



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.04-2005 Part 1

Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

Approved 1 December 2005

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person.

It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.



Documents
Document Sharing Hub

ISA-TR84.00.04-2005 Part 1 --
Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

ISBN: 1-55617-979-0

Copyright © 2005 by 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

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.04-2005 Part 1.

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

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

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

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

This ISA technical report was prepared by ISA-SP84 Working Group 2, which included the following members:

NAME	COMPANY
A. Summers, <i>ISA-SP84 WG2 Leader</i>	SIS-TECH Solutions LLC
W. Johnson, <i>ISA-SP84 Chair</i>	E.I. DuPont
V. Maggioli, <i>ISA-SP84 Managing Director</i>	Feltronics Corp.
R. Dunn, <i>ISA-SP84 Recorder</i>	DuPont Engineering
R. Adamski	Premier Consulting Services
H. Bezecny	Dow Deutschland
D. Bolland	ExxonMobil Research & Engineering Co.
K. Bond	Consultant
S. Brown	Health & Safety Executive (HSE), UK
N. Cammy	UOP LLC
J. Campbell	ConocoPhillips
W. Cohen	KBR
A. Dowell, III	Rohm and Haas Co.
K. Gandhi	KBR
W. Goble	Exida Com LLC
D. Green	Rohm & Haas Company
P. Gruhn	ICS Triplex
J. Harris	UOP LLC
T. Jackson	Bechtel Corp.
K. Klein	Solutia, Inc.
M. Lang	CF Industries
T. Layer	Emerson Process Management
N. McLeod	Arkema
E. Marszal	Kenexis
R. Nelson	Celanese Corp.
D. Novak	BASF Corp.
T. Ostrowski	Oxychem
W. Owen	Chevron Research & Technology Co.
G. Ramachandran	Motiva Enterprises LLC
G. Robertson	Oxy Information Technology
L. Robison	BP Oil
S. Shah	Exxon Mobil Chemical Co.
J. Siebert	Invista
B. Smith	Nova Chemicals
C. Sossman	Washington Safety Management Solutions LLC
P. Stavrianidis	FM Approvals
H. Storey	Shell Global Solutions
R. Strube	Intertek Testing Services NA, Inc.
L. Suttinger	Westinghouse Savannah River Co.
K. Szafron	BP
R. Szanyi	ExxonMobil Research Engineering
R. Taubert	BASF Corp
H. Thomas	Air Products & Chemicals Inc
A. Woltman	Shell Global Solutions
D. Zetterberg	Chevron Energy Technology Co.

This ISA technical report was approved for publication by the ISA Standards and Practices Board on 1 December 2005:

NAME

I. Verhappen, Chair
 F. Amir
 D. Bishop
 M. Coppler
 B. Dumortier
 W. Holland
 E. Içayan
 A. Iverson
 R. Jones
 K. P. Lindner
 V. Maggioli
 T. McAviney
 A. McCauley
 G. McFarland
 R. Reimer
 J. Rennie
 N. Sands
 H. Sasajima
 T. Schnaare
 A. Summers
 J. Tatera
 R. Webb
 W. Weidman
 J. Weiss
 M. Widmeyer
 C. Williams
 M. Zielinski

COMPANY

Syncrude Canada, Ltd.
 E.I. Du Pont Co.
 Consultant
 Ametek Inc.
 Schneider Electric
 Consultant
 ACES Inc.
 Ivy Optiks
 Consultant
 Endress + Hauser Process Solutions
 Feltronics Corp.
 Jacobs Engineering Group
 Chagrin Valley Controls Inc.
 Emerson Process Management
 Rockwell Automation
 Consultant
 E I Du Pont Co.
 Yamatake Corp.
 Rosemount Inc.
 SIS-TECH Solutions LLC
 Tatera & Associates
 Consultant
 Parsons Energy and Chemicals
 KEMA Inc.
 Stanford Linear Accelerator Center
 Eastman Kodak Co.
 Emerson Process Management

Copyright 2005 ISA. All rights reserved.

This page intentionally left blank.

Copyright The Instrumentation, Systems, and Automation Society

Contents

Preface	3
1 Purpose	9
2 Introduction	9
3 Grandfather Clause	10
3.1 General Considerations	11
3.2 Management of Change Considerations	11
4 The Differences	13
4.1 Clause 1 - Scope	13
4.2 Clause 2 – References	14
4.3 Clause 3 – Abbreviations and Definitions	14
4.4 Clause 4 – Conformance to Standard	14
4.5 Clause 5 – Management of Functional Safety	14
4.6 Clause 6 – Safety Lifecycle Requirements	15
4.7 Clause 7 – Verification	15
4.8 Clause 8 – Process Hazard and Risk Analysis	15
4.9 Clause 9 – Allocation of Safety Functions to Protection Layers	17
4.10 Clause 10 – SIS Safety Requirement Specification	18
4.11 Clause 11 – SIS Design and Engineering	18
4.12 Clause 12 – Requirements for Application Software, Including Selection Criteria for Utility Software	19
4.13 Clause 13 – Factory Acceptance Testing (FAT)	19
4.14 Clause 14 – SIS Installation and Commissioning	19
4.15 Clause 15 - SIS Safety Validation	19
4.16 Clause 16 – SIS Operation and Maintenance	19
4.17 Clause 17 SIS Modification	20
4.18 Clause 18 – SIS Decommissioning	20
4.19 Clause 19 – Information and Documentation Requirements	20
Annex A Example Methods for Determining Grandfather Status	23
Annex B Operator Action as an Independent Protection Layer (IPL)	41
Annex C Management of Functional Safety	51
Annex D Verification, Validation and Functional Safety Assessments	81
Annex E Audits	103
Annex F BPCS and Its Relationship to the SIS	109
Annex G Failures - Types, Classifications, Sources and Strategy for Defense	127
Annex H SIF versus Interlocks, Permissives, and Inhibits	141
Annex I Continuous Mode versus Demand Mode	147
Annex J SIL 4 versus Inherently Safer Design	155
Annex K Fault Tolerance Topics	157
Annex L Device Selection	165
Annex M General Purpose versus Safety Logic Solvers	177
Annex N Design Guidance	181
Annex O Software	201
Annex P Response to Detection of a Dangerous Fault	207
Annex Q Acronyms and Abbreviations	213
Annex R References	215

This page intentionally left blank.

1 Purpose

ANSI/ISA-84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, was replaced in 2004 by ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Modified), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. The three-part series is the United States adoption of the international standards, IEC 61511 Parts 1-3, and includes one additional clause, a “grandfather clause” covering existing safety instrumented systems (see ANSI/ISA-84.00.01-2004 Part 1 Clause 1.0 y).

This Part 1 technical report provides guidance related to the transition of programs developed for the 1996 standard to one compliant with the intent of the 2004 standards. This Part 1 technical report also includes 16 informative annexes providing guidance from the ISA-SP84 committee on a wide range of topics related to the new standards. A companion technical report, ISA-TR84.00.04-2005 Part 2, provides an example illustrating some of the lifecycle steps in ANSI/ISA-84.00.01-2004.

This Part 1 technical report contains four main clauses. Clause 1 is the purpose. Clause 2 explains the origins of ANSI/ISA-84.00.01-2004 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 safety instrumented systems. Clause 4 assists the owner/operator in the transition from ANSI/ISA-84.01-1996 to ANSI/ISA-84.00.01-2004.

NOTE: Throughout this technical report, the term “ISA-84.01-2004” is used to refer to ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Modified). The term “ISA-84.01-1996” is used to refer to ANSI/ISA-84.01-1996.

See Annex R of this technical report for a list of references for all documents cited herein.

2 Introduction

In the United States of America, the Occupational Safety and Health Administration (US-OSHA) regulation, 29 CFR 1910.119 (OSHA 1910.119), requires the identification and management of the instrumented systems responsible for safe operation. ISA Standards Committee SP84 developed 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 ISA-SP84 committee resulted in US-OSHA recognizing ISA-84.01-1996 as representing good engineering practice for SIS.

During its initial development, the ISA-SP84 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), e.g., “*Guidelines for the Safe Automation of Chemical Processes*.” Working in parallel with the ISA-SP84 committee effort, the International Electrotechnical Commission (IEC) was developing IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Concepts introduced in the international standard were incorporated into ISA-84.01-1996, resulting in ISA-84.01-1996 being accepted as the US process sector functional safety standard by the US and IEC. Through ISA-84.01-1996, owner/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 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.

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 ISA-SP84 committee adopted IEC 61511 as ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod). Once the standards were adopted by ISA, the SP84 committee immediately initiated the development of this

guideline. ANSI approved the new standards as ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod) in Sept. 2004.

This guidance document facilitates transition from ISA-84.01-1996 to ISA-84.01-2004 by:

- providing grandfather clause application guidance (refer in this technical report to Clause 3.0 and Annex A);
- highlighting the differences between ISA-84.01-1996 and ISA-84.01-2004-1 (refer in this technical report to Clause 4.0); and
- explaining the application of new requirements in ISA-84.01-2004-1 (refer in this technical report to Annexes B through R).

This guidance document is intended to assist owner/operators familiar with the content of ISA-84.01-1996 with the transition to ISA-84.01-2004-1. To utilize this guideline properly, the reader should be 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 (IEC61511) (for information, visit www.isa.org/standards). These differences are presented using the ISA-84.01-2004 lifecycle with supplementary annexes for additional explanation.

NOTE 1 — Both versions of ISA-84.01 utilize a safety lifecycle. However, the scope of ISA-84.01-2004-1 differs considerably from the scope of ISA-84.01-1996, since all elements of the lifecycle are addressed in ISA-84.01-2004-1. Refer to Clause 4.0 in this technical report for presentation of the differences between the two versions. These additional requirements are typical when harmonizing the standards of many countries.

NOTE 2 — There is nothing in this guideline that precludes, replaces, or makes obsolete any requirement of ISA-84.01-1996 or ISA-84.01-2004-1. This guideline is a “how to” approach and provides informative, non-mandatory methods.

3 Grandfather Clause

The concept of the “grandfather clause” in ISA-84.01-2004-1 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 SISs.

The grandfather clause (ISA-84.01-2004-1 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 U.S. OSHA 29 CFR 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 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 change management 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 below in Annex A.2.

The grandfather clause releases the owner/operator from the design and construction requirements of ISA-84.01-2004-1 for existing installations, if the owner/operator 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.

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

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 below in Annex A is intended to supplement the US-OSHA guidance and to provide examples of methodologies that various owner/operators are using to determine whether their SIS meets the intent of the grandfather clause (ISA-84.01-2004-1 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 ISA-84.01-2004-1 should still be implemented, as appropriate. Documentation, procedures, training, testing, and auditing requirements of ISA-84.01-2004-1 are applicable to all SIS, whether existing or new.

It is important for the owner/operator to develop an approach for addressing existing SISs. It is the responsibility of the owner/operator to determine that existing SISs 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. Annex A in this technical report is a collection of methods used by various owners/operators on the ISA-SP84 committee.

3.2 Management of Change Considerations

Owner/operators of grandfathered SIS (i.e., those SIS that have been determined to meet the intent of ISA-84.01-2004-1 Clause 1.0y) should acknowledge that this status does not provide an indefinite shield against the full requirements of ISA-84.01-2004-1. 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 a 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 ISA-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 (PFDs) or considerably revises the process and instrumentation diagrams (P&IDs), can be expected to have an impact on the definition of the safety instrumented functions (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 of 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.

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 a large reduction in operations or maintenance manpower. As owner/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 problems 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,
- reduced efforts in preventative 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, management of change (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 ISA-84.01-2004-1, 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 The Differences

ISA-84.01-1996 is recognized as a good engineering practice for the design, operation, maintenance, inspection, and testing of safety instrumented systems by many owner/operators. ISA-84.01-2004-1 builds upon ISA-84.01-1996 using an enhanced SIS lifecycle that includes:

- 1) requirements for activities that were not covered due to scope limitations of ISA-84.01-1996;
- 2) new requirements necessary to address technology changes; and
- 3) expanded requirements that are the result of new consensus.

The following is a brief overview of requirements of ISA-84.01-2004-1, highlighting some of the significant differences between ISA-84.01-1996 and ISA-84.01-2004-1. It is important that the reader of this Clause be familiar with the content of ISA-84.01-1996. A summary of the differences by topic is provided in Table 4-1.

4.1 Clause 1 - Scope

This clause states that manufacturers who claim that their equipment is designed for use in Safety Instrumented Systems (SIS) should satisfy the requirements defined in IEC 61508. ISA-84.01-1996 does not address this issue.

ISA-84.01-2004-1 provides extensively detailed requirements for application software in Part 1 Clause 12 “Requirements for application software, including selection criteria for utility software.” In comparison, ISA-84.01-1996 provided less definitive requirements for application software in Clause 7.8.3 “Application logic for Programmable Electronic Systems (PES).”

ISA-84.01-2004-1 identifies SIL 4 as the maximum level of performance for a Safety Instrumented Function covered under this standard. ISA-84.01-1996 identified SIL 3 as the maximum level of performance for a Safety Instrumented Function.

ISA-84.01-1996 excluded systems where the operator was the sole means of returning the process to a safe state. ISA-84.01-2004-1 did not specifically exclude this type of system, but did not explicitly include it either. ISA-84.01-2004-1 Clauses 11.3.1 through 11.3.3 provide requirements where the operator is required to take specific action in response to safety critical alarms and diagnostic alarms. When the hazard and risk analysis (H&RA) identifies a critical alarm as a protection layer, the detection and response may include many different components, such as sensor(s), logic solver, operator HMI, and final element(s). It is important that all elements, including the operator, be capable of achieving the required risk reduction. Annex B of this technical report provides additional discussion on this subject.

4.2 Clause 2 – References

ISA-84.01-2004-1 lists four parts of IEC 61508 as normative references. ISA-84.01-1996 lists a number of informative references in its Annex C, but no normative references.

4.3 Clause 3 – Abbreviations and Definitions

There are a number of new abbreviations and terms in ISA-84.01-2004-1. There is also clarification or expansion of some definitions associated with terminology used in ISA-84.01-1996.

Perhaps, the most significant new term is “Safety Instrumented Function” (SIF). In ISA-84.01-1996, there was very little differentiation between an SIS and SIF. ISA-84.01-2004-1 spells out the difference between the SIF (e.g., hardware and software used to mitigate a specific process risk) and the SIS (i.e., the hardware and software used to implement multiple SIFs). For example, consider a process furnace. If the main fuel gas pressure to the burner is too high, the flame may blow out, allowing uncombusted gases to be introduced into the furnace with the potential for a fire within the furnace. To prevent this hazard, an SIF is implemented in which block valves are used to isolate the main fuel gas from the process furnace when high fuel gas pressure is detected. These same main fuel gas valves may also be closed in response to low pilot gas pressure (i.e., a different process hazard). The SIS is the implementation of these two SIFs in the same logic solver.

The term “prior use” is used in ISA-84.01-2004-1. This term is applied when the owner/operator is justifying the implementation of a device in an SIF application based on prior use of the device in a similar operating profile. The standard provides specific requirements for assessing “prior use” for devices based on the device type, safety integrity level, and, in the case of PE logic solvers, the safe failure fraction.

ISA-84.01-2004-1 introduces three types of software languages: fixed program language, limited variability language and full variability language. The standard covers the development of application software using fixed program language and limited variability language. Owner/operators are directed to IEC 61508 for the development of application software using full variability language.

4.4 Clause 4 – Conformance to Standard

The conformance clause in ISA-84.01-2004-1 is very similar to the conformance clause in ISA-84.01-1996.

4.5 Clause 5 – Management of Functional Safety

ISA-84.01-2004-1 has a number of new requirements concerning the management of functional safety. Although a number of these new requirements are not specifically identified in ISA-84.01-1996, they are identified in other documents that are in widespread use in the United States—e.g., OSHA 1910.119 and the CCPS book “*Guidelines for Safe Automation of Chemical Processes*” (see Annex R, References).

ISA-84.01-2004-1 addresses the competency requirements for individuals involved in the safety lifecycle. Competency requirements are not addressed in ISA-84.01-1996, because competency was already addressed in OSHA 1910.119 for all disciplines involved in process plant design, maintenance and operation. Since the standard has an international scope, the competency requirements are presented for the benefit of those owner/operators that do not have a regulatory system in place that defines these requirements. Annex C of this technical report provides additional guidance on the management of functional safety through effective project management and quality control processes.

ISA-84.01-2004-1 requires procedures for evaluating the performance of an SIS after the system has been in operation for a period of time. This includes comparing the actual process demands with what was assumed during the risk assessment and determining whether the actual failures of the SIS

components are in accordance with what was assumed during the design and verification phases. ISA-84.01-1996 did not have specific requirements for this evaluation.

ISA-84.01-2004-1 has specific requirements for conducting functional safety assessments during the SIS lifecycle. It also includes requirements for the composition of the assessment team. The one mandatory assessment is at Stage 3 of the SIS lifecycle. This assessment is included in ISA-84.01-1996 and OSHA 1910.119, but it is called the Pre-Startup Safety Review (PSSR). The standard simply clarifies the PSSR, as it pertains to the SIS. The major difference is that ISA-84.01-2004-1 requires the inclusion of an independent, senior, competent person on the team. Annex C of this technical report has additional discussion concerning this requirement.

The terms verification, validation, and functional safety assessment are used in ISA-84.01-2004-1. Each term implies that specific activities are taking place or that specific requirements are being met. Annex D provides an overview of these three terms.

ISA-84.01-2004-1 has a requirement for periodic auditing to ensure compliance with the requirements in the standard. ISA-84.01-1996 does not have a specific requirement for periodic auditing. Following the ISA-84.01-2004 lifecycle ensures that the intended design, operation, maintenance, and testing of the SIS is sufficient to achieve the functional and integrity requirements. Auditing is a means to ensure that these intentions result in actual work practices. These audits should be considered opportunities to review the effectiveness of the management of change system. Annex E of this technical report provides an example of how to approach and perform an audit.

4.6 Clause 6 – Safety Lifecycle Requirements

The ISA-SP84 committee created ISA-84.01-1996 to supplement OSHA 1910.119 in the areas related to the implementation of instrumentation and controls necessary for safe operation. Rather than repeating OSHA 1910.119 mandates, the standard references OSHA 1910.119 for some key program elements. Specifically, ISA-84.01-1996 does not provide specific requirements for safety management, hazard and risk analysis, pre-startup safety review, or training. ISA-84.01-2004 provides requirements for each of these areas.

4.7 Clause 7 – Verification

ISA-84.01-2004-1 requires the development of a verification plan to define the verification activities that are to take place. There was no specific verification clause in the ISA-84.01-1996 standard. However, most owner/operators include a number of verification steps during project execution for project and quality management purposes.

4.8 Clause 8 – Process Hazard and Risk Analysis

ISA-84.01-2004-1 Clause 8 and ISA-84.01-1996 address the Hazard and Risk Analysis (H&RA). Both mandate the need for H&RA, but neither defines how to specifically execute the H&RA or to identify process risk. Rather than providing specific requirements, ISA-84.01-1996 referred to OSHA 1910.119 and the CCPS books, *Guidelines for Hazard Evaluation Procedures*, *Guidelines for Chemical Process Quantitative Risk Analysis*, and *Guidelines for Safe Automation of Chemical Processes*, for guidance on determining the SIS requirements. ISA-84.01-1996 Annex A also provided examples of H&RA techniques commonly used in 1996.

Two major changes the owner/operator experiences when transitioning to ISA-84.01-2004-1 from ISA-84.01-1996 are:

- 1) the new standard has more normative (i.e., mandatory) H&RA requirements, and
- 2) new H&RA approaches for assignment of SIL are discussed.

ISA-84.01-2004-1 clearly establishes the relationship between the SIS functional and integrity requirements and the H&RA by requiring the following:

- Identification of the process hazards,
- Identification of the initiating cause(s) of each process hazard,
- Determination of the initiating cause frequency,

ISA-84.01-2004-1 limits the performance that can be assumed for the Basic Process Control System (BPCS). Annex F of this technical report provides a brief discussion on this limitation.

- Evaluation of the consequence severity associated with each process hazard,
- Determination of whether process risk (i.e., initiating cause frequency and the consequence severity) exceeds owner/operator's risk criteria,
- Identification of safety functions that reduce the process risk to the risk criteria, and
- Verification that each safety function is designed and managed to meet its allocated risk reduction.

The differences between ISA-84.01-1996 and IEC 61511 resulted in part because:

- ISA-84.01-1996 was a national standard, which relied on regulations and other good engineering practices already in use in the United States.
- In the United States, the Center for Chemical Process Safety (CCPS) is primarily responsible for establishing H&RA guidelines. CCPS developed "*Guidelines for Safe Automation of Chemical Processes*," which established criteria for the H&RA related to control and safety systems. In the United States, ISA is primarily responsible for establishing standards in the field of instrumentation and controls. The ISA-SP84 committee developed ISA-84.01-1996.
- IEC 61511 is an international standard, which should harmonize the various approaches of multiple countries.
- The various countries and associated safety cultures represented by the IEC 61511 committee valued the need to clearly discuss each other's H&RA techniques,
- Owner/operator experience gained in applying ISA-84.01-1996 indicated that the additional guidance provided in ISA-84.01-2004-1 was appropriate.

As a result, the IEC 61511 committee was faced with a number of differing techniques and varying H&RA terminology from the global community. Therefore, rather than mandating a specific method, general requirements were provided and the IEC 61511 committee asked each country delegation to submit examples of techniques for inclusion in IEC 61511-3. IEC 61511-3 Annex A was submitted by the UK. IEC 61511-3 Annexes B, C and F were submitted by the US. IEC 61511-3 Annex F is a precursor to the CCPS book "*Layers of Protection Analysis: Simplified Process Risk Assessment*" (see Annex R, References). IEC 61511-3 Annex E was submitted by Germany. IEC 61511-3 Annex D was submitted by the UK and Finland.

NOTE — The listing of countries above is to provide the owner/operator with the origin of each of these annexes. This listing is not meant to imply that any specific technique is mandated by these countries. The owner/operator should determine the correct method for the application.

4.9 Clause 9 – Allocation of Safety Functions to Protection Layers

Safety functions are allocated to protection layers. For each safety function, the owner/operator should evaluate potential common cause failures that could disable multiple safety functions. Annex G provides additional explanation concerning common cause failures.

When safety functions are allocated to the safety instrumented system layer, they are known as Safety Instrumented Functions (SIF). The differences and/or relationships between safety functions, safety instrumented functions, safety instrumented systems, interlocks, and permissives are important. Annex H provides a discussion including important historical references to assist in the understanding of the new terms.

Safety instrumented functions (SIF) are assigned a safety integrity level (SIL) and a mode of operation (continuous or demand) during the H&RA. These are recent requirements and application guidance is limited at best.

NOTE — The SIL of an SIF is defined as a range of availability targets for the given function. SIL 1, for example, implies a range of availability from 90 to 99%, SIL 2 from 99 to 99.9%, etc. Owner/operators may find this 10:1 ratio within a given SIL to be too wide for practical analysis. For example, a 10:1 ratio for test intervals could mean a test interval from every 6 months to testing every 5 years. For an SIL 1 SIF, the SIF could theoretically be unavailable for as little as 3.65 days per year or as much as 36.5 days a year. The standard requires alternative operational procedures be put in place when the SIF is unavailable. However, alternative procedures may be effective as a compensating measure for a 3.65-day period, but would not be considered sufficient protection during a 36.5-day period. On a project, an SIL 1 system could be installed to meet 99% availability or 90% availability. Both solutions would be 'correct', but would be at the opposite ends of the cost and safety spectrum. Some owner/operators may find that defining the performance requirements in terms of specific availability targets (e.g., 90, 95, 97.5, 99%, etc.) may be more appropriate than simply specifying the required SIL.

Some of the new requirements in this clause include the following:

1) Requirements for continuous mode of operation.

ISA-84.01-2004-1 includes high demand/continuous mode of operation, as well as demand mode. ISA-84.01-1996 only addressed demand mode, because the vast majority of SIS operate in a demand mode. Annex I of this technical report discusses the differences between demand mode and high demand/continuous mode. It also provides an example to illustrate the importance of properly defining any high demand/continuous mode SISs.

2) New requirements for SIL 4 Safety Instrumented Functions.

ISA-84.01-2004-1 requires that SIL 4 safety instrumented functions be designed in compliance with IEC 61508. This requirement is due to the extensive hardware and software verification and validation techniques that should be employed to achieve the integrity requirements. The ISA-SP84 committee strongly advises against the implementation of a single layer SIL 4 SIS. Annex J of this technical report provides guidance on how to address process risk that requires risk reduction equivalent to SIL 4.

3) Requirements for the BPCS when used as a protection layer.

ISA-84.01-2004-1 establishes a limit on the amount of risk reduction that can be assumed for the BPCS. This is because the BPCS is generally not designed, operated, maintained, or tested in accordance with the requirements of the standard. Annex F of this technical report provides further information on the contribution of the BPCS as an initiating cause and as a protection layer.

4.10 Clause 10 – SIS Safety Requirement Specification

The requirements stated in this clause are more extensive than those found in ISA-84.01-1996. The new requirements include information that was typically developed by the owner/operator, if necessary. ISA-84.01-1996 informative Annex B identified these issues. For example, ISA-84.01-2004-1 requires that the owner/operator document the following:

- Criteria for successful operation of the SIF--e.g., are there any specific requirements for tight shutoff valves.
- Requirements for the repair of an SIS fault.
- Requirement for the SIS to survive a major accident event--e.g., is fireproofing on shutoff valves required?

4.11 Clause 11 – SIS Design and Engineering

There are a number of requirements in Clause 11 that are not addressed in ISA-84.01-1996. Some of these requirements include:

- Specific requirements for when a fault is detected in the SIS.
- Minimum hardware fault tolerance for different SILs.

Minimum hardware redundancy is required to ensure that systematic errors made in the calculation of the frequency of failure or probability of failure on demand do not result in inadequate protection against serious process risk. The fault tolerance refers to individual devices or channels. Annex K of this technical report provides additional information concerning fault tolerance. Annex L of this technical report provides a discussion of the IEC 61508 SIL Claim Limit. Annex P of this technical report discusses various considerations when defining the response to dangerous, detected faults.

- Requirements for the selection of SIF devices.

Annex L of this technical report provides a discussion concerning the selection of devices based on compliance with IEC 61508 or Prior Use.

- Requirements for Programmable Electronic (PE) logic solvers that are not designed in compliance with IEC 61508.

ISA-84.01-2004-1 makes a distinction between general-purpose (i.e., off-the-shelf) logic solvers and SIS logic solvers. ISA-84.01-1996 did not make any distinction between the two.

Annex M of this technical report provides a discussion of general-purpose versus safety-configured logic solvers. The discussion includes a listing of various techniques that can be used to implement safety-configured logic solvers.

- Requirements for design of the SIS.

While many of the concepts in ISA-84.01-1996 Annex B were incorporated in ISA-84.01-2004-2, the ISA-SP84 committee wanted to retain the good engineering practice that was documented in ISA-84.01-1996 Annex B. As a result, Annex N of this technical report provides an update of this design guidance.

- Requirement to verify quantitatively that the SIS satisfies the SIL requirements of the SIF.

ISA-TR84.00.02-2002 (visit www.isa.org/standards) is a technical report that discusses how to perform SIL verification calculations.

4.12 Clause 12 – Requirements for Application Software, Including Selection Criteria for Utility Software

ISA-84.01-1996 requires that the application software be developed in accordance with the Safety Requirements Specification (SRS). ISA-84.01-2004-1 also requires this, but discusses the development of the application software with relation to the safety lifecycle. Where hardware is prone to random failures, the software is more prone to systematic failures. The safety lifecycle is important, because it is the primary mechanism for reducing systematic failure. The inclusion of the lifecycle discussion in the software section does result in repetition of the design process described in ISA-84.01-2004-1 Clause 11. This repetition is intended to highlight the importance of the lifecycle in the development, verification and validation of application software. Annex O of this technical report provides a discussion of the evolution of application software development.

4.13 Clause 13 – Factory Acceptance Testing (FAT)

The content of this clause is informative and contains no mandatory requirements. This topic is not discussed in ISA-84.01-1996.

4.14 Clause 14 – SIS Installation and Commissioning

The content of this clause is almost an exact duplicate of what is written in ISA-84.01-1996. There are no new requirements.

4.15 Clause 15 - SIS Safety Validation

The contents of this clause are very similar to what is described in the ISA-84.01-1996 clause on pre-startup acceptance test (PSAT).

4.16 Clause 16 – SIS Operation and Maintenance

OSHA 1910.119 included many requirements for operation and maintenance. Consequently, ISA-84.01-1996 referenced these requirements and included only a few additional requirements specifically related to SIS. ISA-84.01-2004-1 expands the ISA-84.01-1996 requirements for operation and maintenance including the following:

- 1) Operation procedures and associated training should address:
 - o how the SIF functions.
 - o the hazard that the SIF is protecting against.
 - o circumstances under which bypass switches can be activated.
 - o when to execute a manual shutdown.
 - o appropriate response to diagnostic alarms.
- 2) Operation management should collect information regarding process demands on the SIS and SIF device failures.
- 3) Maintenance management is required to collect the results of audits and tests of SIF devices.
- 4) Operation and maintenance management should identify any specific requirements for a visual inspection of hardware integrity.

4.17 Clause 17 SIS Modification

There are no new requirements in this clause. Requirements were previously covered by ISA-84.01-1996 and OSHA 1910.119.

4.18 Clause 18 – SIS Decommissioning

This clause is very similar to what is in ISA-84.01-1996 with no new requirements.

4.19 Clause 19 – Information and Documentation Requirements

There are no new requirements in this clause. Documentation requirements were previously covered by ISA-84.01-1996 and OSHA 1910.119.

Table 4-1 – Summary of Differences

ISA-84.00.01-2004	ISA-84.01-1996
Process and its associated Equipment/IEC 61508	Process and its equipment/ISA-84.01-1996 Clause 3.1.5 makes numerous references to Equipment Under Control(EUC)
SIF	Safety function
SIL for SIF	SIL for SIS
BPCS performance expectations are limited.	Excludes BPCS in Clause 1.2.8
Validation	Pre-startup acceptance test (PSAT)
Safe Failure Fraction (fault tolerance)	None
Hazard and risk analysis requirements	Excluded in Clause 1.2.5 Informative Clauses 4.2.1 – 4.2.5 and Annex A
Design requirement	Less definitive
Operation and maintenance requirement	Less definitive
Tracking trip/demand	Less definitive
Allocation of safety functions to protection layers	Not part of scope
Requirements on BPCS as a layer of protection	Excludes BPCS in Clause 1.2.8
Requirements for system behavior on detection of a fault	Less definitive
Prior Use	User-approved: Clauses 1.2.10 and 3.1.62
Requirements for interfaces	Less definitive
Requirements for competency	Less definitive
Requirements for application software – normative	Much less definitive – informative
Requirements calculation of SIL for SIF	Informative Annex A
Grandfather clause in Clause 1.0y	Grandfather clause in Clause 2.2.1
Not discussed	Fire and gas excluded in Clause 1.2.14
Full variability	Not discussed
Limited variability	Not discussed
Fixed program	Not discussed
Defines use of embedded software	Requirements in Clause 3.1.58.2
Documentation requirements	Less normative
Factory acceptance test (FAT) discussion	Not discussed
Part 3 – global SIL selection methods	US – SIL selection methods Annex A
Layer of Protection Analysis	Not discussed
Example – IEC 61508	Example – Annex A and TR84.00.02
Management of functional safety requirements	Less definitive
References – normative	References – informative
Asset protection referenced	Excluded in Clause 1.2.13

ISA-84.00.01-2004	ISA-84.01-1996
Common cause failure definition	Requirements in Clauses 3.1.7.2 and 3.1.7.1 and discussed in Annexes B.2, B.8, B.10 and D.3
Diagnostics coverage definition	Requirements in Clause 3.1.5 and Discussed in B.4.4.1.1, B.6.4 and B.9.3
Control system definition	Requirements in Clause 3.1.5
E/E/PE	E/E/PE Page 13, paragraph 1, line 2
External risk reduction requirements	None
Functional safety audit details	Much less
Hazard definition	Excluded in Clause 1.2.5. Provided guidance in Informative Clauses 4.2.1 – 4.2.5 and Annex A
Independent organization/department/person requirements	Not discussed
Other technologies	Excludes non-E/E/PE technologies
Safety-related system requirements IEC 61508 Part 2 - Clause 7.4.7 Requirements for E/E/PES Implementation	Discussed in Clause 7.3, but not defined as safety-related system requirements
Protection layer definition	Discussed in Clause 3.1.42 and informative Clauses 4.2.3 and 4.2.4
Safe state definition	Defined in Clause 3.1.50
Safety function (all technologies)	Safety function SIS only
SIL definition (SIF)	Defined SIL (SIS) in Clause 3.1.52
Safety lifecycle	Both versions of ISA-84.01 utilize a safety lifecycle process to address the assessment, design, operation, maintenance, testing, and management of safety instrumented systems
Systematic failure definition	Defined in Clause 3.1.60
Verification quantitative	Verification qualitative or quantitative
Tolerable risk	Discussed in Clause 3.2.89
SIL 1, 2, 3, 4	SIL 1, 2, 3
Illustrates 61508 as normative reference	Illustrates 61508 as draft document
Systematic error guidance	Annex B.8 and B.9 pages 69-72 provide systematic error guidance
Includes operator action in SIS	Excludes operator action (Clause 1.2.14) in SIS

Annex A Example Methods for Determining Grandfather Status

NOTE — Annex A is referenced in Clause 3.0 of this technical report.

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 (ISA-84.01-2004-1 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.3.7 provide examples of methods used by some owner/operators in evaluating existing SIS. These methods are provided as examples and should not be considered the only acceptable approaches. Owner/operators 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, and increased testing.

A.2 Timing

The owner/operator should document the adequacy of the SIS at the cyclic process hazards analysis (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;
- 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; or

NOTE — Clause 3.2 of this technical report provides a list of management of change considerations.

- 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 Process Hazards Analysis (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 the community, an assessment of the protection layers is conducted to determine whether the required functionality and integrity is provided by the existing design. This assessment is sometimes performed as part of the 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 Safety Integrity Level (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) for the SIF. The actual PFD is then compared to the SIL assigned by the PHA team. If the actual PFD 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 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. Owner/operators should decide and document which approach is suitable for their process facilities.

Step 1. Define process facility grandfather clause application rules.

After reviewing Clause 3.0 of this technical report, the owner/operator establishes ground rules that are to be implemented whenever existing SISs 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 – www.isa.org), or • Corporate standard(s). NOTE — Corporate standards should be verified against key requirements of ISA-84.01-2004-1 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: - An SIF whose design basis is not in compliance with GR-1 should be upgraded to ISA-84.01-2004-1 as soon as possible. - An SIF whose design basis meets GR-1 should be upgraded to ISA-84.01-2004-1 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.

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 ISA-84.01-2004-1 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, testing, and operating according to the design basis, the SIF should be upgraded to meet the design basis.

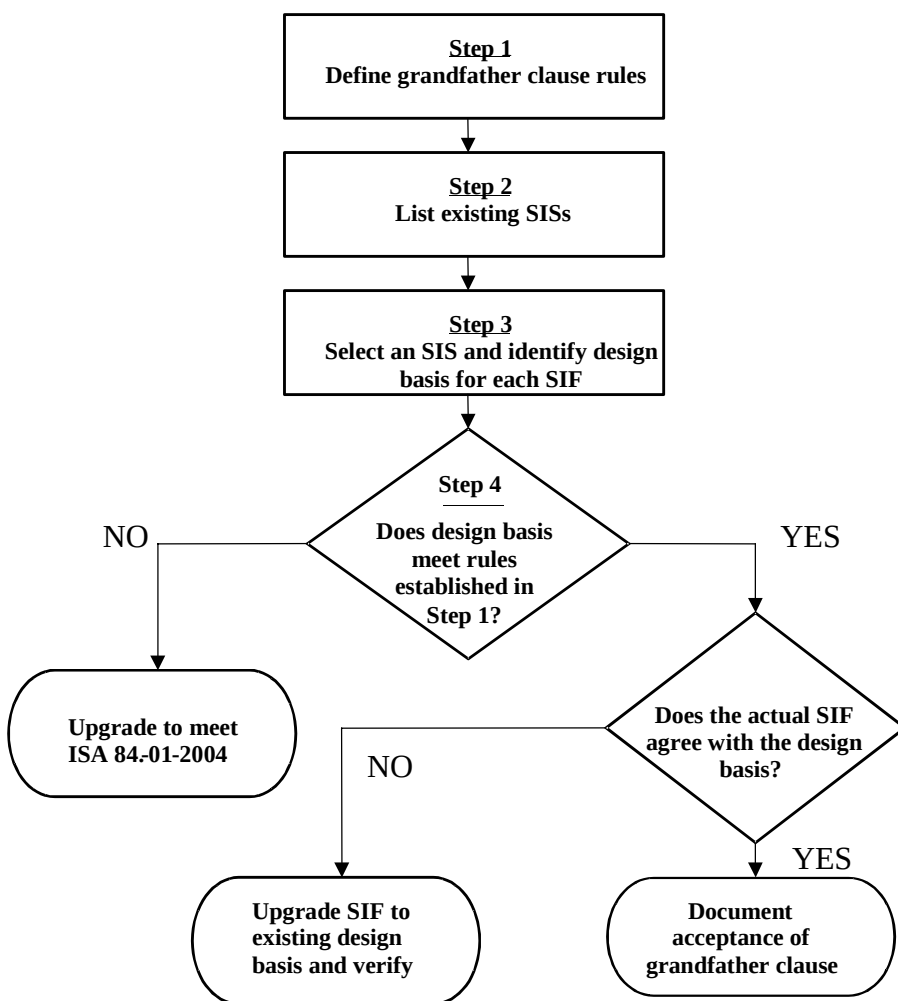


Figure A-1 – Flow Diagram for Example Approach Presented in Annex A.3-2

A.3.3 Comparison with Key ISA-84.01-1996 Requirements

In this method, the owner/operator conducts an assessment, comparing the existing SIS to key ISA-84.01-1996 requirements. Prior to the issuance of ISA-84.01-2004-1, ISA-84.01-1996 was used as a good engineering practice for SIS by this owner/operator. This following questionnaire, Table A-2, was designed for use in verifying whether existing SISs meet the intent of the requirements in 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 ISA-84.01-2004-1.

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 Safety Instrumented Systems (SIS) are defined? For example, 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 Safety Instrumented Functions (SIFs) implemented with the SIS have a Safety Integrity Level (SIL) assigned to them? a. 100% _____ b. 50 to 99% _____ c. 25 to 49% _____ d. < 25% _____ Comment/explanation: _____
3.	What percentage of the SISs 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 SISs 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: _____
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: _____

No.	Question
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 Safety Instrumented System (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 on-line testing documented? a. well documented _____ b. adequately documented _____ c. poorly documented _____ d. not documented _____ Comment/explanation: _____
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: _____

No.	Question
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 ISA-84.01-2004-1 Requirements

Another approach to SIS evaluation is the development of a checklist based upon ISA-84.01-2004-1 requirements. The checklist should address major philosophical and technology issues defined in ISA-84.01-2004-1. 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 in Table A-3.

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 Safety Instrumented Systems (SIS) defined? For example, 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:

No.	Question
5.	Are the SISs designed and built to meet the SIL of the SIF? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
6.	Are the SISs tested frequently enough to maintain the SIL of the SIF? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
7.	Are the SISs 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: _____
9.	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: _____
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: _____

No.	Question
14.	How well are Operations personnel trained on the SIFs of the Safety Instrumented System (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 on-line testing documented? a. well documented _____ b. adequately documented _____ c. poorly documented _____ d. not documented _____ Comment/explanation: _____
17.	Are the SIS inputs and outputs shown on the P&IDs? a. yes _____ b. no _____ c. don't know _____ Comment/explanation: _____
18.	Is 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: _____

No.	Question
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

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

Step 1: Determine the required risk reduction 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 ISA-84.01-2004-1.
- 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 ISA-84.01-2004-1.**

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 PFDavg 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 ISA-84.01-2004-1 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.3-5

NOTE — Example provided by one owner/operator

This table should not be used as a design guide for new installations. It is an example provided by one company to evaluate existing SISs.

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.
	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

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
	Integrated systems	Function protected against changes and override	See user and/or safety manual requirements	See user and/or safety 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
Instrumentation (sensors)	"Smart" Instruments	Acceptable 1oo1/1oo2/ 2oo3/ 1oo2D/ 2oo2D	Acceptable 1oo2/ 2oo3/ 1oo2D/ 2oo2D	Acceptable 1oo2/ 2oo3/ 1oo2D/ 2oo2D
	Certified instruments	Acceptable	Acceptable	Acceptable
	Non-smart analog electronic Instruments	Acceptable 1oo1/1oo2/ 2oo3	Acceptable 1oo2/ 2oo3	Acceptable 1oo2/ 2oo3
	Pneumatic analog Instruments	Acceptable 1oo1/1oo2/ 2oo3	Acceptable 1oo2/ 2oo3	Requires hazard and risk analysis team approval
	Discrete measurements (e.g., pressure switch)	Acceptable 1oo1/1oo2/ 2oo3	Acceptable 1oo2/ 2oo3	Requires hazard and risk analysis team approval
	Pneumatic transmitter with switches (behind panel)	Acceptable 1oo1/1oo2/ 2oo3	Acceptable 1oo2/ 2oo3	Requires hazard and risk analysis team approval
	Pneumatic transmitter with transducer (behind panel)	Acceptable 1oo1/1oo2/ 2oo3	Acceptable 1oo2/ 2oo3	Acceptable 1oo2/ 2oo3
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

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
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 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
	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 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
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 a 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, *Principles for Computers in Safety-Related Systems*, 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 SISs 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 SISs 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 determines whether SIS functionality is achieved. If the design practice is determined acceptable, any SISs designed in accordance with the practice can be considered for the grandfather clause.

For example, a company that is using its own classification system could map its 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 SISs 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 Acceptable 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 industry organizations, such as NFPA, API, ASME, ANSI, and ISA. 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 safety integrity level (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 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 ISA-84.01-2004-1 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 is 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 safety instrumented function (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.
- SIF logic solver requirements.
- SIF devices and required testing interval.

The operating basis documentation should cover the operation and maintenance requirements of ISA-84.01-2004-1 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.

Annex B Operator Action as an Independent Protection Layer (IPL)

NOTE — Annex B is referenced in the following: Clause 4.1, Clause 4.11, Annex K.2, Annex N.9.2., 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 ISA-84.01-2004-1 Clause 8.2.1 for requirements on hazard and risk analysis.

NOTE 2 — Refer to ISA-84.01-2004-1, Clauses 11.3.1 through 11.3.3, for a discussion on the operator response to diagnostic faults.

ISA-84.01-2004-1 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 ISA-84.01-2004-1 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 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 a 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 all requirements of ISA-84.01-2004.
 - 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, ISA, The Engineered Equipment Materials and Users Association (EEMUA), and Health & Safety Executive have developed extensive guidance on alarm management. Design of alarm systems should consider ISA -18.1-1979 (R 2004), ISA-RP 60.3-1985, and ISA-RP 60.6-1984; IEEE-845, IEEE-1023, and IEEE-1289; and NUREG-0700, Chapter 4 (see References, Annex R).

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 factor of less than 10, under the following conditions:

- The guidance in Annex F.2 of this technical report 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 Probability of Failure on Demand (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) principles 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.

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 probability of failure on demand (PFD) 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 (independent protection layer). 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 process safety time, when an operator response to an alarm is being considered for reducing the risk of a specified hazard scenario. The 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 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 Probability of Failure on Demand (PFD) values, the owner/operator is cautioned to do a detailed human reliability assessment to confirm the assumed PFD. The values in the table below represent the PFD of the entire IPL. They are not to be interpreted as PFD of the human action only.

There are a number of methods for evaluating the probability of human error. Two of the more well-known methods are the Technique for Human Error Rate Prediction (THERP) (Reference NUREG/CR-1278) and the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (Reference NUREG/CR-4772). Error rates are usually established on a per demand basis.

The nominal human error rates can be reduced or increased based on 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, things such as: 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, and adequate staffing.

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. They are not to be interpreted as PFD of the human action only.

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.	$1.0 - 1 \times 10^{-1}$ (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.	$> 1 \times 10^{-1}$ (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.	$> 1 \times 10^{-1}$ (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.	$1 \times 10^{-1} - 1 \times 10^{-2}$ (limited by human response)	1×10^{-1} or $1 \times 10^{-1} - 1 \times 10^{-2}$ (as determined by human reliability assessment)

IPL	Comments	PFD from Literature and Industry	Suggested IPL PFD
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.			

* Adapted from *Layer of Protection Analysis, Simplified Process Risk Assessment* (Center for Chemical Process Safety, American Institute of Chemical Engineers, New York: 1996); *Inherently Safer Chemical Processes: A Lifecycle Approach* (Center for Chemical Process Safety, American Institute of Chemical Engineers, New York: 1996); and *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (Swain and Guttman, NUREG/CR-1278, United States Nuclear Regulatory Commission, Washington, DC: 1983).

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

Table B-2 – Checklist for Human Factors Issues

Human Factors Engineering Issues	Yes	No	N/A
Can the operator respond within the required time response for the SIF?			
Are operators provided specific alarm response procedures?			
Are operators adequately trained relative to the required SIS action?			
Are operators periodically evaluated for competency in SIS response?			
Are operators physically capable of accomplishing the response action?			
Are controls and displays adequate, effective, and suitable for operator tasks?			
Is the operator action consistent with existing protocol and procedures, established conventions and operator experience?			
Do separate displays present consistent information?			
Is display movement consistent/compatible with related control movement?			
Is displayed information readable to the necessary precision, concise, complete, and usable without extrapolation?			
Is adequate information about normal and upset conditions displayed?			
Is display failure readily apparent?			
Are displays and controls located within recommended height and reach limits?			
Are SIS alarms obvious to an operator?			
Are related controls, displays and alarms grouped together?			
Is the possibility of accidental operator activation of SIF initiation minimized?			
Is the SIS operator interface in an area that requires frequent operator attention?			
Do displays support operator task requirements in terms of range, precision and accuracy?			
Are normal operating ranges and alarm set points clearly identified?			
Are the completions of commanded SIS actions (i.e., valve position, pump status) displayed?			

B.6 Verification of an Operator-Initiated SIF

As shown in Table B-1, the hazard and risk analysis may identify operator actions that are allocated to the SIS layer. When risk reduction is taken for an operator-initiated SIF, the evaluation of the probability of failure on demand (PFD) of an operator-initiated SIF is performed similarly to the evaluation of an automatic SIF. Figure B-1 is a representation of an operator-initiated SIF. This figure is adapted from ISA-84.01-2004-1 Clause 3.2.72, Figure 7.

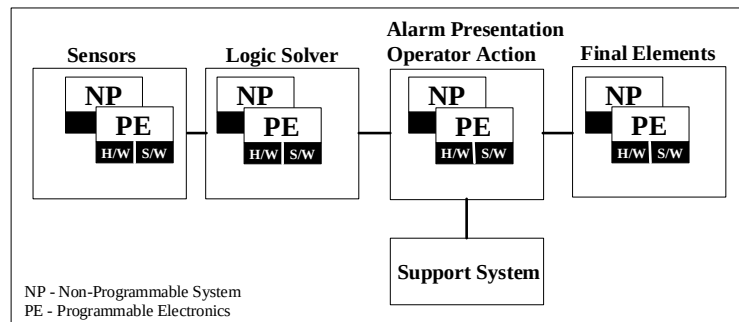
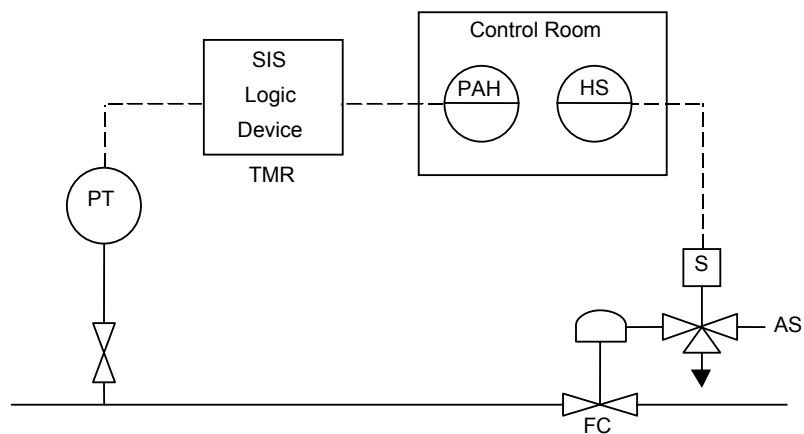


Figure B-1 – Example of Operator-Initiated SIF Architecture

The verification of the operator-initiated SIF should consider the potential for operator error using a user-approved criteria or analysis techniques. This assessment should include the human interface design and operating procedures.

Most automated SIFs are designed as de-energize to trip. As a result, the PFD calculation for these SIFs generally does not take into consideration any utility systems. Operator action inherently requires support systems to complete the safety function. Display/alarms require power to actuate the light and/or horn for operator response. Therefore, the reliability of the electrical power system directly affects the PFD of the credited operator action.

A simplified example of an operator-initiated SIF architecture is provided in Figure B-2. Figure B-3 provides an example of the use of fault tree analysis to evaluate the PFD of the example architecture.



TMR: Tri-modular redundant
 PT: Pressure transmitter
 FC: Fail closed
 S: Solenoid
 AS: Air supply
 PAH: Pressure alarm high
 HS: Hand switch

Figure B-2 – Operator- Initiated SIF Action to Close Valve on High Pressure

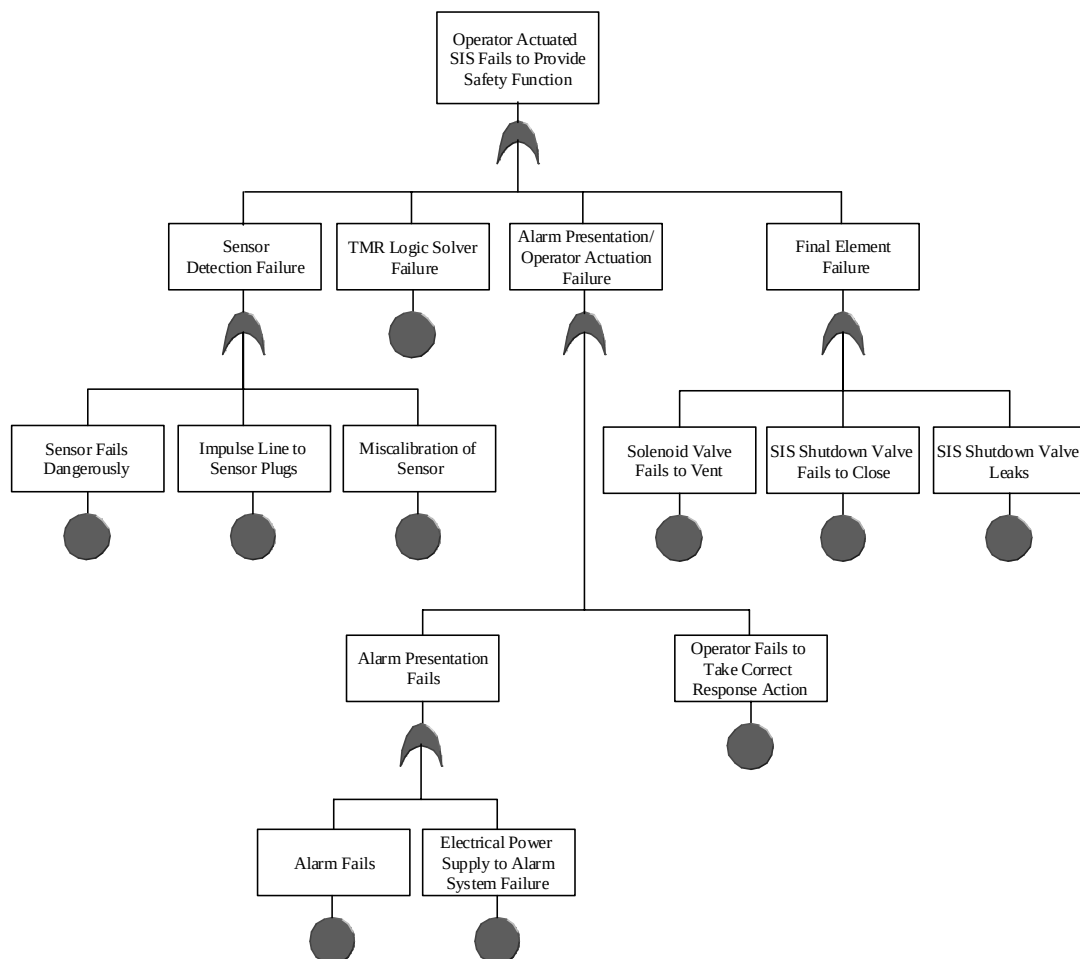


Figure B-3 – Fault Tree Analysis of Figure B-2

This page intentionally left blank.