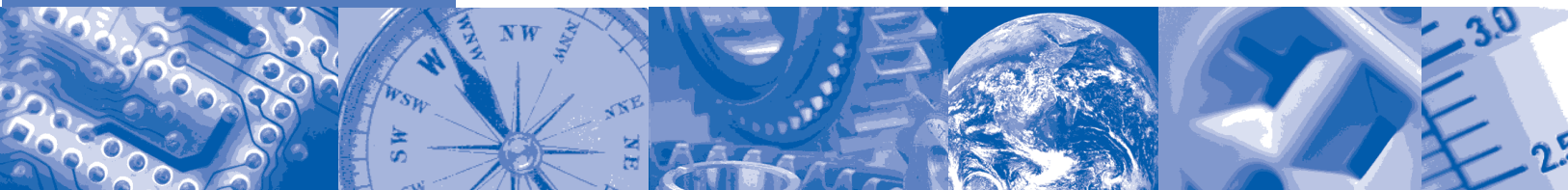


ANSI/ISA-84.01-1996

Formerly ANSI/ISA-S84.01-1996



Application of Safety Instrumented Systems for the Process Industries



**ISA—The Instrumentation,
Systems, and
Automation Society**

Approved 15 March 1997



Documents

Document Sharing Hub

ANSI/ISA-84.01-1996 — Application of Safety Instrumented Systems for the Process Industries

ISBN: 1-55617-590-6

Copyright © 1996 by the Instrument Society of America. All rights reserved. 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, annexes, and draft technical report 84.02 (ISA-dTR84.02) are included for informational purposes and are not part of ANSI/ISA-84.01-1996. ISA-dTR84.02 was still in development at the time that ANSI/ISA-84.01-1996 was published; for information, contact ISA.

This standard has been prepared as part of the service of ISA, the international society for measurement and control, 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.

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

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

S84.01 has been developed with the intent that it will eventually become a part of a group of standards being developed by the International Electrotechnical Commission (IEC). This has resulted in a format and structure that may be somewhat different from previous ISA Standards. Some background information is, therefore, offered to assist the reader in better understanding the focus of S84.01.

IEC has commissioned the development of a set of international standards encompassing all aspects of safety systems for all industries. It is titled "Functional Safety: Safety-Related Systems." This effort is under the direction of IEC Technical Committee No. 65, Subcommittee 65A, Working Group 10. It is titled IEC draft Publication 1508 and is still in development but, as it exists today, there are seven parts:

- Part 1 - General requirements
- Part 2 - Requirements for Electrical/Electronic / Programmable Electronic Systems (E/E/PES)
- Part 3 - Software requirements
- Part 4 - Definitions and abbreviations of terms
- Part 5 - Guidelines on the application of Part 1
- Part 6 - Guidelines on the application of Parts 2 and 3

- Part 7 - Bibliography of techniques and measures

This work is to define requirements common to all industries. It is IEC's intent that there will then be additional standards developed to reflect specific requirements for the various industry sectors, such as nuclear, pharmaceutical, aeronautical, process, etc.

IEC has commissioned a subcommittee, identified as IEC 1511, for the development of an industry-specific international standard that addresses the application of safety instrumented systems for the process industries. ISA-S84.01-1995 has been written with the intent that it will serve as the basis for that sector-specific standard. The structure, format, and content of S84.01 has been developed in this context. There are significant differences in S84.01 from IEC draft Publication 1508-1995, as described in Clause 12. However, IEC draft Publication 1508 was still being developed at the time that S84.01 was published. As a result, ISA SP84 will continue to support and monitor IEC draft Publication 1508 development and will modify S84.01 as needed when IEC draft Publication 1508 is published.

The IEC style guide has been used to facilitate the harmonization of this material with the general standards and other sector-specific standards being developed for IEC draft Publication 1508.

The following people served as active members of ISA Committee SP84:

NAME	COMPANY
V. Maggioli, Chairman	Feltronics Corporation
R. Boyd, Jr., Vice Chairman	Aramco
W. Calder III, Managing Director	Calder Enterprises
*R. Adamski	Triconex
R. Aldridge	Consultant
R. Bailliet	Shell Offshore, Inc.
N. Battikha	ICI Canada, Inc.
L. Beckman	HIMA Americas, Inc.
R. Bell	Technology & Health Sciences Division
S. Bender	S.K. Bender & Associates
P. Bennett	Center for Software Engineering
K. Bingham	Hinz Consulting, Ltd.
W. Black	BP GRE
J. Blagg	Eco Waste Technologies
R. Bloomfield	Adelard
*K. Bond	Shell Oil Company
K. Bosch	G3 IQSE
S. Boyer	Iliad Engineering, Inc.
*B. Bradley	Mobil Research & Development Corporation
A. Brombacher	Eindhoven University of Technology
D. Brown	Fisher-Rosemount Systems
*L. Brown	Arco Oil & Gas
M. Cannon	Industrial Equipment Company
J. Carew	Stone & Webster, Inc.
L. Cheung	W.R. Grace & Company
R. Desrochers (deceased)	Sun Company

*One vote per company

R. Dillman

Conoco, Inc.

NAME

COMPANY

J. Duran
P. Early
*R. Ewbank
T. Fisher
J. Forrest
*T. Frederickson, Jr.
R. Freeman
D. Fritsch
*K. Gandhi
R. Gardner
*F. Gellner
J. Gilman
R. Glaser
W. Goble
*C. Goring
*J. Gray
D. Green
T. Green
J. Greenwald
*R. Grehofsky
P. Gruhn
*A. Habib
*A. Hamers
A. Hammons
B. Hampton
C. Hardin
D. Haysley
*A. Heckman
*K. Hill
L. Hoffman
B. Humes
*D. Inverso
J. Jarvi
W. Jay
K. Jennings
D. Jensen
R. Johnson
*W. Johnson
*D. Karydas
K. Kassner
R. Kier
D. Leonard
*E. Lewis
J. Martel
*T. McAdams

Lagoven SA
ABB Industrial Systems, Inc.
Rhone-Poulenc, Inc.
Lubrizol Corporation
ABS Industrial Verification, Inc.
Triconex
Monsanto
Phillips Petroleum Company
M. W. Kellogg Company
DuPont Engineering
E. I. du Pont de Nemours & Company
Procter & Gamble Company
Dow Chemical Company
Moore Products Company
August Systems, Ltd.
Chevron Research & Technology Company
Rohm & Haas
Stubbs Overbeck & Associates
Fina Oil & Chemical Company
E. I. du Pont de Nemours & Company
Industrial Control Service, Inc.
Rhone-Poulenc, Inc.
Honeywell SMS
Chevron USA
Consultant
Hoechst Celanese Corporation
Murphy Oil Company
Bently Nevada
Mobil Research & Development Corporation
BASF Corporation
Bently Nevada
E.I. du Pont de Nemours & Company
Teknillinen Tarkastuskeskus
Entergy Operations, Inc.
Square D Company
Price Engineering Company
Kingwood Technology Group
E. I. du Pont de Nemours & Company
Factory Mutual Research Corporation
CALTEK Pacific-Minas Corporation
Kinetics Technology International
Consultant
Union Carbide Corporation
Exxon Chemical Company
Allen-Bradley Company

*One vote per company

S. McCormick

3M Company

NAME

COMPANY

*M. McElroy
F. McKenna
N. McLeod
R. McNab
*F. Mears
*W. Mostia, Jr.
I. Nimmo
J. Nye
*D. Ogwude
T. Ostrowski
*J. Palomar
J. Paques
B. Phelps
*W. Purser
R. Raghaven
G. Ramachandran
*K. Rashida
C. Richard
L. Richardson
*C. Rischar
*W. Robinson
G. Russcher
*D. Sanders
K. Schilowsky
J. Schroeder
R. Shah
T. Shephard
*J. Simon
I. Smith
S. Smith
J. Sottnik
R. Spiker
R. Spinks
*P. Stavrianidis
R. Stevens
H. Storey
L. Suttinger
H. Thomas
*C. Thurston
M. Toffolo
*W. Valerie
T. Walczak
D. Watkins
M. Weber
S. Weiner

Pepperl + Fuchs Systems
FMcK Associates, Ltd.
Elf Atochem
Arco Chemical Company
Mobil Research & Development Corporation
Amoco Corporation
Honeywell, Inc.
Exxon Research and Engineering Company
Chevron Research & Technology Company
Occidental Chemical Corporation
Chevron Research & Technology Company
Institut de Recherche
Citgo Petroleum Corporation
Shell Oil Company
Consultant
Cytec Industries, Inc.
Allen-Bradley Company
Mobil Oil Company
UOP
Allen-Bradley Company
Amoco Corporation
Westinghouse Electric Company
August Systems, Ltd.
Marathon Oil Company
Tosco Corporation
Koch Industries
Caltex Services Corporation
M. W. Kellogg Company
Campbell Love Associates
Touch Technology, Inc.
United Engineers & Constructors
GTI Industrial Automation
Petrocon Engineering, Inc.
Factory Mutual Research Corporation
U.S. Department of Energy
Shell Development Company
Westinghouse Savannah River Company
Air Products & Chemicals
Union Carbide Corporation
Elsag Bailey (Canada), Inc.
Arco Oil & Gas
GE Fanuc
Dow Chemical Company
TUV-IQSE
PC&E Consulting Engineers

*One vote per company

W. Welz, Jr.
*G. Wristen

BHP Engineers & Constructors, Inc.
E. I. du Pont de Nemours & Company

This published standard was approved for publication by the ISA Standards and Practices Board on February 15, 1996.

NAME

COMPANY

M. Widmeyer, Vice President	Washington Public Power Supply System
H. Baumann	H. D. Baumann, Inc.
D. Bishop	Chevron USA Production Company
P. Brett	Honeywell, Inc.
W. Calder III	Calder Enterprises
H. Dammeyer	Phoenix Industries, Inc.
R. Dieck	Pratt & Whitney
W. Holland	Southern Company Services, Inc.
A. Iverson	Lyondell Petrochemical Company
K. Lindner	Endress + Hauser GmbH + Company
T. McAvinew	Metro Wastewater Reclamation District
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Honeywell Industrial Automation & Control
J. Mock	Consultant
E. Montgomery	Fluor Daniel, Inc.
D. Rapley	Rapley Engineering Services
R. Reimer	Rockwell Automation A-B
R. Webb	Pacific Gas & Electric Company
W. Weidman	Consultant
J. Weiss	Electric Power Research Institute
J. Whetstone	National Institute of Standards & Technology
H. Wiegler	Canus Corporation
C. Williams	Eastman Kodak Company
G. Wood	Graeme Wood Consulting
M. Zielinski	Fisher-Rosemount

Contents

Introduction	13
1 Scope	15
1.1 Boundaries of the Safety Instrumented System (SIS)	15
1.2 Exclusions	16
2 Conformance to this standard	17
2.1 Conformance guidance	17
2.2 Existing systems	17
3 Definition of terms and acronyms	18
3.1 Definitions	18
3.2 Acronyms	22
4 Safety life cycle	23
4.1 Scope	23
4.2 Safety Life Cycle steps	25
5 Safety requirements specifications development	27
5.1 Objective	27
5.2 Input requirements	27
5.3 Safety functional requirements	27
5.4 Safety integrity requirements	28
6 SIS conceptual design	28
6.1 Objectives	28
6.2 Conceptual design requirements	28
7 SIS detailed design	29
7.1 Objective	29
7.2 General requirements	29
7.3 SIS logic solver	30
7.4 Field devices	31
7.5 Interfaces	32
7.6 Power sources	34
7.7 System environment	34
7.8 Application logic requirements	34
7.9 Maintenance or testing design requirements	35
8 Installation, commissioning and pre-startup acceptance test	36
8.1 Objective	36
8.2 Installation	36
8.3 Commissioning	36
8.4 Pre-Startup Acceptance Test (PSAT)	36

9 SIS operation and maintenance	38
9.1 Objective.....	38
9.2 Training.....	38
9.3 Documentation	38
9.4 SIS operating procedures	38
9.5 Maintenance program.....	38
9.6 Testing, inspection, and maintenance	39
9.7 Functional testing	39
9.8 Documentation of functional testing	40
10 SIS Management Of Change (MOC)	41
10.1 Objective.....	41
10.2 MOC procedure	41
10.3 MOC documentation.....	42
11 Decommissioning	42
11.1 Objective.....	42
11.2 General.....	43
12 Differences	43
12.1 Terminology	44
12.2 Organizational differences	44
12.3 Technology differences	46
Annexes	
A (Informative) — Information and examples illustrating methods for determining Safety Integrity Level (SIL) for a Safety Instrumented System (SIS)	47
A.1 Introduction	47
A.2 Safety Integrity Level (SIL) considerations and the process example.....	48
A.3 Example methods for selecting SIL.....	50
B (Informative) — SIS design considerations	55
B.1 Separation - identical or diverse.....	55
B.2 Redundancy - identical or diverse	58
B.3 Software design considerations	59
B.4 Technology selection	60
B.5 Failure rates and failure modes.....	63
B.6 Architecture	66
B.7 Power sources	66
B.8 Common cause failures	69
B.9 Diagnostics.....	70
B.10 Field devices	72
B.11 User interface.....	75
B.12 Security	77
B.13 Wiring practices.....	78
B.14 Documentation	79
B.15 Functional test interval	79
C (Informative) — Informative references	81

D (Informative) — Example	85
D.1 Introduction to the example problem.....	85
D.2 Safety Life Cycle (Figure 4.1)	85
D.3 Safety requirement specification	85
D.4 Safety integrity requirements (5.4).....	88
D.5 Conceptual design (6.0).....	89
D.6 Detail design (7.0).....	90

E (Informative) — Index.....	93
-------------------------------------	-----------

Figures

1.1 — Definition of Safety Instrumented Systems (SIS)	16
4.1 — Safety Life Cycle	24
A.1 — Company ABC, Site XX, Specific SIL implementation techniques, example only	50
A.2 — Process example	51
A.3 — Company ABC, Site XX, Example of a qualitative matrix for the determining SIL.....	52
D.1 — Basic process control scheme	86
D.2 — Tentative design solution	91

Tables

3.1 — Safety Integrity Level (SIL).....	21
4.1 — Safety Integrity Level performance requirements	25
A.1 — Modified HAZOP documentation example	53
B.5.1 — Typical SIS failure modes	64
B.5.2 — Typical Programmable Electronic Failure Modes.....	65
B.9.1 — Fault types.....	70
B.9.2 — Diagnostic tests for programmable electronics	72

Introduction

Purpose

This standard addresses the application of Safety Instrumented Systems (SIS) for the process industries. The SIS addressed includes Electrical (E)/, Electronic (E)/ and Programmable Electronic (PE) technology. This standard is process industry specific within the framework of the International Electrotechnical Commission (IEC) draft Publication 1508 (References C.8 and C.9). This standard follows the Safety Life Cycle presented later (see Figure 4.1).

This document is intended for those who are involved with SIS in the areas of

- design and manufacture of SIS products, selection, and application
- installation, commissioning, and Pre-Startup Acceptance Test
- operation, maintenance, documentation, and testing

Objective

The objective is to define the requirements for Safety Instrumented Systems.

Organization

This standard is organized into three major parts. The main body of the standard (Clauses 1-11) present mandatory specific requirements. Clause 12 provides key differences between ISA-S84.01 and IEC draft Publication 1508. Informative Annexes A through E present additional non-mandatory (informative) technical information that is useful in SIS applications.

Draft Technical Report 84.02 (ISA-dTR84.02), which is issued under separate cover, provides non-mandatory (informative) technical guidance in Safety Integrity Level analysis.

1 Scope

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

This standard addresses Electrical/Electronic/Programmable Electronic System (E/E/PES), associated sensors, final elements, and interfaces used in automated Safety Instrumented Systems (SIS) for the process industries (Reference C.6). Examples of the E/E/PES technologies are:

- a) Electromechanical relays;
- b) Solid state logic;
- c) PES;
- d) Motor-driven timers;
- e) Solid state relays and timers;
- f) Hard-wired logic; and
- g) Combinations of the above.

1.1 Boundaries of the Safety Instrumented System (SIS)

1.1.1 Figure 1.1 defines the boundaries of the SIS and identifies the devices that may be included in the system. The SIS described in this standard is that portion of the diagram enclosed within the double lined box.

1.1.2 The SIS includes all elements from the sensor to the final element, including inputs, outputs, power supply, and logic solvers. SIS user interface may be in the SIS.

1.1.3 Other interfaces to the SIS are considered a part of the SIS if they have potential impact on its safety function.

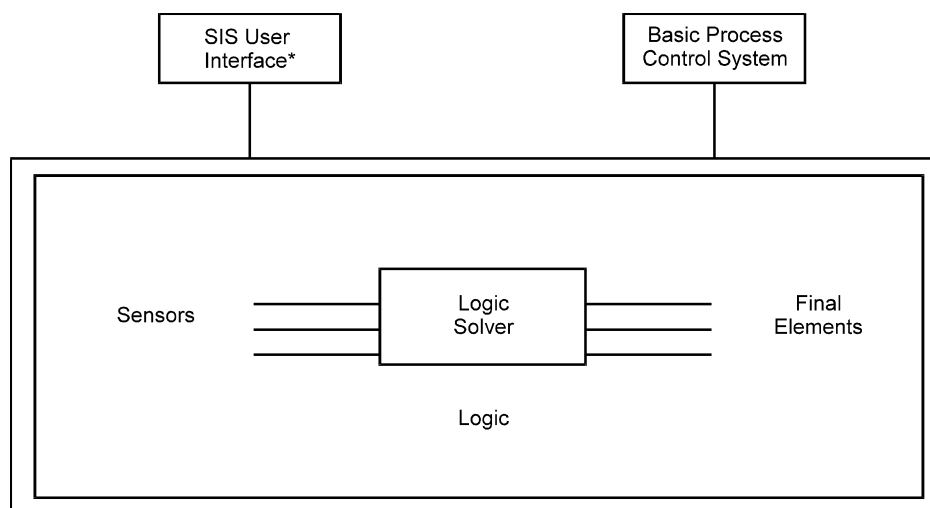


Figure 1.1 — Definition of Safety Instrumented Systems (SIS)

1.2 Exclusions

1.2.1 This standard identifies all the steps of the Safety Life Cycle (see Figure 4.1) but does not define the method(s) that may be used in some of the steps.

1.2.2 This standard does not address management of the non-SIS portion of the design or the management of the startup process.

1.2.3 In jurisdictions where the governing authorities (Federal, State, Province, County, City, etc.) have established Process Safety Design, Process Safety Management, or other requirements, these laws shall in all cases take precedence over those requirements defined in this standard. These factors must be integrated into the Safety Life Cycle at the appropriate step.

1.2.4 This standard does not address the codes, regulations, and other requirements that apply only to the Nuclear Industry.

1.2.5 The activity of identifying process hazards by use of Process Hazards Analysis methods is not part of this standard.

1.2.6 Defining the need for a Safety Instrumented Systems is not included in this standard.

1.2.7 This standard is not intended to be used as a stand-alone system purchase specification. It will not eliminate the need for sound engineering judgment. It also does not mandate the use of any particular technology.

1.2.8 The standard is not intended to apply to Basic Process Control Systems (BPCS).

1.2.9 This standard is not intended for pneumatic or hydraulic logic solvers.

1.2.10 This standard does not consider the use of technology that is not currently utilized in Safety Instrumented Systems. As new technology evolves and becomes available (e.g., ISA SP50 Fieldbus) it will be addressed in scheduled (5 year) revisions to this standard. In the interim, if new system performance justifies its use, new technology shall be user approved before use in safety applications. In these cases, the new technology implementation may require exception to some standard requirements of S84.01. Exceptions shall be documented to demonstrate that the new approach satisfies the safety requirements.

1.2.11 Analysis of the capability of humans to act on human-machine interface information is part of the Process Hazards Analysis and is outside the scope of this standard.

1.2.12 Instrumentation installed for the purpose of monitoring conditions that may lead to chronic health effects is not covered by this standard.

1.2.13 This standard does not cover instrumentation installed principally for the purpose of property protection.

1.2.14 Systems where operator action is the sole means required to return the process to a safe state are not covered by this standard. (e.g., alarm systems, fire and gas monitoring systems, etc.)

2 Conformance to this standard

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

To conform to the requirements of this standard, the following shall be adhered to:

2.1 Conformance guidance

2.1.1 To conform to this Standard, it must be shown that each of the requirements have been satisfied and therefore the Clause objectives have been met.

2.1.2 Where a requirement is qualified by reference to an informative annex, this indicates that a range of techniques and measures can be used to satisfy that requirement including techniques and measures not listed in the informative annex.

2.1.3 The techniques and measures included in normative Clauses 1 through 11 are considered good engineering practices in the design and support of Safety Instrumented Systems.

2.2 Existing systems

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

3 Definition of terms and acronyms

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

3.1 Definitions

For the purposes of this standard, the following definitions apply:

3.1.1 application program: See software (3.1.58.1).

3.1.2 application software: See software (3.1.58.1).

3.1.3 architecture: The arrangement and interconnection of the hardware components or modules that comprise the SIS.

3.1.4 availability: See safety availability (3.1.51).

3.1.5 Basic Process Control System (BPCS): A system that responds to input signals from the equipment under control and/or from an operator and generates output signals, causing the equipment under control to operate in the desired manner. Some examples include control of an exothermic reaction, anti-surge control of a compressor, and fuel/air controls in fired heaters. Also referred to as Process Control System.

3.1.6 bypassing: Act of temporarily defeating a safety function in a SIS.

3.1.7 common cause

3.1.7.1 common cause fault: A single source that will cause failure in multiple elements of a system. The single source may be either internal or external to the system.

3.1.7.2 common cause failure: The result of a common cause fault.

3.1.8 communication

3.1.8.1 external communication: Data exchange between the SIS and a variety of systems or devices that are outside the SIS. These include shared operator interfaces, maintenance/engineering interfaces, data acquisition systems, host computers, etc.

3.1.8.2 internal communication: Data exchange between the various devices within a given SIS. These include bus backplane connections, the local or remote I/O bus, etc.

3.1.9 coverage: See diagnostic coverage (3.1.14).

3.1.10 covert fault: Faults that can be classified as hidden, concealed, undetected, unrevealed, latent, etc.

3.1.11 decommissioning: The permanent removal of a complete SIS from active service.

3.1.12 de-energize to trip: SIS circuits where the outputs and devices are energized under normal operation. Removal of the source of power (e.g., electricity, air) causes a trip action.

3.1.13 demand: A condition or event that requires the SIS to take appropriate action to prevent a hazardous event from occurring or mitigate the consequence of a hazardous event.

3.1.14 diagnostic coverage: For SIS with active fault-detection capabilities, the ratio of detectable faults to the total number of faults.

3.1.15 diverse: Use of different technologies, equipment or design methods to perform a common function with the intent to minimize common cause faults (see 3.1.45, 3.1.55, and B.2).

3.1.16 Electrical (E)/ Electronic (E)/Programmable Electronic Systems (PES) (E/E/PES): When used in this context, electrical refers to logic functions performed by electromechanical techniques, (e.g., electromechanical relay, motor driven timers, etc.), electronic refers to logic functions performed by electronic techniques, (e.g., solid state logic, solid state relay, etc.), and Programmable Electronic System refers to logic performed by programmable or configurable devices [e.g., Programmable Logic Controller (PLC), Single Loop Digital Controller (SLDC), etc.] Field devices are not included in E/E/PES.

3.1.17 electronic (/E): See E/E/PES (3.1.16).

3.1.18 embedded software: See software (3.1.58.2).

3.1.19 energize to trip: SIS circuits where the outputs and devices are de-energized under normal operation. Application of power (e.g., electricity, air) causes a trip action.

3.1.20 fail-safe: The capability to go to a predetermined safe state in the event of a specific malfunction.

3.1.21 fault tolerance: Built-in capability of a system to provide continued correct execution of its assigned function in the presence of a limited number of hardware and software faults.

3.1.22 field devices: Equipment connected to the field side of the SIS I/O terminals. Such equipment includes field wiring, sensors, final control elements, and those operator interface devices hard-wired to SIS I/O terminals.

3.1.23 firmware: Special purpose memory units containing software embedded in protected memory required for the operation of programmable electronics.

3.1.24 forcing: A PES engineering station function that provides the capability to override the application program and to change the states of inputs and outputs.

3.1.25 functional testing: Periodic activity to verify that the SIS is operating per the Safety Requirement Specifications Testing.

3.1.26 hardware configuration: See architecture (3.1.3).

3.1.27 hard-wired: Electrical connections accomplished without the use of software or firmware.

3.1.28 hazard: Chemical or physical condition that has the potential for causing injury to people or the environment (Reference C.12).

3.1.29 input/output modules

3.1.29.1 input module: E/E/PES or subsystem that acts as an interface to external devices and converts input signals into signals that the E/E/PES can utilize.

3.1.29.2 output module: E/E/PES or subsystem that acts as an interface to external devices and converts output signals into signals that can actuate external devices.

3.1.30 interface: Shared boundary through which information is conveyed.

3.1.31 integration: Process of assembling multiple components or subsystems to form a system.

3.1.32 logic solver: E/E/PES components or subsystems that execute the application logic. Electronic and programmable electronics include input/output modules.

3.1.33 off-line: Process, to which the SIS is connected, is shut down.

3.1.34 on-line: Process, to which the SIS is connected, is operating.

3.1.35 overt faults: Faults that are classified as announced, detected, revealed, etc.

3.1.36 permissive: Condition within a logic sequence that must be satisfied before the sequence is allowed to proceed to the next phase.

3.1.37 Pre-Startup Acceptance Test (PSAT): Process of confirming performance of the total integrated SIS to assure its conformance to the Safety Requirement Specifications and design.

3.1.38 preventive maintenance: Maintenance practice in which equipment is maintained on the basis of a fixed schedule, dictated by manufacturer's recommendation or by accumulated data from operating experience.

3.1.39 Probability of Failure on Demand (PFD): A value that indicates the probability of a system failing to respond to a demand. The average probability of a system failing to respond to a demand in a specified time interval is referred to as PFDavg. PFD equals 1 minus Safety Availability [see safety availability (3.1.51)].

3.1.40 process industry sector: Refers to those processes involved in, but not limited to, the production, generation, manufacture, and/or treatment of oil, gas, wood, metals, food, plastics, petrochemicals, chemicals, steam, electric power, pharmaceuticals, and waste material(s).

3.1.41 Programmable Electronic System (PES): See E/E/PES (3.1.16).

3.1.42 protection layer: Engineered safety features or protective systems or layers that typically involve special process designs, process equipment, administrative procedures, the Basic Process Control System (BPCS), and/or planned responses to protect against an imminent hazard. These responses may be either automated or initiated by human actions (see Annex A for guidance).

3.1.43 qualitative methods: Methods of design and evaluation developed through experience and/or the application of good engineering judgement.

3.1.44 quantitative methods: Methods of design and evaluation based on numerical data and mathematical analysis.

3.1.45 redundancy: Use of multiple elements or systems to perform the same function. Redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

3.1.46 reliability: Probability that a system can perform a defined function under stated conditions for a given period of time.

3.1.47 replacement in kind: A replacement that satisfies the design specification.

3.1.48 reset: Action that restores the equipment under control to a predetermined normal enabled or operating state.

3.1.49 risk assessment: Process of making risk estimates and using the results to make decisions.

3.1.50 safe state: State that the equipment under control, or process, shall attain as defined by the Process Hazards Analysis (PHA).

3.1.51 safety availability: Fraction of time that a safety system is able to perform its designated safety service when the process is operating. In this standard, the average Probability of Failure on Demand (PFDavg) is the preferred term. (PFD equals 1 minus Safety Availability; see 3.1.39.)

3.1.52 Safety Integrity Level (SIL): One of three possible discrete integrity levels (SIL 1, SIL 2, SIL 3) of Safety Instrumented Systems. SILs are defined in terms of Probability of Failure on Demand (PFD) (see Table 3.1).

Table 3.1 — Safety Integrity Level (SIL)

Safety Integrity Level (SIL)	Probability of Failure on Demand Average Range (PFD avg)
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}

3.1.53 Safety Instrumented Systems (SIS): System composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated (see Figure 1.1). Other terms commonly used include Emergency Shutdown System (ESD, ESS), Safety Shutdown System (SSD), and Safety Interlock System.

3.1.54 Safety Life Cycle: Sequence of activities involved in the implementation of the Safety Instrumented Systems from conception through decommissioning (see Figure 4.1).

3.1.55 separation: The use of multiple devices or systems to segregate control from safety functions. Separation can be implemented by identical elements (identical separation) or by diverse elements (diverse separation).

3.1.56 shall: Indicates a mandatory requirement.

3.1.57 SIS components: A constituent part of a SIS. Examples of SIS components are field devices, input modules, output modules, and logic solvers.

3.1.58 software

3.1.58.1 application software: Software specific to the user application in that it is the SIS functional description programmed in the PES to meet the overall Safety Requirement Specifications (see Clause 5). In general, it contains logic sequences, permissives, limits, expressions, etc., that control the appropriate input, output, calculations, decisions necessary to meet the safety functional requirements.

3.1.58.2 embedded software: Software that is part of the system supplied by the vendor and is not accessible for modification by the end user. Embedded software is also referred to as firmware or system software.

3.1.58.3 utility software: Software tools for the creation, maintenance, and documentation of application programs. These software tools are not required for the operation of the SIS.

3.1.59 spurious trip: Refers to the shutdown of the process for reasons not associated with a problem in the process that the SIS is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, electrical fault, transient, ground plane interference, etc.). Other terms used include nuisance trip and false shut down.

3.1.60 systematic failures: Failures due to errors (including mistakes and acts of omissions) in Safety Life Cycle activities that cause the SIS to fail under some particular combination of inputs or under a particular environmental condition. Systematic failures can arise in any Safety Life Cycle step.

3.1.61 Test Interval (TI): Time between functional tests.

3.1.62 user approved: Hardware, software, procedures, etc., that the user has evaluated and determined to be acceptable for the application.

3.1.63 verification: Process of confirming for certain steps of the Safety Life Cycle that the objectives are met.

3.1.64 voting system: Redundant system (e.g., "m" out of "n", one out of two [1oo2] to trip, two out of three [2oo3], etc.) that requires at least "m" of the "n" channels to be in agreement before the SIS can take an action.

3.2 Acronyms

BPCS:	Basic Process Control System
CFR:	Code of Federal Regulations
E/E/PES:	Electrical/Electronic/Programmable Electronic System
I/O:	Input/Output
MOC:	Management of Change
MTBF:	Mean Time Between Failures
MTTF:	Mean Time To Failure
MTTR:	Mean Time To Repair
OSHA:	Occupational Safety and Health Administration

PES:	Programmable Electronic System
PFD:	Probability of Failure on Demand
PHA:	Process Hazards Analysis
PSAT:	Pre-Startup Acceptance Test
PSSR:	Pre-Startup Safety Review
SIL:	Safety Integrity Level
SIS:	Safety Instrumented Systems
WDT:	Watchdog Timer

4 Safety life cycle

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

4.1 Scope

The clauses in this standard are organized based on the Safety Life Cycle (see Figure 4.1). The Safety Life Cycle covers the Safety Instrumented Systems (SIS) activities from initial conception through decommissioning. Note that this standard does not address the method for performing initial Safety Life Cycle activities, such as:

- a) Performing conceptual process design
- b) Performing Process Hazards Analysis & risk assessment
- c) Defining non-SIS protection layers
- d) Defining the need for an SIS
- e) Determining required Safety Integrity Level

These activities are outside the scope of this standard.

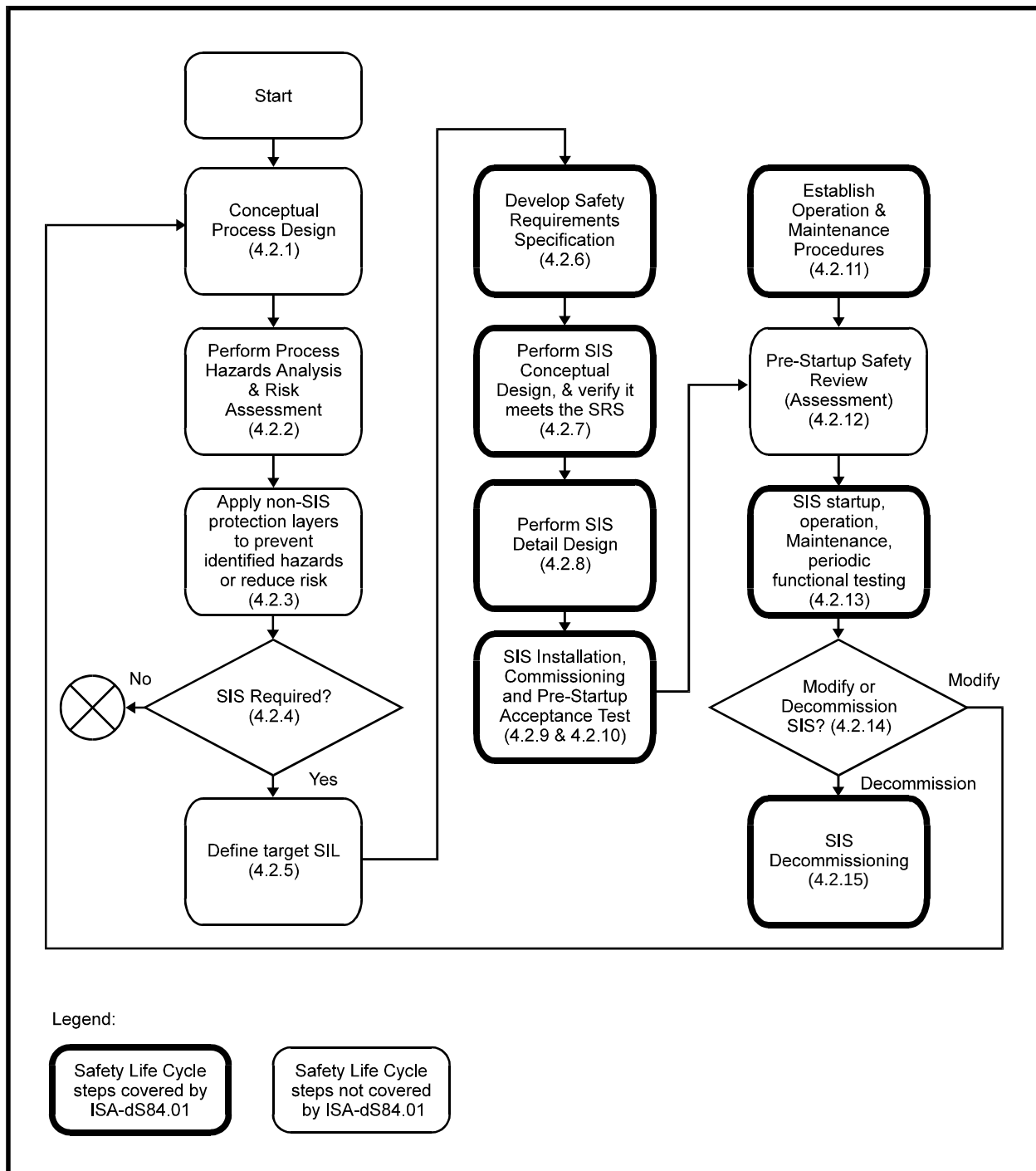


Figure 4.1 — Safety Life Cycle

During the Safety Life Cycle of a SIS, there may be points where iterations are necessary. A few of these are indicated in the Safety Life Cycle presented, but these should not be considered the only points where iteration may be necessary.

4.2 Safety Life Cycle steps

4.2.1 The first step in the Safety Life Cycle is concerned with the conceptual process design. The method for accomplishing this step is outside the scope of this standard.

4.2.2 The second step is concerned with identifying the hazards and hazardous events for a process and assessing the level of risk involved. This standard does not address the methods for performing this analysis and evaluation but assumes it has taken place prior to applying the principles in this document. The method(s) for accomplishing this step is outside the scope of this standard.

4.2.3 Once the hazards and risks have been identified, appropriate technology (including process and equipment modifications) is applied to eliminate the hazard, to mitigate their consequences or reduce the likelihood of the event. The third step involves the application of non-SIS protection layers to the process. The method(s) for accomplishing this step is outside the scope of this standard.

4.2.4 Next an evaluation is made to determine if an adequate number of non-SIS protection layers have been provided.

The desire is to provide appropriate number of non-SIS protection layers, such that SIS protection layer(s) are not required. Therefore, consideration should be given to changing the process and/or its equipment utilizing various non-SIS protection techniques, before considering adding SIS protection layer(s). The method for accomplishing this step is outside the scope of this standard.

4.2.5 If an SIS is appropriate, the next step is establishing the requirements for the SIS by defining a target Safety Integrity Level (SIL) (See Annex A for guidance). A SIL defines the level of performance needed to achieve the user's process safety objective. SILs are defined as 1, 2, and 3. SISs above SIL 3 are not addressed in this standard. The higher the SIL, the more available the safety function of the SIS. Performance is improved by the addition of redundancy, more frequent testing, use of diagnostic fault detection, and use of diverse sensors and final control elements, etc. Performance is also improved through better control of design, operation, and maintenance procedures.

Associated with the SIL are Probability of Failure on Demand average (see Table 4.1).

Table 4.1 — Safety Integrity Level performance requirements

SAFETY INTEGRITY LEVEL	1	2	3
SIS PERFORMANCE REQUIREMENTS	Safety Availability Range		
	0.9 to 0.99	0.99 to 0.999	0.999 to 0.9999
	PFD Average Range		
	10^{-1} to 10^{-2}	10^{-2} to 10^{-3}	10^{-3} to 10^{-4}

The SIL concept is utilized in several steps of the Safety Life Cycle. See Annex A for guidance on SIL determination. The method for accomplishing this step is outside the scope of this standard.

4.2.6 The next step is developing Safety Requirement Specifications. The Safety Requirement Specifications document functional and integrity requirements for the SIS (see Clause 5).

4.2.7 The next step involves developing the SIS Conceptual Designs that may meet the Safety Requirement Specifications. Annex B provides guidance on the selection of architectures to meet SIL requirements (see Clause 6).

4.2.8 Once SIS Conceptual Design is complete, the detailed design can be performed (see Clause 7).

4.2.9 Install the SIS (see Clause 8).

4.2.10 After installation is complete, the Commissioning and Pre-Startup Acceptance Test (PSAT) of the SIS shall be performed (see Clause 8).

4.2.11 SIS Operation and Maintenance Procedures may be developed at any step of the Safety Life Cycle and shall be completed prior to startup (see Clause 9).

4.2.12 Prior to startup of the SIS, a Pre-Startup Safety Review (PSSR) shall take place. This PSSR shall include the following SIS activities:

- a) Verification that the SIS was constructed, installed, and tested in accordance with the Safety Requirement Specifications.
- b) Safety, operating, maintenance, Management of Change (MOC), and emergency procedures pertaining to the SIS are in place and are adequate.
- c) PHA recommendations that apply to the SIS have been resolved or implemented.
- d) Employee training has been completed and includes appropriate information about the SIS.

The planning and execution of this activity is outside the scope of this standard.

4.2.13 After PSSR, the SIS may be placed in operation. This step includes startup, normal operation, maintenance, and periodic Functional Testing (see Clause 9).

4.2.14 If modifications are proposed, their implementation shall follow a Management of Change (MOC) procedure. The appropriate steps in the Safety Life Cycle shall be repeated to address the safety impact of the change (see Clause 10).

4.2.15 At some time, the need for the SIS will cease. For example, this may be caused by plant closure, or the removal or change of the process. The decommissioning of the SIS shall be planned, and appropriate steps should be taken to ensure that this is accomplished in a manner that does not compromise safety (see Clause 11).

5 Safety requirements specifications development

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

5.1 Objective

The objective is to develop specifications for Safety Instrumented Systems (SIS) design. These Safety Requirement Specifications consist of both safety functional requirements and safety integrity requirements. The Safety Requirement Specifications can be a collection of documents or information.

5.2 Input requirements

The information required from the Process Hazards Analysis (PHA) or process design team to develop the Safety Requirement Specifications, includes the following.

- 5.2.1** A list of the safety function(s) required and the SIL of each safety function.
- 5.2.2** Process information (incident cause, dynamics, final elements, etc.) of each potential hazardous event that requires a SIS.
- 5.2.3** Process common cause failure considerations such as corrosion, plugging, coating, etc.
- 5.2.4** Regulatory requirements impacting the SIS.

5.3 Safety functional requirements

The safety functional requirements shall include the following.

- 5.3.1** The definition of the safe state of the process, for each of the identified events.
- 5.3.2** The process inputs to the SIS and their trip points,
- 5.3.3** The normal operating range of the process variables and their operating limits,
- 5.3.4** The process outputs from the SIS and their actions,
- 5.3.5** The functional relationship between process inputs and outputs, including logic, math functions, and any required permissives.
- 5.3.6** Selection of de-energized to trip or energized to trip.
- 5.3.7** Consideration for manual shutdown.
- 5.3.8** Action(s) to be taken on loss of energy source(s) to the SIS.

- 5.3.9 Response time requirements for the SIS to bring the process to a safe state.
- 5.3.10 Response action to any overt fault.
- 5.3.11 Human-machine interfaces requirements.
- 5.3.12 Reset function(s).

5.4 Safety integrity requirements

Safety integrity requirements shall include the following.

- 5.4.1 The required SIL for each safety function.
- 5.4.2 Requirements for diagnostics to achieve the required SIL (see B.9 for guidance).
- 5.4.3 Requirements for maintenance and testing to achieve the required SIL.
- 5.4.4 Reliability requirements if spurious trips may be hazardous.

6 SIS conceptual design

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

6.1 Objectives

To define those requirements needed to develop and verify a SIS Conceptual Design that meets the Safety Requirements Specifications.

6.2 Conceptual design requirements

6.2.1 The Safety Instrumented Systems (SIS) architecture for each safety function shall be selected to meet its required Safety Integrity Level (SIL). (e.g., The selected architecture may be one out of one [1oo1], 1oo2 voting, 2oo3 voting, etc.)

6.2.2 A SIS may have a single safety function or multiple safety functions that have a common logic solver and/or input and output devices. When multiple safety functions share common components, the common components shall satisfy the highest SIL of the shared safety function. Components of the system that are not common must meet the SIL requirements for the safety function that they address. When multiple SISs are combined in a system where they share common logic or components, the potential for common cause faults is increased. Programming, accessibility, maintenance, power supplies, and security are typical common cause issues to consider.

6.2.3 The desired SIL shall be met through a combination of the following design considerations:

- a) Separation - identical or diverse (see B.1 for guidance)
- b) Redundancy - identical or diverse (see B.2 for guidance)
- c) Software design considerations (see B.3 for guidance)
- d) Technology selection (see B.4 for guidance)
- e) Failure rates and failure modes (see B.5 for guidance)
- f) Architecture (see B.6 for guidance)
- g) Power sources (see B.7 for guidance)
- h) Common cause failures (see B.8 for guidance)
- i) Diagnostics (see B.9 for guidance)
- j) Field devices (see B.10 for guidance)
- k) User interface (see B.11 for guidance)
- l) Security (see B.12 for guidance)
- m) Wiring practices (see B.13 for guidance)
- n) Documentation (see B.14 for guidance)
- o) Functional test interval (see B.15 for guidance)

7 SIS detailed design

NOTE — THIS CLAUSE IS PART OF THIS STANDARD AND CONTAINS MANDATORY REQUIREMENTS.

7.1 Objective

To provide detailed requirements for the design of the Safety Instrumented Systems (SIS) to achieve the requirements of the Safety Requirement Specifications and conceptual design.

7.2 General requirements

7.2.1 The SIS design shall be capable of meeting the Safety Integrity Level (SIL).

7.2.2 The SIS may include sequencing functions to take the process to or maintain it in a safe state.

7.2.3 The SIS may contain one or more interlocks or safety functions.

7.2.4 The SIS design documents shall be under control of a formal revision and release control program.

7.2.5 The manufacturer of equipment used in SIS service shall maintain a formal revision and release control program for the equipment, including applicable software. The use of visible markings or user interfaces to identify this information is acceptable (e.g., part #, serial #, batch #, etc.).

7.2.6 The design shall ensure that the hardware and software used in an application are compatible.

7.2.7 The action of any non-safety function, if implemented by the SIS, shall not interrupt or compromise any SIS safety functions.

7.2.8 The required safe states of each SIS component required for the safety function shall be defined.

7.2.9 The SIS shall be designed such that once it has placed the process in a safe state, it shall remain in the safe state until a reset has been initiated. The requirement for a manual or automatic reset shall be as defined in the Safety Requirements Specifications.

7.2.10 Manual means, independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the Safety Requirements Specifications.

7.2.11 Any detected single fault that causes a SIS failure shall result in an automatic, predetermined, safe failure action; and/or a safe process condition if the appropriate response action is undertaken.

7.2.12 The design shall apply codes and standards for environmental and hazardous area classifications (e.g., NFPA 70, National Electrical Code, Article 500)(see C.5 for guidance).

7.2.13 SIS Input/Output power circuits shall be separated from circuits used for any other purpose except where the sensor or final control element is shared as allowed in 7.4.2.2 and 7.4.3.1.

7.3 SIS logic solver

7.3.1 The logic solver supplier shall provide an integrated design including, where applicable, input module(s), output module(s), maintenance interface device(s), communication(s), and utility software. The integrated design shall be documented.

7.3.2 The logic solver supplier shall provide Mean Time To Failure (MTTF) data, covert failure mode listing, and frequency of occurrence of identified covert failures. The method and data sources for the above shall be provided.

7.3.3 PES logic solvers shall have methods (internal and/or external) to protect against covert faults (e.g., comparison of logic solver performance versus process action, embedded or application software testing the logic solver performance).

7.3.4 The logic solver shall be separated (see B.1 for guidance) from the Basic Process Control System (BPCS) except where some applications have combined BPCS and SIS functions in one "logic solver" (e.g., gas turbines). In these cases, the BPCS/SIS logic solver shall meet the SIL (see C.1 for additional guidance).

7.3.5 The logic solver shall be designed to ensure the process will not automatically restart when power is restored, unless Process Hazards Analysis indicates this is appropriate.

7.4 Field devices

7.4.1 General requirements

7.4.1.1 Energize to trip discrete input/output circuits shall apply a method (e.g., end-of-line monitor, such as pilot current continuously monitored to ensure circuit continuity; the pilot current shall not be of sufficient magnitude to affect proper I/O operation) to assure circuit integrity.

7.4.1.2 When remote input/output is used, it shall be evaluated in conjunction with the logic solver (see B.6 for guidance).

7.4.1.3 Each individual field device shall have its own dedicated wiring to the system Input/Output, except in the following cases:

- a) Multiple connected discrete sensors connected in series to a single input if the sensors monitor the same process condition (e.g., motor overloads)
- b) Multiple connected Final Control Elements (FCE) to a single output if each FCE services the same process condition
- c) User approved systems such as fire and gas detection systems
- d) See 1.2.10 for ISA SP50 Fieldbus.

7.4.1.4 Field devices shall be selected and installed to minimize failures that could relate inaccurate information due to conditions arising from the process and environmental conditions. Conditions that shall be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, coking, and temperature and pressure extremes.

7.4.2 Sensor requirements

7.4.2.1 Smart sensors shall be write protected to prevent inadvertent modification from a remote location, unless appropriate safety review allows the use of read/write.

7.4.2.2 Sensors for SIS shall be separated from the sensors for the Basic Process Control System (BPCS). Two exceptions are allowed provided the failure of the sensor does not create a condition that the SIS is intended to protect against:

- a) If redundant sensors are used, they may be connected to both the BPCS and the SIS provided that any failure in the BPCS will not affect the proper operation of the sensor or the ability of the SIS to read the sensor properly (see B.1.5).
- b) If the PHA determines that one or more protection layers other than the BPCS and the SIS offers protection redundant to that provided by the sensor (for further guidance, see Annex A).

7.4.2.3 Sensor diagnostics, vendor or user supplied, shall be provided as required to meet the SIL (see B.9 for guidance).

7.4.3 Final control element requirements

7.4.3.1 A control valve from the BPCS shall not be used as the only final element for SIL 3. A safety review shall be required to use a single BPCS control valve as the only final element for SIL 1 and 2. For additional information, see B.1.6.

7.4.3.2 Motor starters

Motor starters are typically common to both the BPCS and the SIS unless the Process Hazards Analysis dictates otherwise (see B.10.4.3 for guidance).

7.5 Interfaces

This section addresses all human-machine and communication interfaces to the SIS. These can include, but are not limited to

- a) operator interface(s);
- b) maintenance/engineering interface(s); and
- c) communication interface(s).

7.5.1 Operator interface requirements

Operator interface refers to that media (e.g., CRTs, indicating lights, push-buttons, horns, alarms, etc.) used to communicate information between the operator and the SIS.

7.5.1.1 The operator interface system design shall take into consideration the loss of the SIS operator interface and the resulting requirements as defined by appropriate safety review. The design shall ensure that, upon failure of the SIS operator interface, sufficient alternate means shall be provided for the operator to bring the process to a safe state and that the automatic functions of the SIS are not compromised.

7.5.1.2 The SIS status information that is critical to maintaining the SIL shall be available as part of the operator interface. This information may include

- a) where the process is in its sequence;
- b) indication that SIS protective action has occurred;
- c) indication that a protective function is bypassed;
- d) indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- e) status of sensors and final control elements;
- f) the loss of energy where that energy loss impacts safety;
- g) the results of comparison diagnostics; and
- h) failure of environmental conditioning equipment that is necessary to support the SIS.

7.5.1.3 Changes to the SIS application software shall not be allowed from the SIS operator interface. Where the SIS maintenance/engineering interface is used as the operator interface to the SIS, changes to application software from this interface shall require appropriate safety review and access security. There may be some safety-related information that needs to be transmitted from the BPCS to the SIS. For example, in batch systems a SIS may have different setpoints or logic functions depending on the recipe being used. If so, the operator interface may be used to select the appropriate logic function in the SIS or may be used to select recipe-specific tables. For these types of applications, use only SIS systems that offer the ability to selectively allow writing to a SIS variable that is accessible to the BPCS (see B.1.8 for additional guidance), and a confirmation procedure to ensure the proper selection has been transmitted and received in the SIS.

Enabling and disabling the read-write access shall be done only by a configuration or programming process using the Maintenance/Engineering Interface with appropriate documentation and security measures. An Operator Interface shall not be allowed to perform this function.

7.5.2 Maintenance/Engineering interface requirements

Maintenance/Engineering interface is that media provided to allow proper SIS maintenance. It can include instructions and diagnostics that may be found in software, programming terminals, diagnostic tools, indicators, bypass devices, test devices, and calibration devices.

7.5.2.1 The design of SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to bring the process to a safe state. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

7.5.2.2 The maintenance/engineering interface shall provide the following functions:

- a) Access security protection to the SIS operating mode, program, data, means of disabling alarm communication, test, bypass, maintenance, etc.
- b) Access to SIS diagnostic, voting and fault handling services
- c) Access to add, delete, or modify application software
- d) Access to data necessary to troubleshoot the SIS

7.5.3 Communication interface requirements

Communication interface refers to hardware and software communication between the SIS and other devices such as the operator interfaces, maintenance/engineer interfaces, BPCS, network or peripherals.

7.5.3.1 The design of the communication interface of the SIS shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to bring the process to a safe state.

7.5.3.2 Communication signals shall be isolated from other energy sources through the use of good engineering practices, such as the use of shielded cable while maintaining a single ground plane with a single dedicated power source, or the use of fiber optics.