implement the strategy	20
4.3.1	Independence	20
4.3.2	Programmable logic controllers (PLC)	21
4.3.3	User-approved devices.....	21
4.3.4	Response time	21
4.3.5	Support system considerations	21
4.3.6	Verification	22
4.3.7	Proof testing.....	22
4.4	Validate, startup, operate, and maintain the strategy	22
4.5	Manage changes to the strategy	24
5	Acronyms and abbreviations	25
	Annex A Example Methods for Evaluating the Existing SIS	29
	Annex B Alarms and Alerts from the SIS.....	35
	Annex C Management of Functional Safety: Organization and Resources	45
	Annex D Verification, Validation, and Functional Safety Assessments	51
	Annex E Functional Safety Management System Audits	63
	Annex F BPCS and its Relationship to the SIS	75
	Annex G Failures – Types, Classifications, Sources and Strategy for Defense	85
	Annex H SIF versus Interlocks, Permissives, and Inhibits	97
	Annex I Continuous, High, and Low Demand Mode.....	103
	Annex J SIL 4 versus Inherently Safer Design	111
	Annex K Fault Tolerance Topics	113
	Annex L Device Selection	119
	Annex M General Purpose versus Safety Logic Solvers	139
	Annex N Design Guidance	143
	Annex O Application Programming	157
	Annex P Response to Detection of a Dangerous Fault.....	161
	Annex Q Instrumented Safeguard Setpoint Guidance	169
	Annex R Key Performance Indicators	187
	Annex S Safety Manual	191
	Annex T References	195

Figures

Figure 1.1 – SIS safety lifecycle (modified ANSI/ISA-61511-1:2018 Figure 7)	8
Figure B.1 – Example of safety alarm system architecture	39
Figure B.2 – Safety alarm system for increasing process variable with operator action via HMI	42
Figure B.3 – Detail of safety alarm for increasing process variable and manual final control element.....	43
Figure D.1 – Relative cost of design changes as a function of project phase	53
Figure F.1 – Protection layers (ANSI/ISA-61511-1:2018, Figure 9)	77
Figure F.2 – Comparative risk reduction for shared field devices. Lower PFD values provide more risk reduction	84
Figure G.1 – Breakdown of failure classifications	87
Figure G.2 – Venn diagram of failure classifications	88
Figure G.3 – Venn diagram showing the probability of failure on demand for each failure classification	90
Figure G.4 – Venn diagram showing the probability of failure on demand for each failure classification	90
Figure G.5 – Primary cause of failure by lifecycle phase	92
Figure G.6 – Improving the overall quality, the configuration, and the availability of a safety protection layer can help to reduce systematic and random failures	94
Figure H.1 – Definition of safety instrumented system and safety instrumented function	100
Figure I.1 – Case 1 example graphic	107
Figure I.2 – Case 2 example graphic	108
Figure I.3 – Case 3 example graphic	108
Figure I.4 – Case 4 example graphic	109
Figure L.1 – Work process for selecting devices	123
Figure L.2 – Evidence supporting user approval	130
Figure Q.1 – IPL operating region with overall safety factor	171
Figure Q.2 – IPL response time with IPL safety factors	172
Figure Q.3. – Elements of sensor response time.....	173
Figure Q.4. – Elements of logic solver response time	174
Figure Q.5. – Elements of final control element response time with automatic actuation	175
Figure Q.6 – Result of not adjusting design for process lag	176
Figure Q.7 – Adjusting final element closure limit for process lag	177
Figure Q.8 – Adjusting final element closure limit for process lag and TSU	178
Figure Q.9 – Applying response time safety factor and determining MSP	179
Figure Q.10 – Setpoint specification relationships	180
Figure S.1 – Types of information forming safety manual content	191

Tables

Table 1-1– SIS Safety Life Cycle overview (modified ANSI/ISA-61511-1:2018 Table 2)	9
Table A.1 – Example of mapping prior design practice classification to SIL	32
Table C.1 — Example roles and responsibilities matrix.....	47
Table C.2 – Examples of experience or skills for the disciplines in Table C.1	49
Table D.1 – Purpose of relative timing of FSAs.....	53
Table E.1 – Functional safety audit focus topics and key input documents	65
Table E.2 – Example functional safety audit interview questions.....	67
Table G.1 – Key differences between random and systematic failures	86
Table J.1 – Checklist for evaluating feasibility of SIL 4 SIS.....	112
Table L.1 – Equipment approval form	134
Table N.1 – Fault types	147
Table N.2 – Diagnostic tests for programmable electronics.....	149
Table R.1 – Example indicators related to safety instrumented systems (SIS)	188

1 Purpose

This technical report provides discussion on various topics associated with ANSI/ISA-61511-1-2018 Parts 1-3 and includes examples of practical ways to implement the standard. This technical report is informative and provides nonmandatory methods or techniques.

There is nothing in this technical report that precludes, replaces, or makes obsolete any requirement of ANSI/ISA-61511-2018 Part 1.

2 Introduction

In the United States of America, the Occupational Safety and Health Administration (US-OSHA) regulation, 29 CFR 1910.119 (OSHA 1910.119), requires the identification and management of the instrumented systems responsible for safe operation. ISA Standards Panel 84 (ISA84) developed ANSI/ISA-84.01-1996 to define how to manage safety instrumented systems (SIS) using a life-cycle approach. The standard provided a formal, documented process for addressing the design, operation, maintenance, testing, and management of change for SIS. The efforts of the ISA84 committee resulted in US-OSHA recognizing ANSI/ISA-84.01-1996 as representing good engineering practice for SIS.

During its initial development, the ISA84 committee relied on existing US functional safety practices, such as those documented in OSHA 1910.119 and by the Center for Chemical Process Safety (CCPS) "*Guidelines for the Safe Automation of Chemical Processes*." Working in parallel to the ISA84 committee effort, the International Electrotechnical Commission (IEC) was developing IEC 61508. Concepts introduced in the draft international standard were incorporated into ANSI/ISA-84.01-1996, resulting in ANSI/ISA-84.01-1996 being accepted as the US functional safety standard for the process industry sector. Through ANSI/ISA-84.01-1996, owner/operators have become familiar with terms such as safety integrity levels, safety instrumented systems, and safety instrumented functions.

Since 1996, some countries have utilized ANSI/ISA-84.01-1996, while others have used their own national standard or adopted IEC 61508 when it was released in 1999. In an era where design, engineering, and operation can occur in multiple countries, this diversity of standards resulted in an immediate need for an international, consensus process industry sector standard.

The IEC 61511 committee was formed to specifically address SIS in the process industry sector. IEC 61511 is the process industry sector implementation of the basic safety standard, IEC 61508. The first edition of IEC 61511 was published in 2003. IEC 61511 was adopted by the ISA84 committee with one modification and published as ANSI/ISA-84.00.01-2004 (IEC 61511 Mod). Over time, the terminology and the technical clauses used within IEC 61511 have evolved to better support effective application in the process industry sector. The second edition of IEC 61511 was issued by IEC in 2016. After an amendment was integrated into IEC 61511-1, the ISA84 committee accepted IEC 61511-1 as ISA-61511-1 in 2017. ANSI approved the new standard as ANSI/ISA-61511-1:2018.

This guideline is divided into two parts:

- Part 1 provides guidance on a wide range of topics related to the standard.
- Part 2 provides a single user example to illustrate some of the life-cycle steps in ANSI/ISA-61511:2004.

ISA-TR84.00.04 Part 1 (ISA-TR84.00.04-1) contains four main clauses.

- Clause 1 is the purpose.
- Clause 2 explains the history of the standard and discusses its relationship to other regulations, standards, and practices.

- Clause 3 and Annex A specifically address the determination of whether an existing SIS is designed, maintained, inspected, tested, and operating in a safe manner.
- Clause 4 provides an overview of the SIS lifecycle and references to subject-specific annexes for additional guidance on key issues.

3 Existing SIS

The concept of “grandfathering” originated with OSHA 1910.119. The intent of “grandfathering” is to recognize that installed equipment implemented in accordance with previously published practices may provide sufficient safety integrity without upgrading to the latest requirements of the ANSI/ISA-61511-1:2018. The equipment may remain “as is” until the user determines that the equipment is no longer meeting the functional and safety integrity requirements.

NOTE 1 For more detail, see OSHA 29 CFR 1910.119 (d) (iii)

NOTE 2 There are many chemical industrial processes that are not covered under OSHA 1910.119. Some owner/operators choose to manage these processes under the same program as their covered processes. The discussion in this section is considered applicable to noncovered process SISs.

NOTE 3 US-OSHA has published guidance on the interpretation of the OSHA 1910.119 grandfather clause with regard to the Process Safety Management program (Refer to Appendix C to 1910.119 – Compliance Guidelines and Recommendations for Process Safety Management (Nonmandatory) and in various compliance letters published on www.OSHA.gov). The guidance provided in this clause and Annex A in this technical report is intended to supplement the US-OSHA guidance and to provide examples of methodologies that various owner/operators are using to determine whether their existing SIS is acceptable as is.

NOTE 4 Where ANSI/ISA-61511-1:2018 is applied outside of the US, the user should look into the country-specific or company-specific requirements around existing SISs.

ANSI/ISA-61511-1:2018 provides the requirements for the continued use of existing SISs as part of the functional safety management system. As part of the rationale, the user is required to have a process for gathering data on SISs and their equipment. The user then makes a judgement on whether the equipment remains fit for purpose based on this data. This documented assessment of the suitability of the equipment in SISs based on previous operating experience in similar operating environments is defined as “prior use.”

ANSI/ISA-61511-1:2018 Clause 5.2.5.4 states: *“For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard, the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.”*

The existing systems clause provides the basis for justifying the continued use of the installed equipment—the owner/operator of the SIS should determine that the “equipment is designed, maintained, inspected, tested, and operating in a safe manner.” The elements of this determination are incorporated in functional safety management system requirements contained in ANSI/ISA-61511-1:2018 Clauses 5 through 7. The determination relies on information that is gathered during the operation and maintenance of the process and the equipment that controls its safe operation and on a comprehensive review of the existing SIS installation.

The determination of the acceptability of an existing SIS should confirm the following:

- 1) Management practices fulfill the functional safety management requirements for the SIS lifecycle and are sufficient to ensure that the SIS achieves the required functional and safety integrity requirements for all relevant operating modes of the process.

NOTE The functional safety management system applies to existing and new SISs. Prior practices should consider all aspects of ANSI/ISA-61511-1:2018 Clause 5. The functional safety management system, including documentation, assessment, verification, validation, response to detected failure, and management of change, is necessary to identify and prevent random and systematic failures, which impact the safety integrity of the SIS.

- 2) The design of the existing SIS meets the requirements of the previous practice.

NOTE Where the existing SIS is not implemented in accordance with the previous practice, it should not be accepted as is, unless the identified deviations result in equivalent (or higher) safety integrity than the previous practice.

- 3) A hazard and risk analysis, fulfilling Clause 8 and 9 requirements, has determined qualitatively or quantitatively the level of risk reduction needed for each safety instrumented function (SIF) in the SIS.
- 4) An assessment of the existing SIS demonstrates that its design and management is sufficient to achieve the required risk reduction for each SIF.

NOTE The evaluation of the SIF should take into account various factors that affect the probability of random and systematic failure. Consideration should be given to the remaining design life of the equipment, with increasing probability of failure in aging equipment. Refer to ISA-TR84.00.02 for more guidance on analyzing the impact of random and systematic failure on the claimed risk reduction.

- 5) An assessment of the demand rate for each SIF during actual operation agrees with the assumptions made during risk assessment when the risk reduction requirements were determined.

NOTE Where the reliability parameters of the SIS do not agree with the design assumptions, corrective action should be taken to address the performance gap.

- 6) Evaluation of the prior use information demonstrates that the reliability parameters of the SIS are in accordance with those assumed during the original design.

NOTE Where the reliability parameters of the SIS do not agree with the design assumptions, corrective action should be taken to address the performance gap.

- 7) Evaluation of the prior use information demonstrates that systematic failures are sufficiently managed in accordance with the risk reduction claimed for the SIS.

- 8) SIS documentation meets the requirements of ANSI/ISA-61511-1:2018 Clause 19.

NOTE Documentation associated with the SIS should be in compliance with the functional safety management lifecycle to ensure adequate demonstration of continued safe operation.

Various considerations related to the timing of the reviews are discussed in Annex A.2 in this technical report.

The existing systems clause allows the owners/operators to maintain SIS equipment as is, when they can demonstrate these criteria. Over time, modifications to the existing SIS or its equipment should comply with ANSI/ISA-61511-1:2018. Modifications may be triggered for many reasons, such as the need to substitute a new technology to improve reliability, upgrade to the latest version device due to obsolescence of the previous generation, or to deal with aging equipment exhibiting a higher failure rate. For example, a site's automation asset integrity (AAI) program should reevaluate the frequency of asset integrity activities for equipment approaching the end of its useful life. As equipment enters wear-out, the equipment performance can be expected to degrade due to hardware, software, and support infrastructure issues. Additional guidance on the AAI program for equipment used to execute safety functions can be found in ISA-TR84.00.03. Refer to Annex A in this technical report for additional guidance and considerations for evaluating when modifications to the process or the SIS become significant enough to warrant reassessment of the adequacy of the SIS and the acceptability of maintaining the SIS as is.

4 Overview

ANSI/ISA-61511-1:2018 provides an extensive set of requirements covering the SIS lifecycle. Some specialized functions are also covered by industry practices that dictate unique requirements for specific applications. The standard relies on a quality control and quality assurance process to confirm that the SIS achieves the performance necessary to adequately reduce potential risk in the operating environment. The performance target for this quality process is defined in the standard as the SIL, which is related to the SIF's average frequency of failure (i.e., abbreviation is PFH for probability of failure per hour) or average probability of failure on demand (PFD_{avg}). The standard establishes four discrete ranges for benchmarking the performance of each function in

the SIS, where SIL 1 meets the minimum target failure measure (highest PFH or PFD_{avg}) and SIL 4 meets the highest target failure measure (lowest PFH or PFD_{avg}).

Achieving these performance ranges requires that the SIS be rigorously designed, constructed, and managed. An effective management system uses a rigorous approach to manage the risk throughout the process equipment life. With early consideration of process hazards, the SIS can be tailored to meet operating, maintainability, and reliability goals. Safe and reliable operation requires that the process design, SIS design, and operation and maintenance procedures be implemented to achieve both high integrity and reliability. Finally, the management strategy should incorporate periodic assessments of the reliability parameters for existing equipment to determine whether the equipment as installed provides the necessary risk reduction, thus assuring safe and reliable operation. Refer to ISA-TR84.00.03 for more guidance on the AAI program and to ISA-TR84.00.02 for more guidance on the reliability parameters.

4.1 Life-cycle approach

ANSI/ISA-61511:2018 covers a wide range of chemical process operations. Due to its broad scope, the standard has many general requirements addressing the complete lifecycle of the SIS, starting with the identification of SIS requirements in the risk assessment and ending when the SIS is decommissioned. While there are many different ways of representing the lifecycle, a simple four-step approach can be followed:

- 1) Define a risk-management strategy—establish a management system to address how SISs are identified, designed, inspected, maintained, tested, operated, and modified to achieve safe operation, and perform a hazard and risk analysis to identify where SISs are needed and their target SIL.
- 2) Implement the strategy—develop a design basis to achieve the target SIL and execute the detailed design to meet the requirements.
- 3) Validate, startup, operate, and maintain the strategy—implement the SIS following the design basis and detailed design documentation and define what is required of operation and maintenance personnel to sustain the SIL.
- 4) Manage changes to the strategy—ensure the SIS meets the target SIL by monitoring operation, inspection, test, and maintenance records and making changes as necessary to sustain its performance.

The life-cycle approach can be used to address any risk, whether safety, environmental, asset, or business related. Many governments require the use of recognized good engineering practices in the design and management of the instrumented systems that maintain safe and reliable operation in the process industry. Local regulations, applicable codes, or insurance practices may require the use of specific good engineering practices. Consequently, the management strategy should incorporate current good engineering practices and continuous improvement activities to provide a comprehensive program. Annexes C, D, and E in this technical report provide additional guidance on aspects of the management of functional safety. Additional guidance on applying SIS, as well as instrumented protective systems, can be found in *CCPS Guidelines for Safe and Reliable Instrumented Protective Systems*, published in 2007 and *CCPS Guidelines for Safe Automation of Chemical Processes*, published in 2016.

4.2 Define a risk-management strategy

The need for a SIF may be identified by a variety of methods, including internal practice, accepted industry practices, such as NFPA 85 or API 14C, or a process hazard analysis (PHA). While some industry practices mandate the use of SIF, they do not always identify the risk reduction requirements for the SIF, or the SIL for the SIS. There are multiple methods that can be used to determine the risk reduction requirements:

- Layers of protection analysis (LOPA)

- Risk graph
- Risk matrix
- Event tree analysis
- Fault tree analysis
- Bow tie analysis
- Quantitative risk analysis

ANSI/ISA-61511-3:2018 provides a series of examples to illustrate these methods. In addition, the Center for Chemical Process Safety (CCPS) has published multiple books on hazard evaluation and risk analysis. The following CCPS books are frequently cited by users as the basis for their risk management program and risk assessment procedures:

- *Guidelines for Auditing Process Safety Management Systems*
- *Guidelines for Chemical Process Quantitative Risk Analysis*
- *Guidelines for Engineering Design for Process Safety*
- *Guidelines for Preventing Human Error in Process Safety*
- *Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis*
- *Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis*
- *Inherently Safer Chemical Processes: A Life Cycle Approach*
- *Guidelines for Developing Quantitative Safety Risk Criteria*
- *Layer of Protection Analysis: Simplified Process Risk Assessment*
- *Guidelines for Safe Automation of Chemical Processes*

Part of risk allocation is the determination of how much risk reduction is being allocated to the operator in responding to alarms and fault detection. Understanding the time available for operator response, the number of problems that can present themselves concurrently, and the complexity of the decisions to be made can significantly limit the operator effectiveness in responding to process safety events. ANSI/ISA 61511-1 does not contain requirements related to these issues. Refer to ANSI/ISA 18.2 for requirements on alarm management and the ISA 18.2 series technical reports for guidance on many issues that impact alarm system effectiveness.

The risk allocation process may determine that the SIF can be manually initiated, automatically initiated, or both manually and automatically initiated. In other words, the SIS can be designed to execute its allocated SIFs automatically when specified process conditions occur, and/or the SIF can be manually activated based on operator observation, alarm, or procedure. The requirements for manual shutdown are defined as part of the SRS (ANSI/ISA 61511-1:2018 Clauses 10.3.2 and 11.2.8).

The alarm should be subjected to alarm management in accordance with ANSI/ISA 18.2, whether the operator response is to initiate manual shutdown or to manually activate a SIF. The alarm annunciation triggering the operator action to initiate the SIF may or may not be generated by the SIS depending on the site's risk management strategy. Whether in the BPCS or SIS, the alarm annunciation would be considered safety related and managed under process safety management in all cases where the operator response to the alarm is intended to provide risk reduction for a process safety event. Annex B in this technical report provides further guidance on different types of safety-related alarms.

The user needs to verify that the SIS meets the requirements of ANSI/ISA-61511-1:2018 when allocating safety functions and risk reduction to the SIS. The allocated risk reduction determines

the safety integrity level (SIL) requirement. Typically, in the process industry the SIL for the SIS is in the range of SIL 1 through SIL 3. When the SIF is manually activated, the SIL claim is limited by the alarm system and operator response effectiveness. Refer to Annex B in this technical report for more guidance on manually initiated SIFs and manual shutdowns initiated in response to alarms.

If the analysis identifies a need for a SIL 4 SIF, the user should consider more advanced analysis techniques to verify that the design and management of the SIS meets the safety integrity requirements. Refer to Annex J in this technical report for more information.

The demand rate can have a significant impact on the SIF design. Where a demand is placed on the SIF more than once per year, the design requirements for high demand and continuous mode need to be applied. Annex I in this technical report provides guidance on how to determine whether a SIF operates in low demand, high demand, or continuous mode.

The risk-reduction strategy should also address secondary or collateral consequences associated with the operation of the IPLs, such as reduced production, shutdown, and flaring. Secondary or collateral consequences can be thought of as the side effects of the risk-reduction strategy. Each time an IPL takes action, there is an effect on the process. Determine the cost of the spurious operation of IPLs to establish the maximum acceptable spurious activation rate. The final risk-reduction strategy should ensure that the costs and risks associated with spurious operation are understood and acceptable to operations.

4.3 Implement the strategy

The SIS functionality should be documented in a design basis that is maintained under revision control as process safety information for the life of the system. The SIS design basis should address the following:

- detection of and response to potentially hazardous events
- selection of equipment based on a user approval process (see Annex L in this technical report)
- fault detection, such as diagnostics and proof testing
- fault tolerance against dangerous failures
- procedures for maintenance and testing, including the use of bypasses (refer to ISA-TR84.00.03 for additional guidance)
- operation and maintenance procedures required when SIS equipment is out of service
- emergency shutdown capability if the SIS fails to take action as expected
- startup and shutdown of the process equipment

The SIS design basis is covered by ANSI/ISA-61511-1:2018 (Clauses 10 through 12). ISA-TR84.00.04-1 gives guidance on design requirements for the hardware in Annex N and software in Annex O. Uniform facility practices should be considered to promote consistency in SIS implementation, as well as to reduce training costs and the potential for human error.

4.3.1 Independence

If it is intended not to qualify the BPCS to this standard, then the SIS should be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised (ANSI/ISA-61511-1:2018 Clause 11.2.4). The potential for common cause, common mode, and systematic errors, which could result in a process demand and failure of the SIS, should be considered in any assessments of the basic process control system (BPCS) and SIS, including but not limited to equipment technology, equipment design, operations, installation, maintenance, testing, security, and management of change. Annex F in this technical report provides guidance with respect to the role of the BPCS in process safety.

4.3.2 Programmable logic controllers (PLC)

PLCs are complex integrated systems with the potential for large numbers of random and systematic failures. Because of the failure potential, ANSI/ISA-61511-1:2018 (Clause 11.5) requires safety configuration of PLCs for SISs. Safety configuration addresses the widely known failure modes of the inputs, main processors, communications, utilities (e.g., power, instrument air), and outputs. This requires diagnostics and fault-tolerance capabilities that are generally not provided in process control but are needed to identify and manage PLC failures in safety applications. Annex M in this technical report provides further discussion of general-purpose, safety-configured, and IEC 61508-compliant programmable electronic (PE) logic solvers.

4.3.3 User-approved devices

A user approval process should assure that field equipment has an established history of performance in a similar operating environment and that its failure mechanisms are understood and accounted for in the design, operation, and AAI practices. Annex L in this technical report provides guidance on the selection of SIS devices. A SIS should be sufficiently robust to meet the required SIL in the intended operating environment. For each installation, define the environmental conditions that impact SIS equipment selection, such as:

- process composition, e.g., solids, salts, or corrosives
- process operating conditions, e.g., extremes of temperature, pressure, or vibration
- external conditions, e.g., winterization needs, hazardous area classification, or electromagnetic interference

4.3.4 Response time

The SIS is designed to detect the unacceptable process condition and to respond in time to prevent the hazardous event from occurring. How much time the SIS has to respond depends on the process dynamics and the conditions initiating its actions. When multiple engineered safeguards are implemented to address an event, they are often designed to operate in series in a preferred sequence. While the process safety time starts at the deviation that initiates the hazard and ends when the hazardous event would occur if no safeguards intervene, the response time specified for any given safeguard starts when that safeguard is required to take action and ends when that safeguard can no longer prevent or mitigate the hazardous consequence. In many applications, it is desirable that each safeguard be capable of completing its action prior to the initiation of the next in the sequence; the goal being to achieve or maintain a safe state with the safeguard that causes the least impact to process operation.

The SIS begins protective action at a defined process condition or setpoint. Annex Q in this technical report provides guidance on the selection of SIF setpoints. The SIS's speed of response is limited by the sensor dynamics and overall instrument loop response time, which can be significantly affected by the process design itself. The shutdown lag can be long (seconds to minutes), particularly in applications where there is significant retained mass or energy. It can also be short (milliseconds), such as stopping a motor. The SIS should be capable of completing its action within its specified response time.

4.3.5 Support system considerations

Assess potential common causes in the process support systems, such as heat tracing, power, communications, instrument air, cooling water, and hydraulic power. Annex K.3.3 in this technical report provides additional guidance on support system requirements. Ensure that SIS support systems are designed to take the affected equipment to a specified safe state as necessary to achieve the required integrity. Approval of non-fail-safe design should consider the impact on the risk-reduction strategy assumptions, the type of SIS, the support system integrity, and alternative means to achieve a safe state. Human and cyber access to any SIS should be sufficiently restricted using administrative procedures and physical means to ensure that changes to the SIS are approved through a management of change process.

4.3.6 Verification

ANSI/ISA-61511-1:2018 Clause 11.9 requires that the SIS PFD_{avg} (or PFH) be verified quantitatively (refer to ISA-TR84.00.02 for additional guidance on SIL verification). Ensure that the selected equipment is fit for use in the operating environment and SIS application, that the subsystems meet minimum fault-tolerance requirements, and that the system achieves the required functionality and integrity. Annex K in this technical report provides further discussion on fault tolerance. SIS equipment should be included in an AAI program that seeks to maintain the SIS in compliance with the safety requirements specification. AAI includes a variety of activities, such as inspection, maintenance, calibration, repair/replacement, and proof testing. An equipment list should be maintained that identifies SIS equipment by a unique designation and includes the required inspection and proof-test interval necessary to ensure the equipment remains fit for service.

4.3.7 Proof testing

The AAI program is discussed in detail in ISA-TR84.00.03. Asset integrity includes many activities that are intended to sustain the performance of the equipment, such as inspection, preventive maintenance, proof testing, and scheduled replacement/rebuild. The determination of the proof-test interval is impacted by the offline test opportunities, relevant regulations, equipment history in similar operating environments, manufacturer's recommendations, and integrity requirements.

When proof testing is required more frequently than scheduled outages, on-line proof-test and repair facilities will be necessary. If the on-line activity requires bypassing, document the measures or safeguards put in place to compensate for the loss of SIS capability during the out-of-service period. Assess bypass activities and potential hazards to define the compensating measures and the maximum permitted repair time. Implement bypass alarms when practical. In all cases, ensure procedures adequately communicate to the operator that bypasses have been used, especially across shift changes. For example, consider formal handoff of a bypass log and/or a continuous bypass indication on the operator graphics. Ensure that operators know the state of SIS equipment and what to do if abnormal operation or SIS equipment failure occurs. Refer to Annex P in this technical report for more guidance on fault detection and response.

4.4 Validate, startup, operate, and maintain the strategy

The SIS undergoes validation to obtain formal acceptance of the SIS by appropriate stakeholders, including the operations staff and possibly other involved corporate and site support groups (e.g., automation, engineering, maintenance, quality control, tech service, and the safety, health, and environmental groups). An objective of validation is to ensure that the SIS as installed meets the intent of the hazard and risk analysis (H&RA) and the requirements of the SRS. After validation, changes to the SIS are reviewed and approved according to the plant's management of change practices. Validation is performed after instrument commissioning and loop checks have been completed and, where a PE logic solver is used, the application program has been installed. A validation plan is developed to ensure orderly execution of the validation process and that any findings are resolved and fully documented. Annex D in this technical report provides further discussion on conducting functional safety assessments during the validation phase of the SIS lifecycle.

Validation demonstrates that the installed SIS operates according to the SRS and determines that appropriate documentation is in place to support the SIS's long-term management. An input-to-output test is used to prove that the SIS functions properly and that the SIS equipment interacts as intended with other systems, such as the BPCS and operator interface. The site acceptance test (SAT) also provides an opportunity for a first-pass validation of the operating and maintenance procedures. Validation is completed prior to the initiation of any process operating mode where a hazardous event could occur that would require the operation of a new or modified SIS. It is a good practice to repeat validation after major changes to a SIS and also periodically, regardless of the history of the system (due to natural, normal degradation of hardware). In some cases, revalidation may be a good practice after turnarounds or long process outages.

The operator's response to abnormal operation is defined by operating procedures, which should include the expected actions for SIS alarms, SIS trips, and compensating measures. These procedures should clearly define the "never exceed limits," the consequences of deviating from these limits, and the proper action(s) to take when these limits are exceeded. The operating procedures should accurately describe the operator response requirements for SIS alarms and compensating measures. Annex P in this technical report provides application guidance regarding system behavior on detection of a fault. ANSI/ISA-61511-1:2018 Clause 16 addresses operating and maintenance procedure requirements for SISs. Procedures should include:

- a description of the hazardous events being addressed by the SIS
- a description of the SIS functionality
- the required operator response to detected SIS equipment failure and provisions for continued operation with detected faults (i.e., compensating measures)
- coordination, communication, and documentation of any troubleshooting, repair, or test activity between operations and maintenance
- conditions under which it is safe to reset the SIS
- use of startup bypasses and the process conditions to be monitored during startup
- use of maintenance bypasses and compensating measures for SIS repair and test
- the expected operator response when alarms from the SIS are received, and the setpoints for those alarms
- trip setpoints, the expected safe state when a trip is completed, and the form of trip notification (if provided)
- expected operator actions if a safe state is not achieved
- the "never exceed limit" for the process conditions that require manual shutdown

Installed safety equipment is subject to the same operational stresses as control equipment. However, when control equipment fails, the failure can be detected because the process behaves abnormally. In contrast, safety equipment typically operates on demand only, i.e., when an abnormal condition occurs, so failure may not be detected until the equipment is required to act. Equipment often demonstrates a failure rate over time that follows a so-called bathtub curve.

Early failures are often caused by manufacturing, assembly, test, installation, and commissioning errors. Many early failures are the result of rough handling, improper preinstallation storage, and poor installation practices. Rigorous inspection, commissioning, and validation activities are necessary to identify and correct these failures.

The wear-out period is characterized by an increasing failure rate over time. Poor AAI practices have been cited as a primary cause of equipment failure (HSE, 2005). Preventive maintenance can monitor equipment's useful life and improve its reliability. AAI records provide data that equipment is being well-maintained and periodically restored to "as good as new." Consequently, it is necessary for maintenance personnel to be trained on these activities to ensure equipment integrity.

At a minimum, proof tests should be performed at the frequency necessary to support the SIL. Additionally, consideration should be given to the useful life of the equipment, so that needed replacements or upgrades can be identified and planned (refer to ISA-TR84.00.03 for additional guidance on AAI of SISs). Equipment failure should be investigated using techniques such as root-cause analysis. Failure causes can sometimes be eliminated by making changes to the installation, or by replacing equipment with a product that is more suited to the operating environment. The proof-test interval should be periodically evaluated based on plant experience, hardware degradation, software reliability, etc. In the event that the equipment performance does not meet the SIL requirements, the AAI plan (e.g., inspection, preventive maintenance, and proof testing)

should be modified as necessary to achieve the required performance (refer to ISA-TR84.00.03). Consider having maintenance staff review procedures for ease of use, clarity, and completeness.

Execute proof tests using operation and maintenance procedures that ensure the test is completed correctly, consistently, and safely. Proof tests should determine the “as-found/as-left” condition for all defined process operating modes. Test records should be traceable to the procedure, equipment, and person performing the test. Identify and assess deviations from the design basis and equipment specification, e.g., undocumented changes or accelerated degradation. Communicate negative proof-test findings and use lessons learned to train personnel. Implement procedures to track the time that the equipment is out of service and to ensure that the equipment is correctly returned to service following testing (refer to ISA-TR84.00.03 for additional guidance).

Actual risk-reduction can be demonstrated by AAI data and plant performance (Refer to Annex R in this technical report and ISA-TR84.00.03). The records associated with any SIS document that the equipment can operate as specified during all intended process operating modes. Failure tracking and analysis is essential to quality assurance. Repeated failures likely indicate that the installed equipment may not be capable of meeting the performance requirements. Analyze why metrics are trending in the wrong direction, in order to define an action plan on how to change the trend. These actions may include replacing the faulty equipment or some other portion of the system (e.g., the power supply, steam tracing, etc.), but it could also include improving the automation asset integrity system, test facilities, procedures, and personnel training. When previously unknown failures are identified, communicate these findings to personnel and to the manufacturer, ensuring that lessons learned are not hidden in AAI records.

4.5 Manage changes to the strategy

A successful risk-management strategy accepts that humans are involved in every aspect of a SIS's lifecycle. Therefore, the integrity claimed for any SIS is limited by the quality management system that identifies and seeks to eliminate flaws in the system. Reducing human error to the point where it does not significantly impact system integrity is the goal. Assurance of personnel competency is key.

Annexes C, D, and E in this technical report provide guidance with respect to management of functional safety. Refer to ISA-TR84.00.03 for additional guidance on determining the competency of those associated with the AAI plan.

Knowledge evolves over time as research and development yields operational enhancements to process facilities. Annex R in this technical report provides examples of key performance indicators that can be used to monitor aspects of the SIS lifecycle. Events involving abnormal operation may identify weaknesses in the risk-reduction strategy, leading to the need for more safeguards and improved performance metrics. New ideas identify ways to lower risk further.

Finally, installed SIS equipment should be periodically assessed to determine whether equipment is designed, maintained, inspected, tested, and operating in a safe manner. Use a management of change process to plan, review, approve, and document changes to SISs other than replacement-in-kind. Evaluate changes to the process and its equipment to determine their potential impacts on the approved SIS design basis prior to implementing the change. Personnel need to understand when hazards analysis is required and why tracking change is important. Annex E in this technical report provides examples and guidance on how to organize and perform audits to ensure compliance.

Update documents to “as-built” status, incorporating changes made since the last formal drawing/document revision. Maintain documentation under revision control for the life of the equipment. Documentation should be traceable to the H&RA and should be auditable.

5 Acronyms and abbreviations

AAI	Automation Asset Integrity
ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
BPCS	Basic Process Control System
CCF	Common Cause Factor
CCPS	Center for Chemical Process Safety
CFR	Code of Federal Regulations
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
DCS	Distributed Control System
DD	Dangerous Detected
DL	Design Limit
DTT	De-energize to Trip
DU	Dangerous Undetected
E/E/PES	Electrical/Electronic/Programmable Electronic System
EEMUA	Engineering Equipment and Material Users' Association
EMC	Electromagnetic Coupling
EMI	Electromagnetic Interference
ETT	Energize to Trip
FAT	Factory Acceptance Text
FMEA	Failure Modes and Effects Analysis
FPL	Fixed Program Language
FSA	Functional Safety Assessment
FVL	Full Variability Language
HAZOP	Hazard and Operability Study
HFE	Human Factors Engineering
HSE	Health and Safety Executive
H&RA	Hazard and Risk Analysis

HMI	Human Machine Interface
HNIL	High Noise Immunity Logic
IEC	International Electrotechnical Commission
I/O	Input/Output
IPL	Independent Protection Layer
IPRDS	In Plant Reliability Data System
IR	Infrared
ISA	International Society of Automation
KPI	Key Performance Indicator
LOPA	Layers of Protection Analysis
LS	Logic Solver
LVL	Limited Variability Language
MOC	Management of Change
MRT	Mean Repair Time
MSP	Maximum SIS Setpoint
MTTF	Mean Time to Failure
MTTR	Mean Time to Restoration
NAMUR	Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie (An International User Association of Automation Technology in Process Industries)
NEL	Never Exceed Limit
NFPA	National Fire Protection Association
NRTL	Nationally Recognized Testing Laboratory
OSHA	Occupational Safety and Health Administration
OREDA	Offshore Reliability Data
PE	Programmable Electronic
PERD	Process Equipment Reliability Database
PES	Programmable Electronic Systems
PFD _{avg}	Probability of Failure on Demand
PFH	Probability of Failure per Hour (i.e., Average Frequency of Failure)
P&IDs	Piping and Instrumentation Diagrams

PHA	Process Hazard Analysis
PIU	Proven in Use
PLC	Programmable Logic Controller
PPL	Process Parameter Limit
PSAT	Pre-Startup Acceptance Test
PSSR	Pre-Startup Safety Review
PSI	Process Safety Information
PST	Process Safety Time
QRA	Quantitative Risk Analysis
RAGAGEP	Recognized and Generally Accepted Good Engineering Practice
RC	Resistor-Capacitor
RRF	Risk Reduction Factor
RFI	Radio Frequency Interference
RT	Response Time
RTL	Resistor-Transistor Logic
RTD	Resistance Temperature Detector
SAT	Site Acceptance Test
SD	Safe Detected
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SOE	Sequence of Events
SOV	Solenoid Operated Valve
SP	Setpoint
SRS	Safety Requirements Specification
SSP	Specified SIS Setpoint
SU	Safe Undetected
THERP	Technique for Human Error Rate Prediction
TI	Test Interval

TSU	Total Safeguard Uncertainty
TTL	Transistor-Transistor Logic
UPS	Uninterruptible Power Supply
VAC	Volts Alternating Current
VDC	Volts Direct Current

Annex A

Example Methods for Evaluating the Existing SIS

NOTE Annex A is referenced in Clause 2.0, Clause 3.0, Annex L.7 and Annex R.

A.1 Purpose

The purpose of this annex is to discuss the approaches for determining whether an existing SIS meets the intent of the ANSI/ISA-61511-1:2018 Clause 5.2.5.4.

For existing SIS designed and constructed in accordance with codes, standards or practices prior to the issue of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

The examples provided in this annex show the diversity of the approaches that can be used throughout the SIS lifecycle to determine whether existing SIS equipment provides the necessary functionality and safety integrity. The owner/operator should consider the following during the evaluation:

- consistency of the design with current risk tolerance criteria and hazard and risk analysis philosophy,
- consistency of SIS management with the functional safety management plan,
- development of a method for determining whether an existing SIS is acceptable for continued use,
- integration of this method into the existing process safety management program, and
- consistent application of the method for process safety risks.

Once an owner/operator determines that the existing SIS does not meet the intent of ANSI/ISA-61511-1:2018 Clause 5.2.5.4, there should be a defined process to address the identified deviations. The resolution to the identified deviations should be directed at maintaining process safety, such as SIS upgrades, increased monitoring, increased testing, etc.

A.2 Timing

At a minimum, the adequacy of an existing SIS should be reviewed and documented at the cyclic hazards and risk assessment (H&RA). The owner/operator should also periodically assess the adequacy of the existing SIS as part of a functional safety assessment. Consideration should be given to expediting the assessment if the following occurs:

- modifications to the process unit that impact process risk managed by the SIS,
- modifications to the control system that impact protection layers used to achieve safe operation,
- when an incident or near miss investigation has identified a SIS deficiency,
- When the review of another process unit designed according to similar practice has identified a SIS deficiency, or
- When a functional safety assessment or an audit identifies a SIS deficiency.

A.3 General considerations

The owner/operator should be aware that the functional safety management system applies to all SIS, regardless of when they were installed. *Documentation, procedures, training, testing, and auditing requirements of ANSI/ISA-61511-1:2018 are applicable to all SIS, whether existing or*

new. ANSI/ISA-61511-1:2018 Clause 5.2.6.1.9 requires that changes made to the SIS be conducted in compliance with the 2018 edition.

It is important for the owner/operator to develop an approach for addressing existing SISs. It is the responsibility of the owner/operator to determine that existing SISs meet the intent of the ANSI/ISA-61511-1:2018 Clause 5.2.5.4 and to document the operating, testing, inspection, and maintenance conditions under which this remains true.

There are a variety of methods that can be employed to determine whether existing SIS are fit for continued use. Annex A in this technical report is a collection of methods used by various owners/operators on the ISA84 committee.

A.4 Management of change (MOC) considerations

Owner/operators of existing SIS should acknowledge that being old does not provide an indefinite shield against the full requirements of ANSI/ISA-61511-1:2018. Where an existing SIS has been found to meet the intent of the existing SIS clause, changes to the SIS, the management of the SIS, or the process to which it is providing protection may trigger the need to formally reevaluate the SIS's acceptability "as is."

MOC procedures should cover how to plan, review, approve, and document changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element, or an approved substitution that does not require modification to the SIS as installed) in accordance with ANSI/ISA-61511-1:2018 Clause 5.2.6.2.4. The MOC procedures should also identify "changes that will affect the requirements on the SIS (e.g., redesign of a BPCS, changes to manning in a certain area)" per Clause 5.2.6.2.5. Clear MOC guidelines are important, because the modification work should be executed in compliance with ANSI/ISA-61511-1:2018 requirements (Clause 5.2.6.1.9).

The existing system's clause does not protect any owner/operator from the OSHA General Duty Clause, which requires that owners/operators provide a safe working environment. US-OSHA has already stated in their letter to ISA dated March 23, 2000 that "the employer may be in violation of the General Duty Clause, Section 5 (a)(1) of the OSHA, if SIS are utilized which do not conform with S84.01 [1996] and hazards exist related to the SIS which could seriously harm employees."

Further, the process industries are under continuous pressure to improve the operation of their facilities. This optimization results in an environment of constant change, in terms of retrofits, upgrades, and expansions. At some point, the modification of the process unit and/or the SIS may be significant enough to warrant an evaluation of the acceptability of the existing SIS. This can include changes to the process design, such as a new chemical, identification of new hazards, changes to the P&IDs, definition of the safe state, changes to the SRS, changes in management practices including management of organizational changes (MOOC), and upgrading of obsolete equipment.

When changes are made, any new equipment should meet the current design standards, and modification of the existing equipment should consider the amount of change and determine if that equipment needs to be upgraded to the current standard.

A.5 Example methods for applying ANSI/ISA-61511 Clause 5.2.5.4

Clauses A.5.1 through A.5.3 provide three different approaches used by owners/operators in the evaluation of an existing SIS per ANSI/ISA-61511 Clause 5.2.5.4. These methods are provided for illustrative purposes only. Owners/operators are responsible for developing a method for use at their facilities.

A.5.1 Comparison with SIL requirements

The cyclic H&RA is one of the principal opportunities to review an existing SIF and ensure its design and performance satisfies expectations. During the H&RA, the team identifies potential causes of process hazards and the associated consequence severity for various hazardous events.

For those scenarios that involve medium to high risk to employees, the environment, or to the community, an assessment of the protection layers is conducted to determine whether the required functionality and integrity is provided by the existing design. This assessment is sometimes performed as part of the H&RA or in a more focused study that addresses only those scenarios of medium to high process risk.

During the assessment of the protection layers, the team reviews the following:

- functionality

The functionality of each safety function is examined. For the SIS, the team should determine whether the existing functionality is appropriate to achieve the required safety function. For example, does the high pressure SIF address all initiating causes and isolate all necessary sources of pressure? If the functionality is inadequate, the team should recommend the necessary modification to the SIF to achieve the required safety function.

- integrity

The team assigns a risk reduction to each safety function. For each SIF, the allocated risk reduction defines the SIL. Typically, the verification of the SIL is performed after the study is complete for all SIFs. The verification includes the device integrity, architecture, diagnostics, testing, and potential common cause failures. The examination is to verify consistency of the installed SIF with the integrity requirements. This verification can include a calculation of the PFH or PFD_{avg} for each SIF. The actual PFH or PFD_{avg} is then compared to the SIL assigned by the H&RA team. If the actual PFH or PFD_{avg} is inadequate, the team makes recommendations for upgrading the SIF to meet the SIL.

- independence

The team should examine how the safety functions are allocated to each protection layer, such as the basic process control system or safety instrumented system. The assessment should focus on minimizing the common cause failures between the safety functions associated with each identified process hazard. Then, each protection layer should be reviewed to ensure that adequate independence and separation is provided between layers.

The team also reviews MOC documentation associated with the existing SIS. If changes have been made to the process that might impact the expected performance requirements for the SIFs implemented in the SIS, the team reviews the H&RA (e.g., layer of protection analysis) to ensure the defined safety integrity level for each SIF is still adequate. The team also reviews all of the data and assumptions used during the original H&RA to determine whether they are still valid.

The team assesses the number of demands placed on each SIF to ensure they are consistent with what was originally defined. For example, if the original premise was that the SIF would have about one demand for every 10 years, but, in reality, the SIF is exposed to one demand a year, the team modifies the H&RA assumptions based on this new operating experience. This may result in a higher SIL requirement or in the determination that the SIF is operating in high demand mode rather than low demand mode.

Finally, the team should also consider reviewing the periodic proof-test results to identify devices that have failed repeatedly during tests. For example, if the team determines that the SIF has repeatedly failed its periodic, proof test due to a transmitter fault, the team should recommend that the design, installation, and maintenance practices associated with the SIF be reevaluated. The root-cause analysis may result in the selection of a different technology for the process variable

measurement or in a revised installation. Until the process variable measurement has been proven reliable in this service, the defined test interval should be reduced.

A.5.2 Comparison to previous design practices

In this method, the user has an accepted practice that documents minimum design requirements for the SIS. To determine whether SISs designed in accordance with this design practice are fit for continued use, SIL calculations are performed on the various SISs designed to the prior design practice. The calculation determines the suitability of the design practice to achieve the risk reduction or safety integrity requirement. Then, the installed SIS is assessed to determine whether it meets the requirements of the previous design practice. If the design practice is determined acceptable, any SISs installed in accordance with the practice can be considered acceptable as is, so long as the demonstrated performance of the SIS meets the integrity requirements.

For example, a company that is using its own classification system could map its internal classifications to the different SILs. Table A.1 shows an example of how one company made this comparison. The company verifies the SIL for the SISs, considering the likelihood of random failures and systematic errors. SIL calculations of multiple examples are conducted to validate the design practice. Any assumptions used to run the SIL calculations, such as testing interval, are considered when accepting a specific SIS as is, demonstrated performance.

Table A.1 – Example of mapping prior design practice classification to SIL

NOTE Example provided by one owner/operator.

Accepted prior design class	SIL level
Class 1	SIL 3
Class 2	SIL 2
Class 3	SIL 1

A.5.3 Comparison with a recognized and generally accepted good engineering practice

The United States Occupational Safety and Health Administration (US-OSHA) requires the use of recognized and generally accepted good engineering practices (RAGAGEP), such as those documented in industrial standards. There are many good engineering practices issued by industrial organizations, such as NFPA, API, ASME, ANSI, ISA, etc. These industrial standards tend to be developed in response to new knowledge, analysis tools, and technology. They rely upon the cumulative operating experience throughout industry. They are often application specific, addressing a specific type of process, such as API 14C for off-shore platform safety, or fired equipment, such as NPFA 85/86 for boilers and furnaces.

NOTE It is important to recognize that the RAGAGEP may address more than process safety and may include requirements directed at reducing equipment damage, improving operability, or improving reliability.

Industrial standards often define, in a prescriptive manner, the SIFs required to safely manage the process or equipment. For existing SIFs, omission of the SIL verification would only apply when the standard is prescriptive and clearly defines the required architectures and operation/maintenance practices necessary to implement the SIF(s). The scope and coverage of the standard should result in a SIS that provides safe process operation.

A typical example would be “burner management systems” for industrial heating equipment, such as fired process heaters, reformers, and boilers. Industrial standards and practices for this application would include, but are not limited to, API practices, NFPA standards, and insurance practices (e.g., Factory Mutual) that provide prescriptive requirements for the SIS to achieve functional safety in fired equipment.

An owner/operator should periodically perform a gap analysis to confirm all requirements of the standard have been achieved. Changes made to the standard should be carefully considered throughout the life of the equipment. Additionally, the SIS should be managed appropriately with

respect to documentation, training, periodic proof testing, auditing, and management of change as defined by ANSI/ISA-61511-1:2018 requirements. Robustness of components used to construct the SIF(s) should meet owner/operator's requirements of "prior use" for the application in which they are applied. Finally, any implied redundancy in the standard should be carefully considered.

One of the most important requirements when using this method is to determine that the process equipment clearly falls within the scope of the standard. When equipment or process varies from the standard scope, additional analysis using other techniques is necessary to determine the SIS's acceptability. An example of a variation would be a waste fuel that is not included in the scope of a standard governing a burner management system. Any special requirements for handling the waste fuel would need analysis beyond the scope of the standard. An acceptable technique would be an H&RA (may be supplemented with fault tree evaluation of risk) of those parts of the system that do not specifically apply to the scope of the standard. In other words, the owner/operator determines the functionality and integrity (SIL) requirements for those parts of the SIF that are outside the scope of the standard.

This page intentionally left blank.

Annex B

Alarms and Alerts from the SIS

NOTE Annex B is referenced in the following: Clause 4.2, Annex H.6, Annex K.2, Annex N.1, Annex P, and Annex Q.

B.1 Purpose

ANSI/ISA-61511-1:2018 Clause 3.2.67 note 3 states “A SIS may include human action as part of a SIF.” Common process safety applications of this are where the operator takes action:

- using the manual shutdown features included in the SIS (ANSI/ISA-61511-1:2018 Clauses 10.3.2 and 11.2.8) and
- on the SIS as part of a compensating measure (ANSI/ISA-61511-1:2018 Clause 11.3) when an abnormal process condition occurs while the SIS has a fault or is in bypass.

These actions may be triggered by the operator observing a problem with the process operation or by the operator receiving an alarm through the operator interface. The risk reduction claimed for manual action is limited by the operator and alarm system effectiveness, in addition to any constraints posed by the hardware design. Given the uncertainty of the operator response, many users limit the claimed risk reduction for manually initiated shutdowns to 10 or less, regardless of whether it is implemented in a BPCS or SIS. However, operator response can be an effective protection layer when the intended actions are drilled and practiced. The ANSI/ISA-18 series provides the fundamental requirements for implementing alarms and monitoring alarm system effectiveness. This annex provides no guidance for quantitatively assessing the operator's capability of successfully responding to an alarm, which is highly dependent on the alarm management system, operating procedures, competency, training, human machine interface (HMI), and human factors.

ANSI/ISA 18.2:2016 defines a safety alarm as “an alarm that is classified as critical to process safety for the protection of human life or the environment.” This definition aligns well with the intent of a SIF, which is implemented to prevent “injury or damage to the health of people, or damage to property, or to the environment.” (ANSI/ISA-61511-1:2018 Clause 3.2.27). When the operator is expected to initiate a manual SIF or use other manual shutdown features to prevent a process safety event, the alarm triggering the desired response would meet the ANSI/ISA 18.2:2016 definition of a safety alarm and would be included in the operating procedures and asset integrity program as such.

Operator attention and action related to alarms and alerts impact the ability of the SIS to achieve the risk reduction allocated to each SIF in the SIS. Operators receive information about the SIS via the operator interface, which should be designed and managed in accordance with ANSI/ISA-101. For example, the operator interface can include SIS measured variables, indicating lights, push buttons, horns, and alarms (ANSI/ISA-61511-1:2018 Clause 3.2.46). The interface design should consider the criticality and clarity of the displayed information, especially where diagnostic credit has been taken for the operator recognizing and taking corrective action when there is SIS misoperation. The operator can also be made aware of changes to the SIS status through the use of alerts.

This annex provides guidance and examples of alarms and alerts related to the SIS. The principles of this annex can also be applied to safety alarms implemented in the BPCS as well as those implemented in the SIS. Consequently, this annex does provide a comparison of the risk reduction achievable by safety alarms implemented in the BPCS and those implemented in the SIS.

Annex Q in this technical report discusses setpoint determination for an automated SIF. Recognize that some process sensor technologies can have significant measurement error and time lags, which introduce uncertainty in the reporting of the process variable. This annex provides special considerations when selecting the setpoint for a safety alarm.

B.2 Allocated risk reduction

ANSI/ISA-84.91.01 defines safety controls, alarms and interlocks as process safety safeguards:

- implemented with instrumentation and controls,
- used to achieve or maintain a safe state for a process, and
- required to provide risk reduction with respect to a specific hazardous event.

ANSI/ISA-84.91.01 recognizes safety alarms and establishes requirements for their automation asset integrity.

In general, no more than one order of magnitude risk reduction should be claimed for safety alarms in reducing the frequency of a hazardous event. This risk reduction constraint is irrespective of the number of alarm windows, interfaces, or audible notifications, due to human factor limitations associated with the operator responding to the alarms presented during an event. A formal assessment of the human factors should be conducted in cases where the risk reduction strategy against a specific hazardous event proposes:

- allocating risk reduction to more than one safety alarm within any single system.
- allocating risk reduction to multiple safety alarms implemented in multiple systems.
- claims more than one order of magnitude of risk reduction for an alarm.

The analysis should include the potential for common cause associated with the operator, operating procedures, and alarm loop equipment (sensor through final control element).

This annex does not address the SIL verification calculation for a manually initiated SIF. Refer to ISA-TR84.00.02 Annex H for guidance on performing the PFD calculation. In the above cases, the potential common cause and systematic failures between the alarm and other protection layers should be evaluated and determined to be sufficiently low compared to the overall risk reduction in conformance with ANSI/ISA-61511-1 Clause 9.4.

B.2.1 Examples of alarms and alerts in SIS applications

Alerts and alarms are generated for a number of reasons. Many alarms are identified through hazards and risk analysis processes and are used to achieve risk reduction associated with identified hazardous events. Other alarms are required by good engineering practice based on historical incidents. Whether these alarms are referred to as manual safety function alarms, safety alarms, or safety function alarms, they need to be implemented in a manner that supports a high level of operator effectiveness. Alerts, on the other hand, can be related to equipment faults where the risk reduction is not compromised. These alerts are intended to communicate the SIS's degraded status to the operator. The need for alerts should be identified during the design and engineering phase of a SIS and should be documented.

The following sections discuss alerts and alarms and provide considerations for their implementation in the BPCS or SIS. See Annex F in this technical report for further discussion on using the BPCS and SIS as protection layers.

The examples presented are for illustration purposes only and should not be considered minimum requirements.

B.2.1.1 Alerts from the SIS

ANSI/ISA 18.2:2016 defines an alert as an “audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness and which does not meet the criteria for an alarm.”

When timely operator response is required to implement compensating measures due to a diagnosed fault in the SIS, the notification would be categorized as an alarm instead of an alert.

Alerts can be used for indicating status or diagnostic information from the SIS equipment that do not require specific timely action from the operator. Typical examples of alerts issued by the SIS include:

- Indications related to support systems for the SIS that are not required for the SIF and where there is substantial time to detect the support system failure prior to the dangerous failure of the SIS (e.g., climate control, heat tracing, purges).
- Notification of detected faults within the SIS or its subsystems where the required risk reduction is still met. Refer to ANSI/ISA-61511-1:2018-1 Clause 11.3 and Annex P in this technical report for additional discussion on the operator response to the detection of a fault.
- Bypass and other out-of-service notifications concerning the SIS equipment, where the required risk reduction is still met. Refer to ANSI/ISA-61511-1:2018 Clause 15.2.4 for validation requirements for alarm annunciation and bypass requirements. Also, refer to Annex P in this technical report for more guidance on fault detection and response.

The system providing these SIS alerts should be managed under the AAI program, ensuring that proof testing, access security, and management of change are practiced. Refer to ISA-TR84.00.03 for guidance on the AAI program. In addition, refer to the guidance on alerts provided by the ANSI/ISA-18 series.

B.2.1.2 Safety alarms implemented in the BPCS

Examples of this type include alarms classified as critical to process safety and can include:

- Alarms identified as safeguards in a hazards and risk analysis with a claimed risk reduction of 10 or less.
- Alarms associated with SIS equipment bypass where the required risk reduction has been partially lost (i.e., the SIS might not meet the SIL but is still capable of responding to a demand) and the operator is expected to provide a compensating measure.

Alarms allocated to the BPCS are limited to a risk reduction factor of 10 or less (Ref. ANSI/ISA-61511-1:2018, Clause 9.3.2). The following should be considered in evaluating the appropriateness of the claimed risk reduction:

- The common cause and dependent failures between the alarm and the initiating causes and between the alarm and other protection layers for the same hazardous event is sufficiently low. Refer to ISA-TR84.00.04 F.2.
- There is sufficient time for operator response. Refer to ISA-TR84.00.04 B.6.
- The alarm management requirements per ANSI/ISA-18.2 are implemented and the demonstrated alarm management system effectiveness meets the claimed risk reduction. The ANSI/ISA-18.2 clauses associated with response procedures, training, and management of change are especially important for process safety events.
- Devices involved in the process safety event detection and response are subject to proof testing (ANSI/ISA-84.91.01).
- Security has been implemented for the BPCS (Refer to ISA-TR84.00.09).
- Human factors should be considered in the design of the operator interfaces. Human reliability analysis is not required when only a single order of magnitude of risk reduction is claimed.
- The operator response to the alarm is audited periodically to ensure that the operator takes the prescribed actions as and when required.

B.2.1.3 Safety alarm implemented in the SIS

Examples of this type include alarms classified as critical to process safety, which can include:

- Alarms where the claimed risk reduction > 10 for process safety events.
- Alarms allocated to the SIS for process safety events that require independence from BPCS faults.
- Alarms that establish the never exceed limits requiring initiation of manual shutdown via the SIS.
- Diagnostic alarms related to critical support systems for the SIS (e.g., loss of power to the ETT system or loss of instrument air supply for air-to-move valves) where there is limited time before the SIS can be dangerously affected.
- Alarms associated with a detected fault that disables a function within the SIS, and the operator is expected to immediately provide a compensating measure to protect the process.
- Alarms indicating failure of a function within the SIS to operate on demand requiring the operator to take independent action to achieve or maintain a safe state of the process.
- Bypass alarms that disable a function within the SIS and require the operator to provide a compensating measure to protect the process.

A safety alarm with a claimed risk reduction > 10 should be separate and independent from the BPCS to the extent that the risk reduction provided by the safety alarm is not impacted. The alarm is subject to alarm management per ANSI/ISA-18.2.

For risk reduction > 10 , the following should be considered:

- Hardware involved (sensors, logic solvers, alarm systems, and final elements) should meet the design, implementation, operation, maintenance, and testing requirements of ANSI/ISA-61511-1:2018.
- The SIL calculation should cover all hardware involved in the event detection and response, including any sensors, logic solvers, alarm systems, and final elements.
- The alarm management requirements per ANSI/ISA-18.2 are implemented, and the demonstrated alarm management system effectiveness meets the claimed risk reduction. The ANSI/ISA 18.2 clauses associated with response procedures, operator training, and management of change are especially important for process safety events.
- There is sufficient time for operator response. Refer to ISA-TR84.00.04 B.6. The claimed risk reduction should consider operator reliability. Refer to ANSI/ISA-61511-1:2018 Clause 11.9.2 k). The operator's response to alarms is verified against the required action and response time.

B.3 Human response time criteria

In addition to the response time delays originating with the SIS devices, safety alarms have additional delays due to the human response time. The allowable response time for the operator portion of the safety function, as defined by ANSI/ISA-18.2, is the "maximum time between the annunciation of the alarm and when the operator must take corrective action to avoid the consequence." Many human performance shaping factors will affect the amount of time needed for the response action to be sufficiently reliable that the overall safety alarm function will meet the specified risk reduction. Given the uncertainty in typical process safety time estimations, the estimated time required to complete the operator action should be less than the allowable response time by a reasonable safety margin. If the operator action is performed in the field, the design should consider the time required for the operator to activate emergency response (e.g., unit evacuation or shelter in place), in the event the alarm response actions are not working as intended.

Guidance on determining the allowable response time, including a typical alarm response timeline, is provided in ANSI/ISA-18.2:2016 Clause 5.4.1. Additional guidance on the relationship of process safety time and IPL response time is provided in CCPS's *Guidelines for Initiating Events and Independent Protection Layers* and *Guidelines for Safe Automation of Chemical Processes*. The minimum times provided in these CCPS books are based on research and are confirmed by a consensus of industry experience. These sources typically assume positive human factors are in place for the indicated minimum times to be appropriate. For example:

- Alarms should be designed to allow a timely operator action.
- The effectiveness of the alarm management system should be taken into consideration (see performance metrics in ANSI/ISA-18.2).
- In cases where the available response time extends across shifts, active alarms should be discussed at operator shift change.

The CCPS guidelines also provide recommendations on the minimum time needed to claim risk reduction for different types of operating situations. The values from these sources represent the risk reduction of the complete safeguard, including the alarm, operator response, and final element actions and should not be interpreted as the risk reduction for the human action only. If the owner/operator wishes to use shorter response times or greater risk reduction values, a human reliability assessment should be used to verify the risk reduction capability and to periodically validate the timeliness and correctness of the required operator actions.

B.4 Verification of a manually initiated shutdown

An example of the SIL verification analysis of an operator response safeguard is located in ISA-TR84.00.02. When risk reduction >10 is taken for manual shutdown, the evaluation of the PFD_{avg} is performed similarly to the evaluation of an automatic SIF. Figure B.1 is a representation of a safety alarm system used to implement a manual shutdown. This figure is adapted from ANSI/ISA-61511-1:2018 Clause 3.2.67, Figure 6.

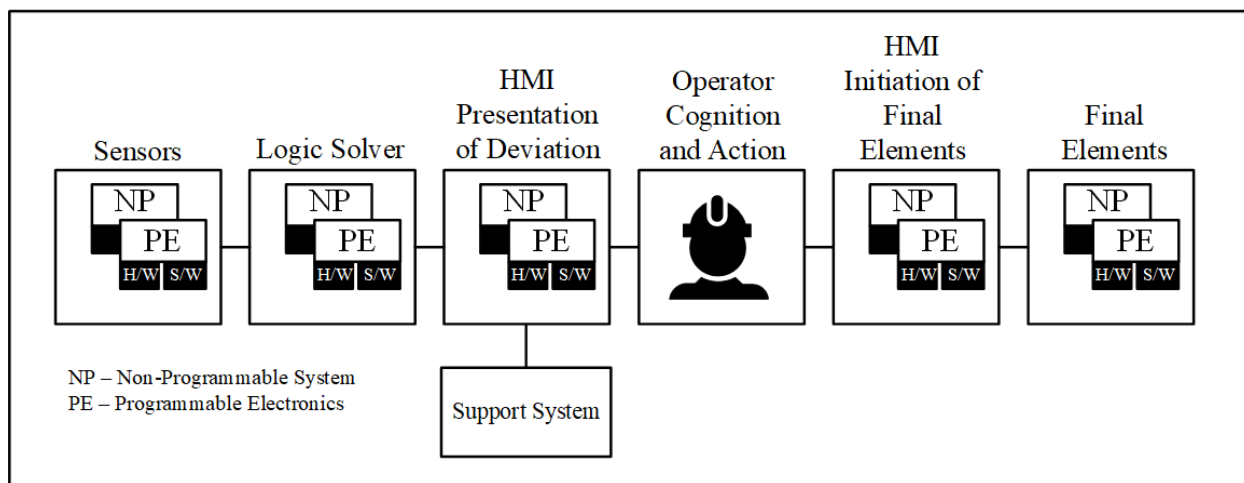


Figure B.1 – Example of safety alarm system architecture

The verification of the safety alarm system should consider the potential for operator error, so the assessment should consider human factors in the design of the operator interfaces to receive the alarm and to take action on the process.

There are a number of methods for evaluating the probability of human error. Two well-known methods are the Technique for Human Error Rate Prediction (THERP) (Reference NUREG/CR-

1278) and the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (Reference NUREG/CR-4772). Error rates are usually established on a per demand basis.

The nominal human error rates can be reduced or increased based on environmental factors (quality of displays, control layout and clarity, control area environment, procedures, access restrictions), personnel factors (training, experience), and stress factors (personal, shift schedules, response time pressure, severity or magnitude of safety condition). The best source for determining the human error rate would be company/facility-specific historical data, but in most organizations this is not available. Therefore, an owner/operator often uses other published, acknowledged sources and adjusts the human error rate for their application and circumstances accordingly.

In addition to the initial evaluation of the operator action, a program should be established to ensure that all assumptions about the reliability of the operator response are maintained and improved. This would include, but is not necessarily limited to, things such as: initial training, refresher training, performance validation, procedures engineered to decrease the likelihood of human error, important human factors that have been identified, potential for alarm overload, adequate time to respond to the safety alarm, adequate staffing, etc.

Interface design also has a significant impact on the operator effectiveness. Poor interface design can lead to confusion and incorrect action even when the alarm system and the operator are fully capable of responding successfully. ANSI/ISA-101.01:2015, *Human Machine Interfaces for Process Automation Systems*, provides requirements for HMI design in the process industry sector. Operating procedures should be sufficiently detailed to ensure that the operator is trained on the likely cause, consequence, corrective action, and allowable response time for the alarm. Operator training can be supplemented with tabletop scenario discussions, drills, simulators, and other hands-on activities to confirm retention and timely recall of key actions.

Most automated SIFs are designed as de-energize to trip. As a result, the PFD_{avg} calculations for most SIFs do not take into consideration any support systems. Operator action inherently requires support systems to complete the safety function. Display/alarms require power to actuate the light and/or horn for operator response. Therefore, the reliability of the electrical power system directly affects the PFD_{avg} .

B.5 Guidance on safety alarm setpoint determination

Guidance on establishing instrument setpoints for SIF can be found in Annex Q in this technical report, including explanations for general terms, such as “never exceed limit.” When establishing a setpoint for a safety alarm requiring operator response, there are additional considerations for the setpoint determination. As shown in Figures B.2 and B.3, the overall safety alarm response time includes a combination of human and hardware delays.

A critical aspect in achieving risk reduction for a safety alarm is how much time the alarm system design gives the operator to respond to the process safety event.

Per ANSI/ISA-61511-1:2018 Clause 3.2.52.1, the process safety time is the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed. It also states that process safety time is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event, taking into account any process lag (e.g., cooling of a vessel). More generally, the process safety time is the time period between the initiating source and the occurrence of the process safety event if the specified safeguards do not operate as specified.

The specified response time for the alarm should be shorter than the process safety time to allow time for the process to recover without exceeding the never exceed limit after final control element action is taken. The operator’s allowable response time will be a subset of the safety alarm’s

specified response time, as the operator response does not begin until the alarm for the hazardous condition is annunciated to the operator and typically ends before the final element movement occurs.

The operator allowable response time, which is the human component of the safety alarm IPL response time, is comprised of the following components:

- 1) Detect – the system detects and annunciates the abnormal condition (alarm setpoint); the operator becomes aware of the deviation from the desired condition by an alarm caused by a disturbance. The design of the alarm system and the operator interface facilitates the detection of deviation.
- 2) Diagnose – the operator uses knowledge and skills to interpret the information, diagnose the situation, and determine the corrective action to take in response to the deviation. The alarm response procedures aid the operator's diagnosis.
- 3) Respond – the operator takes corrective action in response to the deviation (either manually or through the HMI) and monitors the process to determine if the deviation is corrected or a safe state is achieved.

With the notable exception of temperature and analyzer instrument technologies, the time for the sensor to detect and the logic solver to annunciate a problem is often on the order of seconds, while the operator's allowable response time (comprised of the time to detect the alarm, diagnose the problem, and take action) is typically on the order of minutes. The more complex the response procedure is, the more time is typically needed for troubleshooting and response.

There may also be response time lags that take place after the operator completes the human portion of the response action. The response to an alarm can include the manual operation of a final control element accessible via the HMI in the control room, in the field, or a combination of both. Stopping the process condition from propagating toward the hazardous event is dependent upon the response being completed in a timely manner. For example, Figure B.2 provides a graphical representation of establishing an alarm setpoint for an increasing process variable when the safety alarm response is performed by initiating the action of an automated final element through an HMI. In this example, after the operator response is taken, there would be additional response time contributions from communication lags, the logic solver, and the manipulation of the final control element. In contrast, Figure B.3 represents establishing an alarm setpoint when the safety alarm response is performed using a manually actuated final element.

Finally, the process lag, which can be on the order of minutes, is also taken into account when defining the alarm setpoints. For ANSI/ISA 18.2, the process deadtime includes the output delay and process lag time, when the response action is automated, such as pushing a manual shutdown button (Figure B.2). In contrast, the operator allowable response time includes the output delay when the response action involves manual activities in the field, such as closing a manual block valve (Figure B.3). In this latter case, the process lag time and process deadtime are analogous.

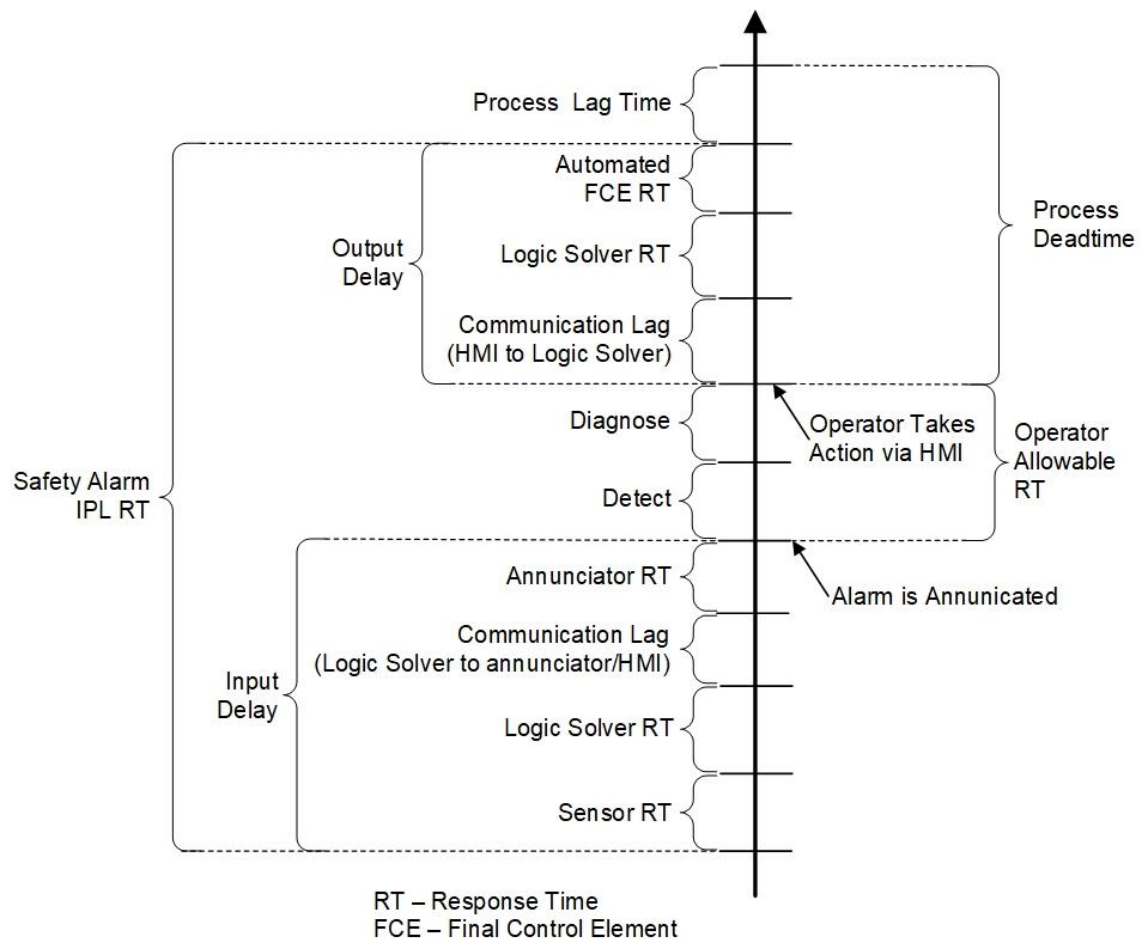


Figure B.2 – Safety alarm system for increasing process variable with operator action via HMI

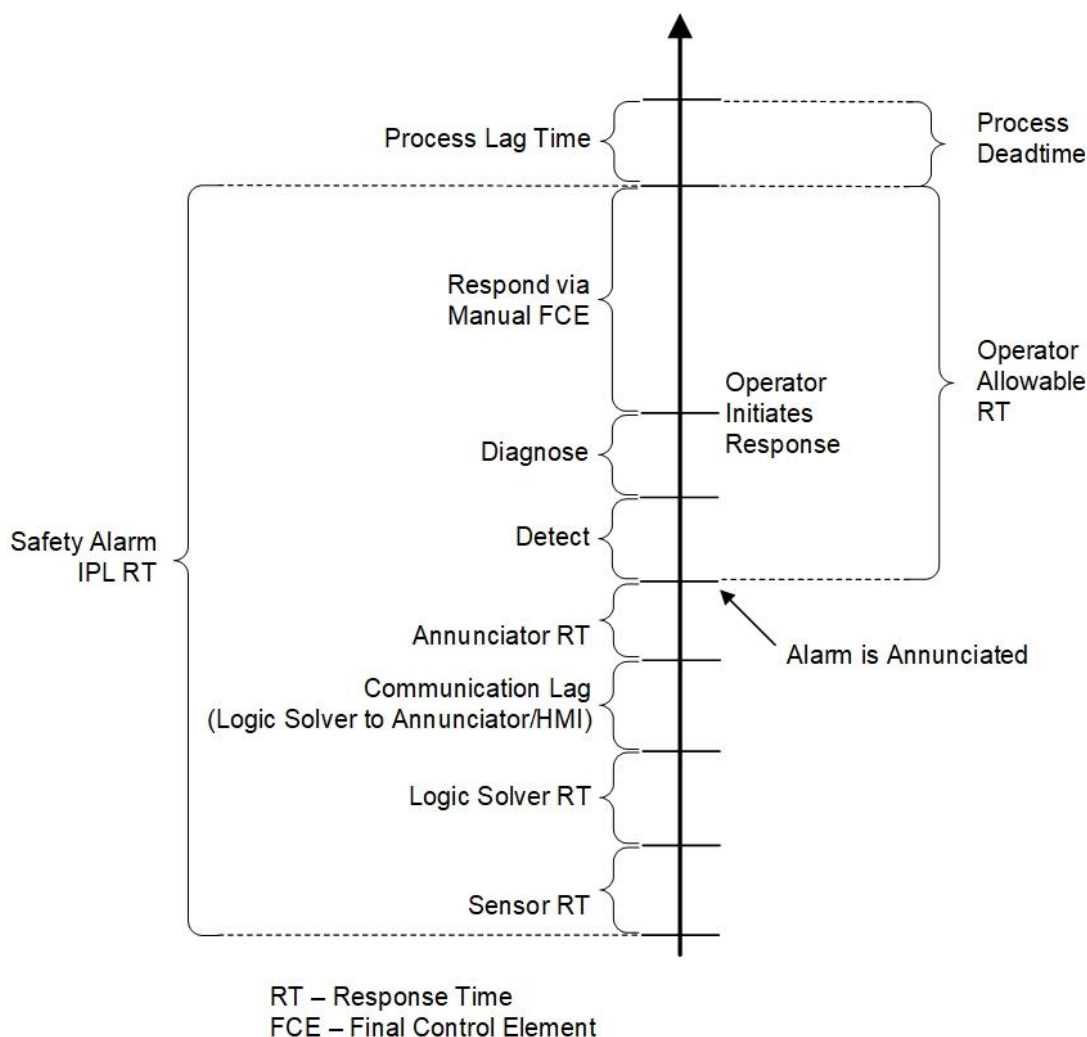


Figure B.3 – Detail of safety alarm for increasing process variable and manual final control element

When the risk management strategy involves multiple instrumented safeguards, setpoints should be selected to allow each safety function to complete its action in the desired order. Overlapping the safeguard actions can have an impact on the design of the instrumented systems. When one of the safety functions is an operator response to alarm, the most positive human factors for successful execution will occur when there is no overlap between the specified response period for that safeguard and the initiation of any other safeguards. For example, when the primary objective of the operator response is to return the process to normal operation, the safeguards should be staged so that the operator response can be reliably completed before the action of any automated safety functions. Examples of staging multiple instrumented safeguards against a common hazard without overlap are depicted in Annex Q, Figures Q.1 and Q.2 in this technical report.

This page intentionally left blank.

Annex C

Management of Functional Safety: Organization and Resources

NOTE Annex C is referenced in the following: Clause 4.1 and Annex E.5.2.

C.1 Purpose

Management of functional safety is a fundamental requirement of ANSI/ISA-61511-1:2018, and it has always been considered a necessary activity by OSHA 1910.119. The intent of this annex is to provide additional guidance on the organization and resource element of the ISA-61511-1 Clause 5.2 on the management of functional safety.

C.1.1 Identification of the right people

The intent of ANSI/ISA-61511-1:2018 is to achieve functional safety throughout all phases of plant operation. To achieve functional safety, the standard requires identification of the following:

- the activities that should take place throughout the execution of a project to achieve safe operation,
- the activities that should take place during the operation of the plant to maintain safe operation, and
- the personnel that are responsible for conducting each activity.

In addition to meeting the functional safety requirements, all designs should consider the reliability, operability, and maintainability requirements of the process unit. Designing a SIF that requires frequent off-line testing to achieve its SIL may not be supported by a plant that wants to increase its service factor by extending the turnaround interval. Consequently, part of identifying the right people to work on SIS projects is to determine whether they follow design practices that are geared toward the requirements of the standard and achieve the plant targets for reliability, operability, and maintainability. The right people also need to know a lot more than what is contained in ANSI/ISA-61511:2018. Knowledge of the standard can supplement education and experience, but cannot replace it. For example, the SIS specialist should understand the process, the equipment, the operation, basic process control system design, protection layer design, safety instrumented system design, human ergonomics, consequence modeling, and hazard and risk analysis.

Clearly established roles and responsibilities enable the necessary resources to be defined early ensuring that the project is correctly staffed. Table C.1 provides an example of a roles and responsibilities matrix. For this project, a SIS specialist was the project lead.

Personnel assigned to a specific project often represent multiple companies, such as the owner/operator, engineering contractor, integrator, manufacturer, or consultant. For this reason, the standard refers to the identification of individuals, departments or organizations that are responsible for each lifecycle task. Personnel education and experience should be evaluated to determine whether mentoring, supervision, or additional training is necessary. For example, Table C.2 provides suggested education and experience for the various disciplines that are shown in Table C.1.

All documents created for a project should be reviewed by an independent person from the creator of the document. At certain stages of the lifecycle, the standard recommends that a functional safety assessment be performed by an assessment team that contains at least one senior, independent, competent person. This independent person can be an employee of the company or a contracted third-party, as long as the reviewer understands the process hazards, the company's management system, the full SIS lifecycle, and the fundamentals of appropriate design, installation, operation, maintenance, testing, and reliability. This person should not be part of the project team, should not report to project team management, and should not report to plant operations.

C.2 Planning of a work process

The owner/operator should define when verification, assessments, auditing and validation activities take place to ensure that adequate time and resources have been assigned to these activities. The highest quality projects are obtained when procedures or guidelines are in place to ensure that all activities occur in the proper order with the necessary content. For example, many projects have experienced delays when SIL verification was performed late in the project and the SIS design was found to be inadequate.

Procedures for evaluating the performance of the SIF after it has been installed (e.g., performance audits, tracking failures rates, etc.) should also be developed. For further information on auditing activities, refer to Annex E in this technical report.

C.3 Roles and responsibilities matrix

One option for the management of functional safety is developing and using a roles and responsibilities matrix. The attached roles and responsibilities matrix is provided for illustration purposes only. It is typically developed for each specific project. In the roles and responsibilities matrix, each clause or step is divided into four activities—planning, inputs, outputs, and verification.

The verification portion includes all the specific requirements (all the “shall” statements) from the standard. Whoever has the review responsibility for any lifecycle activity deliverable should consider developing a verification list that addresses relevant requirements from the standard.

Table C.1 — Example roles and responsibilities matrix

ANSI/ISA-61511-1:2018 Clause	SIS Specialist	Project Leader	Area Supervisor (note 1)	Operations Rep	Maint/Elec Rep	Process/ Design Engineer	Project SIS Contractor	Corporate/ Plant HS&E
Clause 5.2.5 – Implementing and monitoring	L	R/A	A	P/R		P	P	R
Clause 6 – Safety lifecycle requirements	L	R/A	P			P	P	
Clause 7 – Verification	L	R/A	P			P	P	
Clause 8 – Hazard and risk assessment Clause 9 – Allocation of safety functions to protection layers	L	R	A	R	R	P	P	A
Clause 10 – SIS safety requirement specification (SRS)	L	R	A	R	R	P	P	
Clause 11 – SIS design and engineering	L	R	A	R	R		P	
Clause 12 – Requirements for application program, including selection criteria for utility software	L	R	A	R	R		P	
Clause 13 – Factory acceptance test (FAT)	L	R	A	R	R		P	
Clause 14 – SIS installation and commissioning	L	R	A	R	R		P	
Clause 15 – SIS safety validation (SAT)	L	R	A	R	R		P	
Clause 16 – SIS operation and maintenance	L	R	A	R	R		P	
Clause 17 – SIS modification	L	R	A	R	R		P	
Clause 18 – SIS decommissioning	L	R	A	R	R		P	
Clause 19 – Information and documentation requirements	L	R	A	R	P	R	P	

Legend:

A – Approval. Decides when the activity or deliverable is complete.

L – Lead. May perform the work or just coordinate it. Has responsibility to see that the activity or deliverable is completed.

P – Participate. Performs a portion of the work. Participates as a member of the team as directed by the “Lead.”

R – Review. May provide initial examples or reviews the final material.

Blank – No involvement.

NOTE 1 The successful implementation of a quality SIS requires that plant personnel and contractors work as a team. The SIS team coordinates the work, gathers information to make informed decisions, and gains consensus on the final design. For each SIS project, there are core members that take responsibility for design and implementation of the SIS. In addition, a number of additional resources may be needed. The SIS team and the additional resources are provided below.

NOTE 2 SIS project members assigned to every project:

- **Project Manager** – Coordinates activities. Manages the budget and schedule.
- **SIS Specialist** – Keeper of technology.
- **Maintenance Representative** – Coordinates maintenance input.

NOTE 3 Other project members assigned by the unit installing the safety system:

- **Area Supervisor** – Person that owner/operator designates as having approval authority
- **Operations Representative** – Coordinates operational input, for example, graphics design and location of manual shutdown pushbuttons.
- **Process Engineer** – Coordinates process input, e.g., what are the trip setpoint values and justification for value.

NOTE 4 Additional resources may include representatives from the following groups:

- Maintenance
- Operations
- Process engineering
- Reliability
- Health, safety and environment

Table C.2 – Examples of experience or skills for the disciplines in Table C.1

Discipline	Experience or skills
SIS Specialist	Very familiar with ANSI/ISA-61511:2018 and any applicable previous version
	Understands the risk criteria to be applied during the design
	Experience/training on hazard and risk analysis methodology
	Knowledgeable in device common mode/common cause failures
	Knowledgeable in the work process for selection of devices
	Knowledgeable in the design, installation, and management of SIS
	Knowledgeable in the appropriate selection of integrity and reliability data
	Knowledgeable on the methods for verifying SIL
	Understands the roles and responsibilities of the other parties in the project
Corporate/Plant Health, Safety, and Environmental Representative	Experience/training with SIS lifecycle and understands personal role and responsibility
	Knowledgeable in the risk criteria to be applied during the design
	Knowledgeable in hazards and risk analysis methodology
	Experience/training in equipment design limitations, process hazards and interactions with other process units
Process/Design Engineer	Experience/training with SIS lifecycle and understands personal role and responsibility
	Knowledgeable in the process under evaluation
	Experience/training in hazards and risk analysis
	Experience/training in the risk criteria to be applied during the design
	Understands equipment design limitations, process hazards and interactions with other process units.
	Understands operating procedures for various modes of operation
	Experience/training on the development of input information required by those executing the SIS design
	Experience/training in selection of SIS devices and technologies
Project SIS Contractor	Knowledgeable with ANSI/ISA-61511:2018 and any applicable previous version
	Understands the risk criteria to be applied during the design
	Experienced/training on hazard and risk analysis methodology
	Experienced/training in device common mode/common cause failures
	Experienced/training in the work process for selection of devices
	Experienced/training in the design, installation, and management of SIS
	Experienced/training in the appropriate selection of integrity and reliability data
	Experienced/training on the methods for verifying SIL
Maintenance/Electrical Representative	Experience/training with SIS lifecycle and understands personal role and responsibility
	Knowledgeable in maintenance and testing practices and procedures
	Knowledgeable concerning equipment (including fixed equipment and instrumentation) failure history and causes.
	Experience/training on process hazards
	Experience/training on integrity/reliability data

Discipline	Experience or skills
Operations Representative	Experience/training on the impact of testing on SIS performance
	Experience/training on the impact of maintenance activities on plant operation
	Experience/training with SIS lifecycle and understands personal role and responsibility
	Knowledgeable in operating procedures including response to diagnostic and safety alarms
	Experience/training on process hazards
	Experience/training on integrity/reliability data
	Experience/training on the impact of proof testing on plant operation
	Experience/training on the impact of alarm response on safe operation
	Experience/training on the impact of operational activities on safe operation
Area Supervisor	Experience/training with SIS lifecycle and understands personal role and responsibility
	Knowledgeable concerning operator training, responsibilities and capabilities
	Knowledgeable concerning maintenance training, responsibilities and capability
	Knowledgeable concerning process hazards
	Experience/training on integrity/reliability data
	Experience/training on the impact of operational activities on safe operation
	Experience/training on the impact of testing on SIS performance