

**TECHNICAL REPORT
ISA-TR84.00.04-2011
Part 1
Guidelines for the Implementation of ANSI/ISA-84.00.01-2004
(IEC 61511 Mod)**

Approved 14 October 2011

ISA-TR84.00.04-2011

Part 1 - Guideline for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)

ISBN: 978-1-937560-24-9

Copyright © 2011 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 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Copyright 2011 ISA. All rights reserved.

Preface

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

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. 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 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, NON-DISCRIMINATORY 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 NON-DISCRIMINATORY.

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 members of ISA84 in developing this technical report:

NAME	COMPANY
W. Johnson, Chair	DuPont Sustainable Solutions
V. Maggioli, Co-Managing Director	Feltronics Corp
D. Zetterberg, Co-Managing Director	Chevron Energy Technology Company
A. Summers, TR Working Group Leader	SIS-TECH Solutions LP
R. Adamski	RA Safety Consulting LLC
T. Ando	Yokogawa Electric Co
R. Avali	Westinghouse Electric Corp
L. Beckman	Safeplex Systems Inc
J. Campbell	ConocoPhillips
I. Chen	Aramco
R. Chittilapilly	Oil & Natural Gas Corp
M. Coppler	Ametek Inc
M. Corbo	ExxonMobil
P. Early	Langdon Coffman Services
C. Fialkowski	Siemens Inc
K. Gandhi	KBR
I. Gibson	Consultant
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida
P. Gruhn	ICS Triplex
B. Hampshire	BP
J. Harris	UOP A Honeywell Company
J. Jamison	EnCana Corporation Ltd
R. Johnson	Dow Process Automation
K. Klein	Celanese Corp
T. Layer	Emerson Process Management
E. Marszal	Kenexis Consulting Corp
N. McLeod	ARKEMA
M. Mollicone	SYM Consultoria
G. Ramachandran	Systems Research Intl Inc
R. Roberts	Suncor Energy Inc
M. Scott	AE Solutions
D. Sniezek	Lockheed Martin Federal Services
C. Sossman	CLS Tech-Reg Consultants
R. Strube	Strube Industries
L. Suttinger	Savannah River Nuclear Solutions
T. Walczak	Conversions Inc
M. Weber	System Safety Inc
A. Woltman	Shell Global Solutions
P. Wright	BHP Engineering & Construction Inc

Copyright 2011 ISA. All rights reserved.

This technical report was approved for revision by the ISA Standards and Practices Board on 14 October 2011.

NAME

D. Dunn, Vice President
E. Cosman, Vice President-Elect
D. Bartusiak
P. Brett
J. Campbell
M. Coppler
B. Dumortier
J. Federlein
J. Gilsinn
E. Icahan
J. Jamison
K. Lindner
V. Maggioli
T. McAviney
R. Reimer
S. Russell
N. Sands
H. Sasajima
T. Schnaare
J. Tatera
I. Verhappen
W. Weidman
J. Weiss
M. Wilkins
D. Zetterberg

COMPANY

Aramco Services Co.
The Dow Chemical Co.
ExxonMobil Research & Engineering
Honeywell Inc.
ConocoPhillips
Ametek Inc.
Schneider Electric
Federlein & Assoc. Inc.
NIST/MEL
ACES Inc.
EnCana Corporation Ltd.
Endress+Hauser Process Solutions AG
Feltronics Corp.
Jacobs Engineering
Rockwell Automation
Valero Energy Corp.
DuPont
Yamatake Corp.
Rosemount Inc.
Tatera & Associates Inc.
Industrial Automation Networks Inc.
Consultant
Applied Control Solutions LLC
Yokogawa IA Global Marketing (USMK)
Chevron Energy Technology Company

This page intentionally left blank.

Copyright 2011 ISA. All rights reserved.

Foreword

ANSI/ISA-84.00.01-2004 gives requirements for the specification, design, installation, operation and maintenance of SIS, so that it can be confidently entrusted to place and/or maintain the process in a safe state. These requirements are presented in the standard, using the safety lifecycle shown in ANSI/ISA-84.00.01-2004-1, Figure 8, and described in ANSI/ISA-84.00.01-2004-1 Table 2.

The ISA84 committee has developed a series of complimentary 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 8 and Table 2 have been adapted for this foreword as shown in ISA-TR84.00.04 Figure 1 and Table 1, respectively. A brief overview of each technical report is given below, including the report's relationship to the lifecycle requirements and the intended scope of each report's guidance.

ISA-TR84.00.02—Safety Integrity Level (SIL) Verification of Safety Instrumented Functions—Lifecycle 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-84.00.01 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 mechanical integrity (MI) 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 MI requirements for any given SIL. Once an SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured MI program as described in ISA-TR84.00.03

ISA-TR84.00.03—Mechanical Integrity of Safety Instrumented Systems (SIS)—Lifecycle 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 MI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective MI program that demonstrates, through traceable and auditable documentation, that the SIS and its equipment are maintained in the “as good as new” condition. The technical report addresses the identification of personnel roles and responsibilities when establishing an MI plan, important considerations in establishing an effective MI program, and detailed examples to illustrate user work processes used to support various activities of the MI program. Data and information collected as part of the MI 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 ISA-TR84.00.04 Annex L.

ISA-TR84.00.04—Guidelines for the Implementation of ANSI/ISA-84.00.01—Lifecycle 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-84.00.01. This report covers many aspects of the safety lifecycle, including such topics as: “grandfathering” existing SIS (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, which only provides a brief introduction to the topic of failure calculations. ISA-TR84.00.04 does not address the MI program, which is discussed in ISA-TR84.00.03.

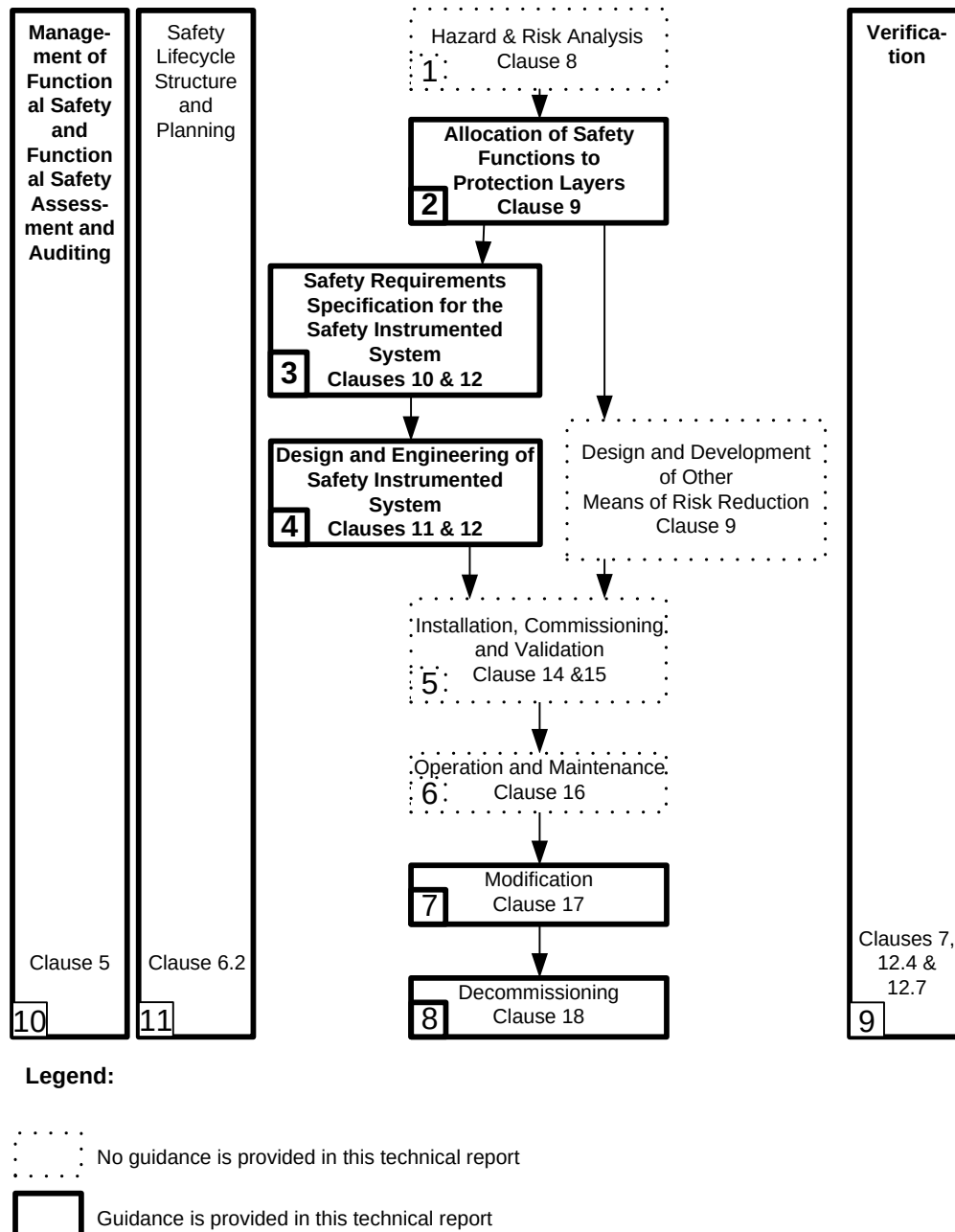


Figure 1 – SIS Safety Lifecycle (modified ANSI/ISA-84.00.01-1 Figure 8)

Copyright 2011 ISA. All rights reserved.

Table 1 - SIS safety life-cycle overview (modified ANSI/ISA-84.00.01-1 Table 2)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 Requirements Clause	ISA-84 Technical Report Reference
Figure 1 box number	Title			
1	Hazard and risk analysis	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 safety instrumented function, the associated safety integrity level.	9	ISA-TR84.00.04 Annexes B, F, and J
3	SIS safety requirements specification (SRS)	To specify the requirements for each SIS, in terms of the required safety instrumented functions 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 & engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity.	11 & 12.4	ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q ISA-TR84.00.02
5	SIS installation commissioning & 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 Safety Instrumented Functions and the required safety integrity.	12.3, 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

(Continued on next page)

Copyright 2011 ISA. All rights reserved.

(Table 1 continued from previous page)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 Requirements Clause	ISA-84 Technical Report Reference
Figure 1 box number	Title			
7	SIS modification	To make corrections, enhancements, or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained.	17	Apply appropriate safety lifecycle phase during management-of-change activity.
8	Decommissioning	To ensure proper review, sector organization, and ensure Safety Instrumented Function (SIF) remain appropriate.	18	Apply appropriate safety lifecycle 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, 12.7	ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02
10	SIS functional safety assessment	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

Copyright 2011 ISA. All rights reserved.

CONTENTS

1	Purpose	17
2	Introduction.....	17
3	Grandfather clause.....	18
3.1	General considerations	19
3.2	Management-of-change considerations.....	19
4	Overview	21
4.1	Lifecycle approach	22
4.2	Define a risk-management strategy	22
4.3	Implement the strategy.....	23
4.4	Validate, start-up, operate and maintain the strategy	26
4.5	Manage changes to the strategy.....	27
Annex A – Example methods for determining grandfather status		29
A.1	Purpose	29
A.2	Timing.....	29
A.3	Approaches to the grandfather clause	30
Annex B – Operator action as an Independent Protection Layer (IPL)		47
B.1	Purpose	47
B.2	Key points.....	47
B.3	BPCS operator action	48
B.4	Operator-initiated SIF.....	48
B.5	Human response-time criteria	49
B.6	Verification of an operator-initiated SIF.....	52
Annex C – Management of functional safety		55
C.1	Purpose	55
C.2	Identification of the right people	55
C.3	Development of a work process.....	56
C.4	Roles and responsibilities matrix.....	56
Annex D – Verification, validation, and functional safety assessments		85
D.1	Purpose	85
D.2	Verification.....	85
D.3	Validation.....	85
D.4	Functional Safety Assessment (FSA)	86
Annex E – Audits.....		112

E.1	Purpose	112
E.2	Audit frequency	112
E.3	Audit participants.....	112
E.4	Auditing against requirements.....	112
E.5	Audit preparation	112
E.6	Audit kickoff.....	113
E.7	Audit protocol	113
E.8	Procedure review	113
E.9	Interviews	114
E.10	Record review	114
E.11	Field audit.....	114
E.12	Presentation of findings.....	114
E.13	Examples of audit findings	114
Annex F – BPCS and its relationship to the SIS		118
F.1	Purpose	118
F.2	Considerations on the use of the BPCS	118
F.3	Sharing the logic solver between the SIS and the BPCS	121
F.4	Physically separate and diverse SIS logic solver.....	123
F.5	Sharing of field devices between the BPCS and the SIS	124
F.6	Example	128
Annex G – Failures - Types, classifications, sources and strategy for defense		134
G.1	Purpose	134
G.2	Systematic failures	134
G.3	Random failures	135
G.4	Summary of differences between random and systematic failure	135
G.5	Failure classifications	135
G.6	Sources of failures by lifecycle phase	140
G.7	Common-cause failure	142
G.8	Strategy for defense against failures	143
Annex H – SIF versus interlocks, permissives, and inhibits		148
H.1	Purpose	148
H.2	Interlock.....	148
H.3	Permissives	149
H.4	Inhibits	149

Copyright 2011 ISA. All rights reserved.

H.5	Safety function.....	150
H.6	Safety Instrumented Function (SIF)	151
H.7	Safety Instrumented System (SIS).....	152
Annex I – Continuous, high, and low demand mode		154
I.1	Purpose	154
I.2	Introduction.....	154
I.3	Continuous mode examples.....	157
I.4	High-demand-mode examples	158
I.5	Low-demand examples	159
I.6	Application guidance	162
I.7	Consideration of diagnostics in high/continuous demand.....	163
Annex J – SIL 4 versus inherently safer design		165
J.1	Purpose	165
J.2	Re-evaluate the allocation of safety functions to protection layers	165
J.3	Reduce risk by applying inherently safer principles	166
Annex K – Fault tolerance topics		167
K.1	Purpose	167
K.2	General consideration	167
K.3	Fault tolerance and common-cause failures	168
K.4	Safe failure fraction	173
Annex L – Device selection.....		175
L.1	Purpose	175
L.2	Scope	175
L.3	Terminology.....	176
L.4	Device selection process	178
L.5	IEC 61508 compliance	178
L.6	ANSI/ISA-84.00.01-2004 prior use assessment	182
L.7	Optimal approach to device selection “user approved”	184
L.8	SIL claim limit considerations	194
Annex M – General purpose versus safety logic solvers		195
M.1	Purpose	195
M.2	General purpose logic solver background	195
M.3	General purpose logic solvers for safety applications	196
M.4	Safety-configured logic solvers for safety applications	197
M.5	IEC 61508 compliant PE logic solvers	197

Annex N – Design guidance	199
N.1 Purpose	199
N.2 Communications between BPCS and SIS	199
N.3 Architecture	200
N.4 Technology selection	200
N.5 Electronic technology used in SIS	202
N.6 PES technology used in SIS	203
N.7 Diagnostics	203
N.8 Field devices	206
N.9 User interface	208
N.10 Security	210
N.11 Wiring practices	211
N.12 Proof-test interval	212
N.13 Power sources	212
Annex O – Software	217
O.1 Purpose	217
O.2 What are the differences	217
O.3 Software design considerations	219
O.4 Handling of software systematic errors	220
Annex P – Response to detection of a dangerous fault	223
P.1 Purpose	223
P.2 The basics	223
P.3 Manual shutdown requirements	225
P.4 Fault tolerant mode – Demand and continuous mode	226
P.5 No fault tolerance - Demand mode	227
P.6 No fault tolerance - Continuous mode	227
P.7 Advantages and disadvantages of the diagnostic alarm response alternatives	227
P.8 Examples	229
Annex Q – Setpoint guidance	231
Q.1 Purpose	231
Q.2 Scope	231
Q.3 Definitions	231
Q.4 Establishment of setpoints	233
Q.5 Documentation	238

Copyright 2011 ISA. All rights reserved.

Q.6	Testing and maintenance of SIS setpoints	239
Annex R	– Key performance indicators	241
Annex S	– Differences between 1996 and 2004 versions	245
S.1	Clause 1 - Scope	245
S.2	Clause 2 – References	245
S.3	Clause 3 – Abbreviations and definitions	246
S.4	Clause 4 – Conformance to standard	246
S.5	Clause 5 – Management of functional safety	246
S.6	Clause 6 – Safety lifecycle requirements	247
S.7	Clause 7 – Verification	247
S.8	Clause 8 – Process hazard and risk analysis	247
S.9	Clause 9 – Allocation of safety functions to protection layers.....	249
S.10	Clause 10 – SIS safety requirement specification	250
S.11	Clause 11 – SIS design and engineering.....	250
S.12	Clause 12 – Requirements for application software, including selection criteria for utility software	251
S.13	Clause 13 – Factory Acceptance Testing (FAT)	251
S.14	Clause 14 – SIS installation and commissioning	251
S.15	Clause 15 - SIS safety validation	251
S.16	Clause 16 – SIS operation and maintenance	251
S.17	Clause 17 SIS modification	252
S.18	Clause 18 – SIS decommissioning	252
S.19	Clause 19 – Information and documentation requirements	252
Annex T	– Acronyms and abbreviations	255
Annex U	– References	259

This page intentionally left blank.

Copyright 2011 ISA. All rights reserved.

1 Purpose

ANSI/ISA-84.01-1996 has been retired and replaced with ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod). The new standard is the ANSI/ISA adoption of the international standard, IEC 61511, and includes one additional clause, a grandfather clause covering existing SIS (ANSI/ISA-84.00.01-2004 Part 1 Clause 1.0 y).

This technical report 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 lifecycle steps in ANSI/ISA-84.00.01-2004.

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

- Clause 1 is the purpose.
- Clause 2 explains the origins of the new standard and discusses its relationship to other regulations, standards, and practices.
- Clause 3 and Annex A specifically address the grandfather clause and provide guidance on the evaluation of existing SIS.
- Clause 4 provides an overview of the SIS lifecycle and references to subject-specific annexes for additional guidance on key issues.

There is nothing in this guideline that precludes, replaces, or makes obsolete any requirement of ANSI/ISA-84.01-1996 or ANSI/ISA-84.00.01-2004-1. This guideline is a “how to” approach and provides informative, non-mandatory methods.

2 Introduction

In the United States of America, the Occupational Safety and Health Administration (US-OSHA) regulation, 29CFR1910.119 (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 lifecycle 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 practices 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 sector. Through ANSI/ISA-84.01-1996, owners/operators have become familiar with terms, such as safety integrity levels, safety instrumented systems, and safety functions (i.e., safety instrumented function).

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-sector standard.

Copyright 2011 ISA. All rights reserved.

The IEC 61511 committee was formed to specifically address the process sector under the framework of IEC 61508. This international consensus standard was issued in 2003. With the completion of IEC 61511, the ISA84 committee accepted IEC 61511 as ISA-84.00.01-2004 (IEC 61511 modified). Once the standard was accepted by ISA, the ISA84 committee immediately initiated the development of this guideline. ANSI approved the new standard as ANSI/ISA-84.00.01-2004 in September 2004.

- The 1st edition of ISA-TR84.00.04 was intended for readers who were familiar with ANSI/ISA 91.00.01-2001, ANSI/ISA-84.01-1996, ISA-TR84.00.02, ISA-TR84.00.03, and ANSI/ISA-84.00.01-2004 (IEC 61511 modified).
- ISA-TR84.00.04-1 Annex S provides an overview of the differences between ISA-84.01-1996 and ISA-84.00.01-2004.
- This 2nd edition of ISA-TR84.00.04-1 amends and updates some guidance, but predominantly expands guidance related to user approval (Annex L), setpoint determination (Annex Q), and performance metrics (Annex R). 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.

3 Grandfather clause

The concept of the grandfather clause in ANSI/ISA-84.00.01-2004-1 originated with OSHA 1910.119. The grandfather clause's intent is to recognize prior good engineering practices (e.g., ANSI/ISA-84.01-1996) and to allow their continued use with regard to existing SIS.

The grandfather clause (ANSI/ISA-84.00.01-2004-1 Clause 1.0 y) states: "For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard (e.g. ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner."

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

The grandfather clause establishes that the owner/operator of an SIS designed and constructed prior to the issuance of the standard should demonstrate that the "equipment is designed, maintained, inspected, tested and operating in a safe manner." There are two essential steps:

- 1) Confirm that a hazard and risk analysis has been done to determine qualitatively or quantitatively the level of risk reduction needed for each Safety Instrumented Function (SIF) in the SIS.
- 2) Confirm that an assessment of the existing SIF has been performed to determine that it delivers the needed level of risk reduction.

NOTE The evaluation of the SIF should take into account various factors, such as device failure rates and associated design, operation, maintenance, testing, inspection and management-of-change practices.

If the above activities have not been done, they should be scheduled for review at the next appropriate opportunity. Various considerations related to timing are discussed in ISA-TR84.00.04-1 Annex A.2.

The grandfather clause releases the owner/operator from the design and construction requirements of ANSI/ISA-84.00.01-2004-1 for existing installations if they can demonstrate these criteria. This leads to questions regarding how to demonstrate compliance with the grandfather clause and at what point modifications to the process or the SIS have become significant enough to warrant reassessment of the adequacy of the SIS.

Copyright 2011 ISA. All rights reserved.

NOTE 1 There are many processes that are not covered under OSHA 1910.119. Some owners/operators choose to manage these processes under the same program as their covered processes. The discussion in this section is considered applicable to non-covered process SIS.

NOTE 2 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 (Non-mandatory) and in various compliance letters published on www.OSHA.gov). The guidance provided in this clause and ISA-TR84.00.04-1 Annex A is intended to supplement the US-OSHA guidance and to provide examples of methodologies that various owners/operators are using to determine whether their SIS meets the intent of the grandfather clause (ANSI/ISA-84.00.01-2004-1 Clause 1.0 y).

3.1 General considerations

The owner/operator should be aware that the grandfather clause only addresses the SIS design and construction. The other requirements of ANSI/ISA-84.00.01-2004-1 should still be implemented, as appropriate. Documentation, procedures, training, testing, and auditing requirements of ANSI/ISA-84.00.01-2004-1 are applicable to all SIS, whether existing or new.

It is important for the owner/operator to develop an approach for addressing existing SIS. It is the responsibility of the owner/operator to determine that existing SIS meet the intent of the grandfather clause 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 and document” the applicability of the grandfather clause. ISA-TR 84.00.04-1 Annex A is a collection of methods used by various owners/operators on the ISA84 committee.

3.2 Management of change considerations

Owners/operators of grandfathered SIS (i.e., those SIS that have been determined to meet the intent of ANSI/ISA-84.00.01-2004-1 Clause 1.0y) should acknowledge that this status does not provide an indefinite shield against the full requirements of ANSI/ISA-84.00.01-2004-1. The grandfather clause does not protect any owner/operator from the OSH Act General Duty clause, which requires that owners/operators provide a safe working environment. And 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 OSH Act, 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 trigger a management of change (MOC) review of the grandfather clause status of the SIS. The following sections provide examples of criteria that can be used to trigger a reassessment of the applicability of the grandfather clause.

3.2.1 Process design

Any change to the process design, which changes the Process Flow Diagrams or considerably revises the Process and Instrumentation Diagrams (P&IDs), can be expected to have an impact on the definition of the SIF used to mitigate the process risk. The addition of new process equipment may require the addition of new SIFs. The addition of a new chemical to the process could change the process hazard, create new process hazards, and/or change the demand rate on the SIF. Existing SIFs that are affected by a modification may also require re-design due to changes in the potential process hazard, the definition of the safe state of the process, or the performance requirements of the SIS.

3.2.2 Safety Requirements Specification (SRS)

The SRS provides the functional and integrity requirements for each SIF implemented in an SIS. Changes to the SRS that may impact the grandfather status of the SIS are as follows:

- changes in the definition of the safe state of the process (e.g., modification of the SIS action),
- changes in the functional relationship between process inputs and outputs,
- changes in the selection of energize or de-energize-to-trip,
- changes in the expected SIS performance (e.g., increase in the expected number of demands on the SIS, increase in the expected consequence of the event, the removal or decrease in the risk reduction of other independent protection layers, which increase the SIS requirements),
- changes in the safety integrity level, and
- changes in the required testing interval.

3.2.3 SIS Design

Changes in the SIS design should be evaluated for impact to the functionality and integrity of each SIF. Any change that can impact the SIL should be carefully evaluated. Examples include:

- changes in the separation of the SIS and the BPCS,
- changes in SIS logic solver technology ,
- changes in redundancy and architecture for process sensors, logic solver, or final elements (e.g., 1-out-of-2 to 2-out-of-2 sensors),
- changes in the power sources to SIS elements (e.g., electrical power, hydraulic power, pneumatic power),
- changes in the field device type or technology,
- changes in device failures (e.g., hardware aging, impact of process is greater than expected),
- changes in process demand on the SIS,
- changes in SIS equipment manufacturer,
- modifications to the operator; maintenance/engineering; and communications interfaces,
- changes in the SIS environmental controls (should remain within manufacturer specified ranges),
- changes in facilities for SIS maintenance and testing (changes in mechanical or electrical equipment involved in testing, not changes in testing interval), and
- changes in wiring practices.

Copyright 2011 ISA. All rights reserved.

3.2.4 SIS operation, maintenance, testing, and inspection

When evaluating changes to operating and maintenance procedures, it is important to keep in mind that only those changes that can have a negative impact on the process risk need to be considered. One possible change that may significantly impact the requirements or performance of the SIS is extending the plant turnaround schedule such that offline inspection, preventive maintenance, and proof testing are performed less frequently. Another possible change is a large reduction in operations or maintenance manpower. As owners/operators reduce the available workforce, it may become difficult for the operators to fulfill their requirements in response to SIS trips or alarms. SIS performance problems may also result from reduced or inexperienced maintenance support. These issues potentially include:

- reduced operator diligence in diagnosing failures of SIS equipment,
- inability of maintenance to respond to SIS failures in a timely manner,
- increased errors in SIS equipment repair, calibration, inspection or testing due to, among other causes, loss of plant knowledge through retirement of experienced personnel or transfer of duties to external contractors,
- reduced efforts in preventive maintenance, and
- reduced documentation of problem resolution.

These inadequacies could lead to an increase in systematic errors due to inadequate testing or errors in calibration and repair activities.

3.2.5 Management of change

Even if an existing SIS has been found to meet the intent of the grandfather clause, changes to the SIS or the process to which it is providing protection may trigger the need to formally re-evaluate its grandfather status. Therefore, MOC procedures should specifically address the issue of SIS modification. An MOC review should be conducted whenever the change potentially affects the process risk.

Within ANSI/ISA-84.00.01-2004-1, MOC is a significant phase of the Safety Lifecycle Model. Prior to the initiation of a change to the SIS or to the process, the impact of the change on the SIS performance should be assessed according to the requirements of the appropriate lifecycle phase, i.e., the first phase affected by the modification. The elements of all subsequent lifecycle phases are then addressed. This includes evaluating the effect of the change on the SIL.

4 Overview

ANSI/ISA-84.00.01-2004-1 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 process to ensure 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 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 has the lowest (highest PFD_{avg}) and SIL 4 has the highest (lowest PFD_{avg}) performance.

Achieving these performance ranges requires that the SIS be rigorously designed 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 operation requires that the process design, SIS design, and operation and maintenance procedures are successfully integrated to achieve high integrity and reliability.

Copyright 2011 ISA. All rights reserved.

Finally, the management strategy should incorporate periodic assessments of existing equipment performance to identify opportunities for further reduction of risk, thus yielding safer operation.

4.1 Lifecycle approach

ANSI/ISA-84.00.01-2004 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 facility management system for how SIS are identified, designed, inspected, maintained, tested, and operated to achieve safe operation and perform a hazard and risk analysis to identify where SIS 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, start-up, 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 improve its performance.

The lifecycle 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 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. ISA-TR84.00.04-1 Annexes C, D, and E provide additional guidance on the management of functional safety.

4.2 Define a risk-management strategy

A chemical process operator has cradle-to-grave responsibility for a facility's safe operation. Risk derived from the operation of chemical processes can be successfully and cost-effectively managed throughout the life of the process. The earlier a risk-management strategy is defined, the better it will work and the less it will cost. Identify process hazards early in the project planning and process design, so measures can be implemented to reduce or eliminate hazards through inherently safer design.

Once process design is complete, the risk associated with process operation will need to be managed for the life of the process equipment. Although inherently safer design may increase the initial capital cost, it substantially reduces long-term risks and their associated costs. Safety systems should only be applied when inherently safer design becomes impractical because safety equipment requires long-term investment in administrative, operating, and maintenance activities.

To develop the risk-management strategy, start with a process hazards analysis (PHA) and review the process design and its control, operation, and maintenance practices. Select a multidisciplinary team with expertise in these areas, and use an accepted hazard-evaluation procedure, such as a hazard and operability (HAZOP), what-if, or checklist analysis, to determine how process deviations from intended

Copyright 2011 ISA. All rights reserved.

operation lead to process hazards. ISA-TR84.00.04-1 Annex I provides guidance for instances where the SIF operates in high demand or continuous mode.

Identify the causes or conditions that lead to deviations. For example, low flow can be caused by the failure of the flow control loop. Events can be caused by a single failure or by multiple failures. Ensure that the identified causes are the minimum that will lead to the process deviation. The most common initiating causes are related to control system failures, which can happen multiple times over the life of the process. If the consequence is significant, safety systems are generally required to address identified process hazards.

Estimate the severity of the consequence, taking into account likely event conditions. Occupancy during an abnormal event is typically not the same as during normal operation. If abnormal operation occurs, what are the responsibilities of the field operators or maintenance crew? If a safety alarm goes off, is the field operator expected to respond locally? The slower the event, the more likely there will be field response and higher occupancy, possibly including supervisory, operations, and maintenance personnel. ISA-TR84.00.04-1 Annex B provides guidance with respect to the role of the operator in process safety.

The process risk of a particular event is related to how often the event could occur and the severity of the consequences if it does. Compare the process risk to facility risk criteria to determine if the risk is tolerable or whether additional protection is required to reduce it below the defined criteria. Residual risk represents a likelihood that an unacceptable consequence could occur, so drive it as low as reasonably practicable. ISA-TR84.00.04-1 Annex J provides guidance on how to address process risk that requires SIL 4 equivalent risk reduction.

To lower risk, implement a defense-in-depth strategy in which one or more independent protection layers (IPLs) act to interrupt the event sequence. Verify during the PHA that identified IPLs are designed to detect and respond to the hazardous event in a timely manner. IPLs can be implemented using a variety of systems, such as safety alarms, pressure relief devices, and SIS. ISA-TR84.00.04-1 Annex H clarifies the differences between interlocks, permissives, inhibits, safety functions, SIS, and SIF. Independence is achieved when the IPL operation is not affected by the occurrence of the initiating event or by the failure of other IPLs. ISA-TR84.00.04-1 Annex G discusses SIF failure and measures that should be taken to reduce the likelihood of failure. In addition to addressing the risk arising from identified process deviations, the risk-reduction strategy should also address secondary consequences associated with the operation of the IPLs, such as reduced production, shutdown, and flaring. Secondary 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 side effects are acceptable or properly managed.

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 potential hazardous events
- Selection of equipment based on prior history
- Fault detection, such as diagnostics and proof testing
- Fault tolerance against dangerous failures
- Procedures for maintenance and test, 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
- Start-up and shutdown of the process equipment

The SIS design basis is covered by ANSI/ISA-84.00.01-2004 (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

The SIS should also be designed to be separate and independent from the basic process control system to provide protection against postulated control system malfunctions. ISA-TR84.00.04-1 Annex F provides guidance with respect to the role of the Basic Process Control System (BPCS) in process safety. SIS operate best when they are initiated by direct measurement of the process deviation and take action on the process in a manner that directly addresses the deviation, thereby achieving or maintaining a safe state. For example, “when the high-pressure alarm initiates, open the pressure control vent,” or “when high temperature occurs, close the steam valve.” This logic is simple enough that it can be implemented in a hard-wired system. Use programmable logic controllers (PLCs) when the process logic is complex, requires sequencing, or needs to be adjusted on operating mode.

4.3.2 PLCs

PLCs are complex integrated systems with the potential for large numbers of random and systematic failures. Because of the failure potential, ANSI/ISA-84.00.01-2004 (Clause 11.5) requires safety-configuration of PLCs for SIS. 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 needed to identify and manage PLC failures in safety applications. ISA-TR84.00.04-1 Annex M 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 mechanical integrity practices. ISA-TR84.00.04-1 Annex L provides guidance on the selection of SIF devices. An SIS must be sufficiently robust to meet the required SIL under operating environment conditions. For each installation, define the conditions that impact SIS equipment selection, such as:

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

Copyright 2011 ISA. All rights reserved.

4.3.4 Response time

The SIS must detect the process hazard and respond in time to prevent the hazardous event. 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 a preferred sequence. The available process safety time for any given safeguard starts when it is required to take action and ends at the point where the event can no longer be prevented. In many applications, it is desirable that each safeguard be capable of completing its action prior to the initiation of the next one in the sequence, the goal being to achieve or maintain a safe state with the safeguard that causes the least impact to process operation. Regardless, the need to allocate a limited process safety time to multiple safeguards leads to less time being available for safeguards operating later in the sequence.

The SIS begins protective action at a defined process condition or setpoint. ISA-TR84.00.04-1 Annex Q 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 that must be removed. It can also be short (milliseconds), such as stopping a motor. Given the degree of uncertainty in the process safety time, the SIS should be capable of completing its action within one-half of its allocated process safety time.

4.3.5 Support system considerations

Assess potential common causes in the process support systems, such as power, communications, instrument air, cooling water and hydraulic power. ISA-TR84.00.04-1 Annex K.3.3 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-84.00.01-2004 Clause 11.9 also requires that the SIS PFD_{avg} 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, that the subsystems meet minimum fault tolerance requirements, and that the system achieves the required functionality and integrity. ISA-TR84.00.04-1 Annex K provides further discussion on fault tolerance. SIS equipment should be included in a mechanical integrity program that seeks to maintain the SIS in the "as good as new" condition. Mechanical integrity 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 initial proof-test interval is determined based on 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, online proof-test and repair facilities will be necessary. If the online 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 allowable repair time. Implement bypass alarms when practical, and ensure operating procedures adequately communicate bypass activity across operator shift changes, e.g., re-initiate bypass and safety alarms across shifts. Ensure that operators know the state of SIS equipment and what to do if abnormal

operation occurs. ISA-TR84.00.04-1 Annexes B and P provide guidance on operator response to alarms and compensating measures when operating with a detected failure.

4.4 **Validate, start-up, operate, and maintain the strategy**

The SIS must undergo validation to obtain formal acceptance of the SIS by the plant operations staff. The equipment is proven to work as required, and from this point forward, changes are reviewed and approved according to the plant's management-of-change practices. Validation is performed after instrument calibration and loop checks have been completed. A validation plan is developed to ensure orderly execution and thorough documentation and resolution of any findings. ISA-TR84.00.04-1 Annex D provides further discussion on conducting functional safety assessments during the SIS lifecycle.

Validation demonstrates that the installed SIS operates according to the design basis and that appropriate documentation is in place to support its 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 must be completed prior to the initiation of any operating mode where a hazardous event could occur that would require the operation of a new or modified SIS. Some users require that validation be repeated after any major process outage or shutdown.

Clearly define the safe operating limits in the operating procedures, the consequences of deviating from these limits, and the proper action to take when these limits are exceeded. The operator's response to an indication, alert, alarm, or incident is dictated first by procedures and training and then by experience. Validate the operator's response to SIS diagnostic and safety alarms. ISA-TR84.00.04-1 Annex B provides guidance on SIS alarms. ISA-TR84.00.04-1 Annex P provides application guidance regarding system behavior on detection of a fault. ANSI/ISA-84.00.01-2004 (Clause 16 and 17) addresses operator and maintenance procedure requirements for SIS. Procedures should include:

- a description of the hazardous events being prevented
- a description of the SIS
- the appropriate operator response to detected SIS equipment failure and provisions for operation with detected faults (i.e., compensating measures)
- coordination/communication with maintenance during any troubleshooting, repair or test activity
- conditions under which it is safe to reset the SIS
- use of start-up bypasses and the process conditions to be monitored during start-up
- the expected operator response when safety alarms 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, never deviate" process conditions that require manual shutdown

Copyright 2011 ISA. All rights reserved.

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 it 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 pre-installation storage, poor installation practices, or sloppy construction 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 mechanical integrity practices have been cited as a primary cause of equipment failure (HSE, 2005). Preventive maintenance can extend equipment useful life and improve its reliability. Mechanical integrity records provide data that equipment is being maintained in the “as good as new” condition and justify its continued use. Consequently, maintenance personnel must be trained on the activities necessary to ensure equipment integrity.

Periodic proof tests should be performed at a frequency sufficient to detect the transition from the useful-life period to the wear-out period, so that the need for equipment replacement or upgrade can be identified and planned (refer to ISA-TR84.00.03 for additional guidance on mechanical integrity of SIS). Equipment failure should be investigated using root-cause analysis to reduce or eliminate failure causes, such as changes to the installation or replacement of the equipment with something more suitable for the operating environment. The proof-test interval should be periodically evaluated based on plant experience, hardware degradation, demonstrated software reliability, etc. In the event that the equipment performance does not meet the SIL requirements, the mechanical integrity 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).

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 operating modes. Documentation 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. Use the proof-test results and findings to train personnel and to verify procedure clarity and completeness. Implement procedures to track the time that the equipment is out of service and to ensure that the equipment is returned to service following testing (refer to ISA-TR84.00.03 for additional guidance).

Actual risk reduction can be demonstrated by mechanical integrity data and plant performance (refer to ISA-TR84.00.04-1 Annex R and ISA-TR84.00.03). The records associated with any SIS must show that the equipment can operate as specified during all intended operating modes. Failure tracking and analysis is essential to quality assurance. Repeated failures likely indicate that the installed equipment is not capable of meeting the performance requirements. Use root-cause analysis to determine why metrics are trending in the wrong direction in order to implement action plans that improve the management system, equipment, procedures, and personnel training. Identify special and previously unknown failures and communicate these to personnel, ensuring that lessons learned are not hidden in mechanical integrity records.

4.5 Manage changes to the strategy

A successful risk-management strategy accepts that humans are involved in every aspect of an SIS 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. Human error must be reduced to the point where it does not significantly impact system integrity. Assurance of personnel competency is key. ISA-TR84.00.04-1 Annexes C, D, and E provide guidance with respect to management of functional safety.

Refer to ISA-TR84.00.03 for additional guidance of determining the competency of those associated with the mechanical integrity plan.

Knowledge evolves over time as research and development yields operational enhancements to process facilities. ISA-TR84.00.04-1 Annex R 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 initiate, document, review and approve changes to SIS 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 hazard analysis is required and why tracking change is important. ISA-TR84.00.04-1 Annex E 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 process hazard analysis and should be auditable.

Copyright 2011 ISA. All rights reserved.

Annex A – Example methods for determining grandfather status

NOTE -- Annex A is referenced in Clause 3.0.

A.1 Purpose

As discussed in Clause 3, the purpose of this annex is to illustrate approaches for determining whether an existing SIS meets the intent of the grandfather clause (ANSI/ISA-84.00.01-2004-1 Clause 1.0 y). There are two essential steps:

- 1) Confirm that a hazard and risk analysis has been done to determine qualitatively or quantitatively the level of risk reduction needed for each SIF in the SIS.
- 2) Confirm that an assessment of the existing SIF has been performed to determine that it delivers the needed level of risk reduction.

NOTE -- The evaluation of the SIF should take into account various factors, such as equipment failure and associated design, operation, maintenance, testing, and inspection work practices.

If the above activities have not been done, they should be scheduled for review at the next appropriate opportunity.

Clauses A.3.1 through A.3.8 provide examples of methods used by some owners/operators in evaluating existing SIS. These methods are provided as examples and should not be considered the only acceptable approaches. The owner/operator should select a method or methods based on their hazard- and risk-analysis philosophy and prior design practices with consideration for the following:

- Development of a method for “determining and documenting” the grandfather status of the SIS,
- Integration of this method into the existing process safety management program, and
- Consistent application of the method, considering potential risks to human health and the environment.
- Once an owner/operator determines that the existing SIS does not meet the intent of the grandfather clause, there should be a defined decision-making 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

The owner/operator should document the adequacy of the SIS at the cyclic PHA. Analysis of the adequacy of the SIS should be expedited if the following occurs:

- Modifications to the process unit that impact process risk managed by the SIS
- NOTE -- ISA-TR84.00.04-1 Clause 3.2 provides a list of management-of-change considerations.
- Modifications to the control system that impact protection layers used to achieve safe operation
 - When an incident or near-miss investigation has identified an SIS deficiency

- When the review of another process unit designed according to similar practice has identified an SIS deficiency

A.3 Approaches to the grandfather clause

Clauses A.3.1 through A.3.8 provide eight different approaches used by owners/operators in the evaluation of the applicability of the grandfather clause. These methods are provided for illustrative purposes only. Owners/operators are responsible for developing a method for use at their facilities.

A.3.1 Comparison with SIL requirements

At a minimum, the adequacy of an existing SIF should be reviewed and documented at the cyclic PHA, such as those required by OSHA 1910.119. The cyclic PHA is one of the principal opportunities to review an existing SIF and ensure its design and performance satisfies expectation. During the PHA, the team identifies potential causes of process hazards and the associated consequence severity for various hazard scenarios.

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 are provided by the existing design. This assessment is sometimes performed as part of the PHA 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 may include a calculation of the Probability of Failure on Demand (PFD_{avg}) for the SIF. The actual PFD_{avg} is then compared to the SIL assigned by the PHA team. If the actual 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 management-of-change documentation associated with the existing SIS. If changes have been made to the process that might impact the expected performance requirements for

Copyright 2011 ISA. All rights reserved.

the SIFs implemented in the SIS, the team reviews the PHA (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 PHA 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 ten years, but, in reality, the SIF is exposed to one demand a year, the team modifies the PHA 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 re-evaluated. 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.3.2 Comparison with existing design basis

A flow diagram (Figure A.1) is provided to illustrate the method discussed in this section. This method provides one approach for evaluating the grandfather status of an SIS. Alternative approaches can be used. The owner/operator should decide and document which approach is suitable for their process facility.

Step 1. Define process facility grandfather clause application rules.

After reviewing ISA-TR84.00.04-1 Clause 3.0, the owner/operator establishes ground rules that are to be implemented whenever existing SIS are analyzed for grandfather clause application. An example of ground rules is provided in Table A.1.

Table A.1 — Example Ground Rules (GR)

NOTE -- Example provided by one owner/operator

GR-1	The owner/operator utilizes approved and documented existing good engineering practices, such as: ANSI/ISA-84.01-1996, ISA "Alarm & Interlock Systems" 1984, ISBN 0-87664-736-0, or Corporate standards. NOTE -- Corporate standards should be verified against key ANSI/ISA-84.00.01-2004-1 requirements to determine their suitability.
GR-2	The plant processes to be considered for grandfather clause implementation are process sector-related (e.g., continuous and batch) processes only.
GR-3	The process facility ground rules for upgrading each SIF are based on the following: a. An SIF whose design basis is not in compliance with GR-1 should be upgraded to ANSI/ISA-84.00.01-2004-1 as soon as possible. b. An SIF whose design basis meets GR-1 should be upgraded to ANSI/ISA-84.00.01-2004-1 as part of the next cyclical PHA review.

Step 2. List existing SIFs, then select one SIF at a time and proceed as noted below.

Step 3. Identify the design basis for each SIF.

Copyright 2011 ISA. All rights reserved.

Step 4. Analyze the SIF design basis and determine if it meets the grandfather clause ground rules.

- a) If the SIF does not meet GR-1, then the SIF should be upgraded to meet ANSI/ISA-84.00.01-2004-1 as soon as possible.
- b) If the SIF does meet GR-1, each SIF should be evaluated to determine if it is designed, installed, maintained, inspected, tested, and operating according to the design basis.
- If the SIF is designed, installed, maintained, inspected, tested, and operating according to the design basis, the grandfather clause is applicable.
- If the SIF is not designed, installed, maintained, inspected, tested, and operating according to the design basis, the SIF should be upgraded to meet the design basis.

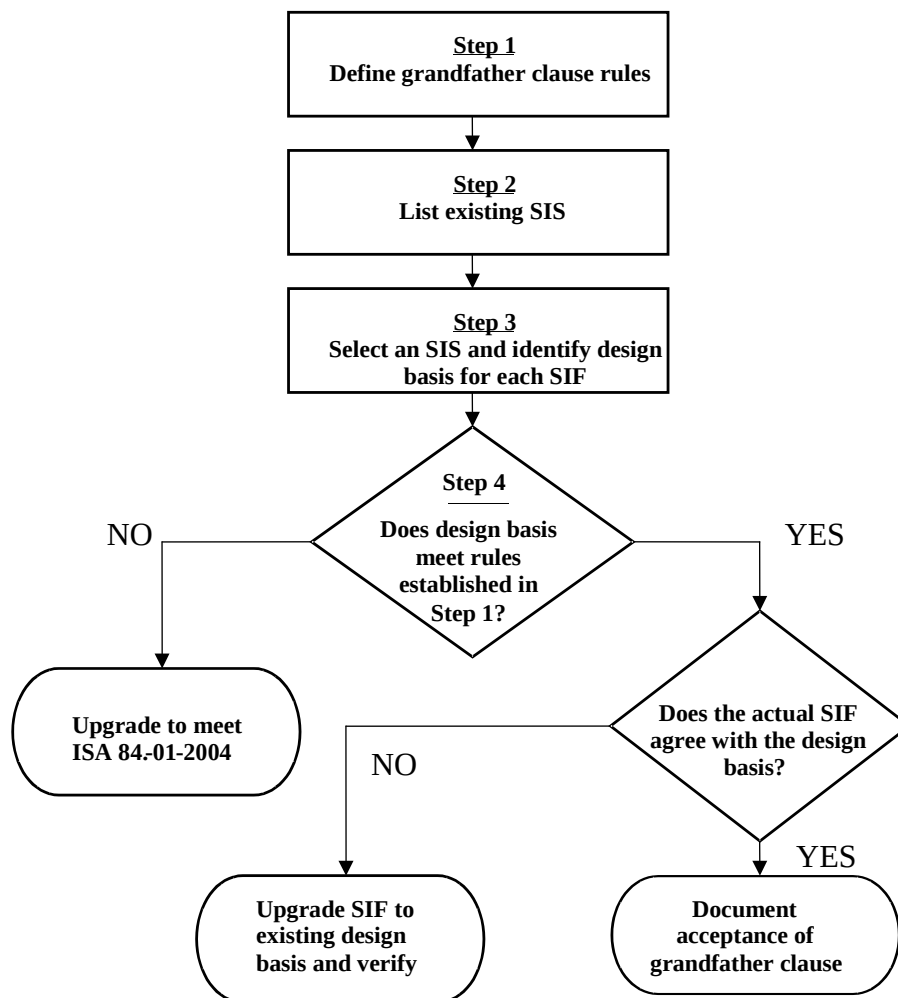


Figure A.1 — Flow diagram for example approach presented in Annex A.3.2

Copyright 2011 ISA. All rights reserved.

A.3.3 Comparison with key ANSI/ISA-84.01-1996 requirements

In this method, the owner/operator conducts an assessment, comparing the existing SIS to key requirements in ANSI/ISA-84.01-1996. Prior to the issuance of ANSI/ISA-84.00.01-2004-1, ANSI/ISA-84.01-1996 was used as a good engineering practice for SIS by this owner/operator. The following questionnaire was designed for use in verifying whether existing SIS meet the intent of the requirements in ANSI/ISA-84.01-1996. To qualify for grandfathering using this method, any shortfall (i.e., less than 100%) requires a plan to bring the SIS in question into compliance with ANSI/ISA-84.00.01-2004-1.

NOTE 1 A Safety Instrumented System (SIS) should be designed, built, tested, and maintained to provide the required risk reduction.

NOTE 2 Example provided by one owner/operator.

Table A.2 — Checklist for example approach presented in Annex A.3.3

No.	Question
1.	What percentage of the SIS are defined? – e.g. any of the following: logic narrative, cause and effects matrix, logic diagram. a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ Comment/explanation:
2.	What percentage of the SIFs implemented with the SIS have a SIL assigned to them? a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ Comment/explanation:
3.	What percentage of the SIS were designed and built to meet the SIL of the SIF? a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ Comment/explanation:
4.	What percentage of SIS are tested frequently enough to maintain the SIL of the SIF? a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ e. Don't know _____ Comment/explanation:
5.	Do current maintenance practices support the SIL of the SIFs – is the assumed Mean Time to Repair (MTTR) on fault detection met? This should include analog input maintenance based on deviation alarms. a. yes _____ b. no _____ c. don't know _____ d. SIFs are tested at the following frequency ____. Comment/explanation:

No.	Question
6.	Are SIS smart sensors write-protected, and do they require a safety review for modification? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
7.	How well are the maintenance personnel or computer support personnel (whoever maintains the SIS) trained on the SIS? a. well trained _____ b. adequately trained _____ c. poorly trained _____ d. not trained _____ Comment/explanation:
8.	How well are maintenance procedures maintained for the SIS? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
9.	How well is maintenance documentation maintained? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
10.	How well are Operations personnel trained on the SIFs of the SIS? a. well trained _____ b. adequately trained _____ c. poorly trained _____ d. not trained _____ Comment/explanation:
11.	How well are operating procedures maintained for the SIS? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
12.	How well are the results of the SIS online testing documented? a. well documented _____ b. adequately documented _____ c. poorly documented _____ d. not documented _____ Comment/explanation:

Copyright 2011 ISA. All rights reserved.

No.	Question
13.	What percentage of SIS inputs and outputs is shown on the P&IDs? a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ Comment/explanation:
14.	Are the SIS hardware, embedded software, and utility software under a formal revision and release control program? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
15.	Who on your site receives the critical problem notifications from the SIS manufacturer? a. name _____ b. don't know _____ Comment/explanation:
16.	Is the SIS application logic under a formal revision and release control program? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
17.	Do all SIS energize-to-trip circuits have an end-of-line current monitor? a. yes _____ b. no _____ c. don't know _____ d. does not apply, all circuits are de-energized to trip _____ Comment/explanation:
18.	Are SIS Inputs or outputs forced as part of operating procedures? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:

A.3.4 Comparison with key ANSI/ISA-84.00.01-2004-1 requirements

Another approach to SIS evaluation is the development of a checklist based upon ANSI/ISA-84.00.01-2004-1 requirements. The checklist should address major philosophical and technology issues defined in ANSI/ISA-84.00.01-2004-1. Any "no" answers (e.g., response other than "a") would exclude the SIS under consideration from the "grandfather" clause. A few examples of the types of questions that could be addressed in the checklist are provided below.

NOTE -- Example provided by one owner/operator.

Table A.3 — Checklist for example approach presented in Annex A.3.4

No.	Question
1.	Are the SIS defined? – E.g., any of the following: logic narrative, cause and effects matrix, logic diagram. a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
2.	Have the Safety Instrumented Functions (SIFs) implemented with the SIS been assigned a Safety Integrity Level (SIL)? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
3.	Are SIS field devices and logic solver independent of the initiating cause? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
4.	Are SIS field devices and logic solver independent of other protection layers? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
5.	Are the SIS designed and built to meet the SIL of the SIF? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
6.	Are the SIS tested frequently enough to maintain the SIL of the SIF? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
7.	Are the SIS designed to meet the required fault tolerance for the SIL of the SIF? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
8.	Are field devices and logic solver functionally separate from the BPCS? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____

Copyright 2011 ISA. All rights reserved.

No.	Question
9.	Do current maintenance practices support the SIL of the SIFs – is the assumed MTTR on fault detection met? This should Include analog input maintenance based on deviation alarms. a. yes _____ b. no _____ c. don't know _____ d. SIFs are tested at the following frequency ____. Comment/explanation:
10.	Are SIS smart sensors write-protected and do they require a safety review to modify? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
11.	How well are the maintenance personnel or computer support personnel (whoever maintains the SIS) trained on the SIS? a. well trained _____ b. adequately trained _____ c. poorly trained _____ d. not trained _____ Comment/explanation:
12.	How well are maintenance procedures maintained for the SIS? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
13.	How well is maintenance documentation maintained? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
14.	How well are Operations personnel trained on the SIFs of the SIS? a. well trained _____ b. adequately trained _____ c. poorly trained _____ d. not trained _____ Comment/explanation:
15.	How well are operating procedures maintained for the SIS? a. well maintained _____ b. adequately maintained _____ c. poorly maintained _____ d. not maintained _____ Comment/explanation:
16.	How well are the results of the SIS online testing documented? a. well documented _____ b. adequately documented _____ c. poorly documented _____ d. not documented _____ Comment/explanation:

No.	Question
17.	Are the SIS inputs and outputs shown on the P&IDs? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
18.	Are the SIS hardware, embedded software, and utility software under a formal revision and release control program? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
19.	Who on your site receives the critical problem notifications from the SIS manufacturer? a. name _____ b. don't know _____ Comment/explanation:
20.	Is the SIS application logic under a formal revision and release control program? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
21.	Do all SIS energize-to-trip circuits have an end-of-line current monitor? a. yes _____ b. no _____ c. don't know _____ d. does not apply, all circuits are de-energized to trip _____ Comment/explanation:
22.	Are SIS Inputs or outputs forced as part of operating procedures? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
23.	Historically, has the SIS performance met the operating demands? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:
24.	Historically, has the spurious activation of the SIS caused process incidents? a. yes _____ b. no _____ c. don't know _____ Comment/explanation:

A.3.5 Comparison to Accepted Prior Design Practices - A

Clause A.3.5 illustrates one company's approach to determining if an existing SIF meets the grandfather clause requirements. This approach involves four steps, as follows:

Copyright 2011 ISA. All rights reserved.

Step 1: The required risk reduction is determined for each SIF, using an approved hazard and risk analysis method.

Step 2: Review the historical performance of each SIF.

If the historical performance indicates the need to upgrade the current design and associated functions, the grandfather clause should not be claimed, and the SIF should be upgraded to meet ANSI/ISA-84.00.01-2004-1.

If the historical performance indicates the current design and associated functions are providing the desired safe plant operation, proceed to step 3.

Step 3: Select one SIF (with its associated risk reduction) at a time and compare the existing SIF against the required attributes in Table A.4. This table is developed for use by the owner/operator. It establishes a pre-existing list of ground rules to determine whether an existing SIF meets the required risk reduction. This table is used for existing SIFs only. **New or modified SIFs are designed in accordance with ANSI/ISA-84.00.01-2004-1.**

NOTE 1 When an owner/operator develops this type of method, the owner/operator should continuously evaluate their internal practices and corporate standards to ensure the ground rules and their associated risk reduction criteria are valid.

NOTE 2 Table A.4 defines minimum qualitative requirements that should be met for existing SIFs to be considered sufficient to meet a specific level of risk reduction.

NOTE 3 The required risk reduction is referred to as a risk reduction factor (RRF) in Table A.4. The values provided in the table represent the lower bounds of the range of risk reduction for which this architecture may be utilized, pending verification of the PFD_{avg} of the SIF. When the hazard and risk analysis establishes a risk reduction target of 10, the SIF should be designed to meet SIL 1 or a risk reduction factor of >10 to 99. Likewise, when the hazard and risk analysis establishes a risk reduction target of 100 the SIF should be designed to meet a risk reduction of >100 to 999 or, for a RRF of 1000 (SIL 3), the risk reduction target is >1000 to 9999.

If the SIF satisfies the minimum requirements of Table A.4, the SIF is considered to meet the grandfather clause. Proceed to step 4.

If parts of the SIF do not comply with the minimum practices or use any unacceptable practices (not acceptable) shown in Table A.4, those parts of the SIF should be upgraded to meet the minimum practices in Table A.4. Alternatively, an upgrade of the SIF in accordance with ANSI/ISA-84.00.01-2004-1 is recommended.

Step 4: Verify that the SIF meets its SIL requirements by acceptable analysis method(s).

Table A.4 — Checklist for example approach presented in Annex A.3-4

NOTE -- Example provided by one owner/operator.

GENERAL CATEGORY	SUBJECT	Independent protection layer specification credit from Risk Assessment		
		RRF 10 for SIS or BPCS or alarms	RRF 100 for SIS	RRF 1000 for SIS
SIS system hardware	Programmable Logic Solver (PLC)	Acceptable	Single system with diagnostic (overrun detection, fail safe properties) and watchdog or Dual system (without watchdog) 1oo2	Redundant system 1oo2 or Redundant systems 2oo3 with overrun detection and fail safe properties
	Programmable Logic Solver (PLC/SIS) with DIN certificate	Acceptable	AK 4*	AK 5* or higher 4 credits can be used for AK-6* certified systems (DIN VDE 801)
	Solid state logic	No requirements	System with fail safe logic	Advanced system with fail safe logic
	Pneumatic logic	Acceptable	Not acceptable	Not acceptable
	Relays	Acceptable	Acceptable if high grade commercial quality. Need to review each system on status.	No, unless guided contacts and prior use. No jumpers. Need to review each system on status.
	Distributed Control System (DCS)	Acceptable for 1 SIS credit or 2 credits for BPCS and Alarm on 1 platform if applied into different control boxes - prior use	Not acceptable	Not acceptable
SIS/ BPCS logic solver hardware requirements	Separate systems	Acceptable	Acceptable	Acceptable
	Integrated systems	Acceptable	Not acceptable unless IEC 61508 compliant	Not acceptable unless IEC 61508 compliant
SIS Logic solver Software requirements	Separate systems	Limited variability language (e.g. ladder logic), or requirements of the user and/or safety manual	Limited variability language (e.g. ladder logic) or requirements of the user and/or safety manual	Limited variability language (e.g. ladder logic) or requirements of the user and/or safety manual
	Integrated systems	Function protected against changes and override	See user and/or safety manual requirements	See user and/or manual requirements
	General verification requirements	Program verification performed and documented	For verification requirements from user and/or safety manual	For verification requirements from user and/or safety manual

Copyright 2011 ISA. All rights reserved.

GENERAL CATEGORY	SUBJECT	Independent protection layer specification credit from Risk Assessment		
		RRF 10 for SIS or BPCS or alarms	RRF 100 for SIS	RRF 1000 for SIS
Instrumentation (sensors)	"Smart" Instruments	Acceptable 1001/1002/ 2003/ 1002D/ 2002D	Acceptable 1002/ 2003/ 1002D/ 2002D	Acceptable 1002/ 2003/ 1002D/ 2002D
	Certified instruments	Acceptable	Acceptable	Acceptable
	Non-smart analog electronic Instruments	Acceptable 1001/1002/ 2003	Acceptable 1002/ 2003	Acceptable 1002/ 2003
	Pneumatic analog instruments	Acceptable 1001/1002/ 2003	Acceptable 1002/ 2003	Requires hazard and risk analysis team approval
	Discrete measurements (e.g. pressure switch)	Acceptable 1001/1002/ 2003	Acceptable 1002/ 2003	Requires hazard and risk analysis team approval
	Pneumatic transmitter with switches (behind panel)	Acceptable 1001/1002/ 2003	Acceptable 1002/ 2003	Requires hazard and risk analysis team approval
	Pneumatic transmitter with transducer (behind panel)	Acceptable 1001/1002/ 2003	Acceptable 1002/ 2003	Acceptable 1002/ 2003
Sharing of sensors	Separate sensors	Acceptable	Acceptable	Acceptable
	Shared sensors	Acceptable when two or more sensors are used	Acceptable when two or more sensors are used	Acceptable when two or more sensors are used
Instrument Installation	Instrumentation according to proven practice	Recommended	Recommended	Recommended
Final elements	Final elements from an approved manufacturer suppliers list	Acceptable 1001/1002	Acceptable 1001/1002	Acceptable 1002
	Control valve as final element if: -proof test and maintenance records demonstrate that it meets the shutoff & closing speed needs -the fail safe action is defined correctly -it is not shared with another IPL for the same scenario -the interlock has to work direct on the actuator	Acceptable if the valve is not the only IPL which reacts within the process safety time for this scenario (e.g. PSV or alarm but non-safety related)	Acceptable as second final element	Acceptable second final element NOTE: This architecture is not allowed for new or upgraded installations.
	Analog operated block valves with direct actuation of SIS function	Acceptable like normal block valves	Acceptable like normal block valves	Acceptable like normal block valves
Test frequencies calculated from PFD	Sensors	Use proven test interval or use default Mean Time to Failure (MTTF) from publications for PFD calculations	Use proven test interval or use default MTTF from publications for PFD calculations	Unless known, use default MTTF from publications for PFD calculations

GENERAL CATEGORY	SUBJECT	Independent protection layer specification credit from Risk Assessment		
		RRF 10 for SIS or BPCS or alarms	RRF 100 for SIS	RRF 1000 for SIS
	Logic solver system	Use system manufacturer MTTF data for PFD calculation	Use system manufacturer MTTF data for PFD calculation	Use system manufacturer MTTF data for PFD calculation
	Final element	Use proven test interval or use default MTTF from publications for PFD calculations	Use proven test interval or use default MTTF from publications for PFD calculations	Unless known use default MTTF from publications for PFD calculations
	Maintenance and repair	Procedures required. Repair time as required by instrument redundancy	Procedures required. Repair time as required by instrument redundancy	Procedures required. Repair time as required by instrument redundancy
General requirements	Test procedures	A detailed written test procedure should be prepared for each safety relevant instrument. Test procedures should incorporate the testing of each element in the loop, from the measuring element through the final control element.		
	Testing documentation	Records of test completion dates (as-found/as-left) should be kept for the current and preceding test (at least one year). The identity of the person conducting the test and any unsatisfactory performance of the instrument is recorded. A history of poor reliability or proof-test failures requires action plans to correct.		
	Fail safe design	Fail safe condition of loop components is defined		
	Overrides and bypasses	Generally no bypass or override should be designed or used. Any override or bypass needs separate evaluation and approval. A procedure should be followed when bypass or override is applied.		
	MOC	Any change to SIS should follow an MOC procedure.		
	Audits	Audit of SIS is done periodically as part of the US-OSHA safety audit. This audit reviews performance and adequacy of the SIF and SIS.		

* AK refers to the classification system established for PES in DIN VDE 0801, which is a German standard.

A.3.6 Comparison with Accepted Prior Design Practices - B

In this method, the company has an Accepted Prior Design Practice that documents minimum design requirements for the SIS. This design practice has been used for many years. To determine whether SIS designed in accordance with this design practice can be considered for grandfather status, a two-step evaluation is performed. First, SIL calculations are performed on the various SIS designed to the Accepted Prior Design Practice. The calculation determines the suitability of the design practice to achieve the risk reduction or integrity requirement. Second, the design practice is evaluated using a method similar to those described in Annexes A.3.3 through A.3.5. This evaluation determined whether SIS functionality is achieved. If the design practice is determined acceptable, any SIS designed in accordance with the practice can be considered for the grandfather clause.

Copyright 2011 ISA. All rights reserved.

For example, a company that is using their own classification system could map their internal classifications to the different SILs. Table A.5 shows an example of how one company made this comparison. The company should verify the SIL for the SIS that are grandfathered. SIL calculations of multiple examples from each SIL level should be conducted to validate the design practice. Any assumptions used to run the SIL calculations, such as testing interval, should be considered when granting grandfather status to a specific SIS.

Table A.5 — Example of Mapping Prior Design Practice Classification to SIL Levels

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.3.7 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 an 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 that 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-84.00.01-2004-1 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 for determining applicability of grandfathering are required. 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 a hazard and risk analysis (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.

A.3.8 Evaluation of existing automated shutdowns

Clause A.3.8 illustrates one company's approach to determining if an existing SIF meets the grandfather clause requirements. This approach involves three steps, as follows:

Step 1: Identify existing automated shutdowns.

Step 2: Perform Hazard and Risk Analysis (H&RA).

- Identify the hazard scenario(s) that each automated shutdown is protecting against.
- Identify the process risk of the hazard scenario(s).
- Determine the overall required risk reduction necessary to reduce the process risk to the defined risk criteria.
- Identify safety functions that fully mitigate the hazard scenario.
- Allocate risk reduction to each safety function as necessary to achieve the overall required risk reduction.
- Allocate each safety function to a protection layer that is designed and managed to achieve its allocated risk reduction.

Step 3 For each identified SIF, review the existing design and operating basis documentation for clarity, correctness, and completeness. The design basis documentation should cover the following areas at a minimum:

- Process hazard mitigated by the SIF.
- SIF description detailing the process variables measured and voting architecture, decision logic for initiation of the mitigating action, and the final elements and voting architecture along with any equipment necessary for actuation of the final elements (relays, solenoid operated valves etc.). Any support systems required for SIF, such as air/hydraulic/electrical supply should be documented.
- SIF reset functional description.
- SIF diagnostics and automated testing requirements.
- SIF alarms (diagnostic, pre-trip and trip, bypasses) requirements.
- SIF maintenance provisions (bypasses) requirements.
- SIF manual shutdown requirements.

Copyright 2011 ISA. All rights reserved.

- SIF logic solver requirements.
- SIF devices and required testing interval.

The operating basis documentation should cover the operation and maintenance requirements of ANSI/ISA-84.00.01-2004-1 in the following areas:

- Operating procedures
- Test procedures
- Management of change procedures, including software and configuration management
- Failure tracking procedures
- Training procedures
- Audit procedures

Step 4 A quantitative assessment of the existing SIF is performed to determine that the design basis and testing interval achieve the target SIL.

This page intentionally left blank.

Copyright 2011 ISA. All rights reserved.

Annex B – Operator action as an Independent Protection Layer (IPL)

NOTE -- Annex B is referenced in the following: Clause 4.2, Clause 4.3, Clause 4.4, Annex K.3.3.1, Annex N.9.2, Annex 9.3, and Annex P.2.

B.1 Purpose

The purpose of this Annex is to provide guidance for the design and limits of risk reduction that can be claimed where an operator, as a result of an alarm, takes action on the process to achieve a safe state or maintain safe operation.

NOTE 1 Refer to ANSI/ISA-84.00.01-2004-1, Clause 8.2.1, for requirements on hazard and risk analysis.

NOTE 2 Refer to ANSI/ISA-84.00.01-2004-1, Clause 11.3.1, through 11.3.3 for a discussion on the operator response to diagnostic faults.

ANSI/ISA-84.00.01-2004-1 establishes the premise that operator action can be a part of an SIF. The capability of the operator should be addressed when allocating risk reduction to an operator-initiated SIF.

NOTE -- Refer to ANSI/ISA-84.00.01-2004-1 Clause 3.2.72, NOTE -- 5, for additional guidance on the definition of SIS.

B.2 Key points

1. Operators often take control actions on a process through the BPCS. Normal process control actions are generally not considered safety functions.

2. When the operator is expected to take action in response to an alarm to prevent a process safety incident, the operator alarm and associated action is considered a safety function. These alarms are classified as safety-related and are designed and managed in a manner that supports the allocated risk reduction.

3. In general, no more than one order-of-magnitude risk reduction should be taken, irrespective of the number of alarms or the protection layer allocation. This is due to potential operator/procedural common-mode failure. Additional guidance on evaluating operator error is provided in Annex B.5.

4. Alarms for which an operator or facility worker is required to evacuate an area (e.g., fire and gas alarms) and are not intended to direct the operator to take action on the process are generally not considered safety instrumented functions. These alarms should not be allocated to the BPCS but may be allocated to the SIS or to another independent protection layer. Refer to Annex F, Figure F.1, for an overview of protection layers. These alarms are generally classified as safety-related and are designed and managed in a manner that supports the allocated risk reduction.

5. Alarms for which an operator is required to notify maintenance to repair a faulty SIS device in response to a diagnostic alarm may be part of the BPCS, but are subject to proof testing and management of change. These alarms should be classified as safety-related, and operators should be trained on the response to these diagnostic alarms. The devices should also be managed as safety-related instrumentation under the mechanical integrity program, ensuring that validation, access security, and management of change is practiced.

6. When credit for a risk reduction equal to or greater than 10 for a single operator action is proposed, the following should be considered:

NOTE -- Layer of protection analysis (LOPA) is often implemented as an order-of-magnitude assessment. Consequently, it is typical for the purpose of the LOPA calculation to assume a rounded off risk reduction factor of 10 for an operator action IPL implemented in the BPCS layer when it has met the other criteria discussed in this Annex and in Annex F.

- All hardware involved should fully meet the requirements of ANSI/ISA-84.00.01-2004.

Copyright 2011 ISA. All rights reserved.

- Potential credit for the operator should be determined via rigorous analysis.
- A program should be implemented to ensure that all human-error analysis assumptions are maintained or improved.

7. Process owners should also consider alarm-system guidance provided in other standards and practices. For example, the Engineered Equipment and Materials Users' Association (EEMUA), Health & Safety Executive (HSE), and The International Society of Automation (ISA) have developed extensive guidance on alarm management. Design of alarm systems should consider ISA 18.1-1979, ANSI/ISA 18.2-2009, ISA RP 60.3-1985, ISA RP 60.6-1984, EEMUA 191-2007, ANSI/IEEE-845-1999, ANSI/IEEE-Std 1023-2004, IEEE-1289-1998 and NUREG-0700 Rev 2-2002.

B.3 BPCS operator action

Operator actions that are implemented through the BPCS, in response to process conditions, can be credited with a risk reduction of less than 10 under the following conditions:

- The guidance in ISA-TR84.00.04-1 Annex F.2 is followed.
- There is sufficient time for operator response. Refer to B.5.
- Operator actions are covered by an operating procedure.
- The operator is trained on the procedure.
- All devices involved in the hazard scenario detection and response are subject to proof testing, access security, and management of change.

The hardware associated with a BPCS operator action is not covered by the standard. However, its performance should be monitored to ensure that it is sufficient. Formal PFD calculation is typically not required. Human factors should be considered in the design of any critical operator activity. For example, the design of the BPCS operator interface should incorporate human factors engineering (HFE) principals to ensure that the operator responds adequately to an alarm or process indication. However, a detailed human-error analysis is not required for operator actions implemented in the BPCS. Refer to Table B-1 for additional allocation and risk-reduction guidance.

B.4 Operator-initiated SIF

A risk reduction equal to or greater than 10 can be claimed where an operator, as a result of an alarm, takes action to place the process in a safe state. To take credit for a risk reduction equal to or greater than 10, a risk analysis should be performed to verify its feasibility. It is especially important to determine whether there is sufficient human response time. Refer to Annex B.5 for more discussion on human response time.

Operator-initiated SIFs can be allocated risk reduction when certain criteria are met. These criteria include consideration for the human factors of the operator interacting with the process and the integrity of the equipment used to bring the process to a safe state. For all safety-related operator actions, the alarm should be covered by a procedure that uses a clear and reliable indication that a defined action is required and includes a well-documented action. The devices should also be managed as safety-related instrumentation under the mechanical integrity program, ensuring that validation, access security, and management of change is practiced.

Copyright 2011 ISA. All rights reserved.

An operator-initiated SIF is often associated with a “never exceed never deviate” alarm, where the operator is expected to mitigate risk in much the same manner as an automated SIF. Operator-initiated SIFs are generally used when it is not possible to completely automate the function. The manually initiated action is typically comprised of the sensor detecting the hazardous condition, the logic solver that determines that the safety condition exists, alarm presentation, human response, and the equipment used by the operator to bring the process to a safe state. When risk reduction is taken for an operator-initiated SIF, the PFD_{avg} should be determined for the instrumented system. This is discussed further in B.6.

Finally, when allocating risk reduction, it is important to remember that one operator equals one response. Multiple alarms generally do not yield higher performance because the operator is the single point of failure for the necessary response. If the team has allocated risk reduction to an operator action in the BPCS layer, additional risk reduction should not be taken for an operator action allocated to the SIS layer for the same hazard scenario unless a detailed analysis is performed. When examining the overall risk reduction that can be provided by the alarms, it is important to recognize the potential for common-mode failure due to operator or procedural error.

B.5 Human response time criteria

Table B.1 provides an example of criteria that can be established for operator action as an IPL. According to this example, the risk reduction allocation is related to the protection layer allocation, human response time and the complexity of the action. The human response time should be less than the available process safety time, when an operator response to an alarm is being considered for reducing the risk of a specified hazard scenario. The available process safety time is the time it takes the process to go from the alarm condition to the hazardous condition. Human error occurs when an operator fails to respond correctly within the available process safety time.

The human response time is the time from the alarm/process indication to the completion of the actions necessary to place the process into a safe state. The human response can be broken down into four functions: (1) Recognize the unsafe condition, (2) Analyze the condition properly, (3) Perform the required safety action, and (4) Continue to monitor the process to determine whether safety actions were sufficient.

Sample times for human action in response to alarms are shown in Table B.1. These IPL time limits are based on research and are confirmed by industry experience. If the owner/operator wishes to use shorter response times or lower PFD_{avg} values, the owner/operator is cautioned to do a detailed human reliability assessment to confirm the assumed PFD_{avg} . The values in the table below represent the PFD of the entire IPL. They are not to be interpreted as PFD_{avg} of the human action only.

There are a number of methods for evaluating the probability of human error. Two of the better-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 operator-related environmental factors (quality of displays, control layout and clarity, control area environment, procedures, access), 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 credited 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: initial training, refresher training, 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. See Table B.2 for a checklist of human factors issues.

Table B.1 – Sample of IPL Criteria for Operator Response to Alarms*

The values in the table below represent the PFD of the entire IPL and should not be interpreted as the PFD of the human action only. (CCPS 2001, CCPS 2008, and NUREG/CR-1278, 1983)

IPL	Comments	PFD from Literature and Industry	Suggested IPL PFD
Human response to a visual observation of a process hazard (e.g., visible vapor cloud, obvious loss of containment) with ≥ 10 minutes response time (not a response to instrumentation)	Simple well-documented action with clear and reliable indication that the action is required. The operator does not have to perform troubleshooting or diagnostics to take the action.	$1.0 \text{ -- } 1 \times 10^{-1}$ (limited by human response)	$\sim 1 \times 10^{-1}$
Human response to a visual observation of a process hazard (e.g., visible vapor cloud, obvious loss of containment) with ≥ 40 minutes response time (not a response to instrumentation)	Simple well-documented action with clear and reliable indication that the action is required. Minor troubleshooting or diagnostics is allowed if needed before taking action.	1×10^{-2} (limited by human response)	1×10^{-2}
Human response to BPCS indication or alarm with ≥ 10 minutes response time	Simple well-documented action with clear and reliable indication that the action is required. The operator does not have to perform troubleshooting or diagnostics to take the action.	$\geq 1 \times 10^{-1}$ (limited by ISA-84.00.01-2004)	$\sim 1 \times 10^{-1**}$
Human response to BPCS indication or alarm with ≥ 40 minutes response time	Simple well-documented action with clear and reliable indication that the action is required. Minor troubleshooting or diagnostics is allowed if needed before taking action.	$\geq 1 \times 10^{-1}$ (limited by ISA-84.00.01-2004)	$\sim 1 \times 10^{-1**}$
Human response to SIS indication or alarm with ≥ 10 minutes response time	Simple well-documented action with clear and reliable indication that the action is required. The operator does not have to perform troubleshooting or diagnostics to take the action.	1×10^{-1} (limited by human response)	1×10^{-1}
Human response to SIS indication or alarm with ≥ 40 minutes response time	Simple well-documented action with clear and reliable indication that the action is required. Minor troubleshooting or diagnostics is allowed if needed before taking action.	1×10^{-1} to 1×10^{-2} (limited by human response)	1×10^{-1} or 1×10^{-1} to 1×10^{-2} (as determined by human reliability assessment)
Human response to SIS indication or alarm with more than 24 hours response time; assumes multiple operators have an opportunity to detect the alarm(s) and take action	Simple well-documented action with clear and reliable indication that the action is required. Minor troubleshooting or diagnostics is allowed if needed before taking the action.	1×10^{-1} -- 1×10^{-3} (limited by human response)	1×10^{-2} or 1×10^{-1} -- 1×10^{-3} (as determined by human reliability assessment)
Assuming adequate documentation, training, and testing procedures, and drills for the human.			

* Rounded to 1×10^{-1} for ease of computation, while recognizing the ISA-84.00.01-2004-1 limit of $\geq 10^{-1}$.

Copyright 2011 ISA. All rights reserved.