

ISA-TR84.00.02-2002 - Part 1



Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 1: Introduction

NOTICE OF COPYRIGHT

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



ISA—The Instrumentation,
Systems, and
Automation Society

Approved 17 June 2002



Documents
Document Sharing Hub

ISA-TR84.00.02-2002 – Part 1

Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques Part 1:
Introduction

ISBN: 1-55617-802-6

Copyright © 2002 by ISA —The Instrumentation, Systems, and Automation Society. 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-TR84.00.02-2002 – Part 1.

This document has been prepared as part of the service of ISA—the Instrumentation, Systems, and Automation Society—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. 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-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, 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, 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 STANDARD, 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 STANDARD OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS STANDARD, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE STANDARD 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 STANDARD. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE STANDARD OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE STANDARD FOR THE USER'S INTENDED APPLICATION.

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

ADDITIONALLY, THE USE OF THIS STANDARD MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE STANDARD CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS STANDARD 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 STANDARD.

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

The following people served as members of ISA Committee SP84:

NAME	COMPANY
V. Maggioli, Chair	Feltronics Corporation
R. Webb, Managing Director	POWER Engineers
C. Ackerman	Air Products & Chemicals Inc.
R. Adamski	Invensys
C. Adler	Moore Industries International Inc.
R. Bailliet	Syscon International Inc.
N. Battikha	Bergo Tech Inc.
L. Beckman	HIMA Americas Inc.
S. Bender	S K Bender & Associates
K. Bond	Shell Global Solutions
A. Brombacher	Eindhoven University of Technology
S. Brown*	DuPont Company
J. Carew	Consultant
K. Dejmek	Baker Engineering & Lisk Consulting
A. Dowell*	Rohm & Haas Company
R. Dunn*	DuPont Engineering
P. Early	ABB Industrial Systems Inc.
T. Fisher	Deceased
J. Flynt	Consultant
A. Frederickson	Triconex Corporation
R. Freeman	ABS Consulting
D. Fritsch	Fritsch Consulting Service
K. Gandhi	Kellogg Brown & Root
R. Gardner*	Dupont
J. Gilman	Consultant
W. Goble	exida.com LLC
D. Green*	Rohm & Haas Company
P. Gruhn	Siemens
C. Hardin	CDH Consulting Inc.
J. Harris	UOP LLC
D. Haysley	Albert Garaody & Associates
M. Houtermans	TUV Product Service Inc.
J. Jamison	Bantrel Inc.
W. Johnson*	E I du Pont
D. Karydas*	Factory Mutual Research Corporation
L. Laskowski	Solutia Inc.
T. Layer	Emerson Process Management
D. Leonard	D J Leonard Consultants
E. Lewis	Consultant
E. Marszal	Exida.com
N. McLeod	Atofina
W. Mostia	WLM Engineering Company
D. Ogwude	Creative Systems International

G. Ramachandran
K. Schilowsky
D. Sniezek
C. Sossman
R. Spiker
P. Stavrianidis*
H. Storey
A. Summers
L. Suttinger
R. Szanyi
R. Taubert
H. Tausch
T. Walczak
M. Weber
D. Zetterberg

Cytec Industries Inc.
Marathon Ashland Petroleum Company LLC
Lockheed Martin Federal Services
WG-W Safety Management Solutions
Yokogawa Industrial Safety Systems BV
Factory Mutual Research Corporation
Equilon Enterprises LLC
SIS-TECH Solutions LLC
Westinghouse Savannah River Company
ExxonMobil Research Engineering
BASF Corporation
Honeywell Inc.
GE FANUC Automation
System Safety Inc.
Chevron Texaco ERTC

* One vote per company.

This standard was approved for publication by the ISA Standards and Practices Board on 17 June 2002.

NAME

COMPANY

M. Zielinski
D. Bishop
D. Bouchard
M. Cohen
M. Coppler
B. Dumortier
W. Holland
E. Icahan
A. Iverson
R. Jones
V. Maggioli
T. McAviney
A. McCauley, Jr.
G. McFarland
R. Reimer
J. Rennie
H. Sasajima
I. Verhappen
R. Webb
W. Weidman
J. Weiss
M. Widmeyer
C. Williams
G. Wood

Emerson Process Management
David N Bishop, Consultant
Paprican
Consultant
Ametek, Inc.
Schneider Electric
Southern Company
ACES Inc
Ivy Optiks
Dow Chemical Company
Feltronics Corporation
ForeRunner Corporation
Chagrin Valley Controls, Inc.
Westinghouse Process Control Inc.
Rockwell Automation
Factory Mutual Research Corporation
Yamatake Corporation
Syncrude Canada Ltd.
POWER Engineers
Parsons Energy & Chemicals Group
KEMA Consulting
Stanford Linear Accelerator Center
Eastman Kodak Company
Graeme Wood Consulting



This page intentionally left blank.

Document ID: TR84.00.02Part1 2002

Contents

Foreword	9
Introduction	11
1 Scope	17
2 References	17
3 Definitions of terms and symbols.....	19
3.1 Definition of terms.....	19
3.2 Definition of symbols	33
4 Probability of failure on demand (PFD)	43
5 Modeling of SIF element failures	44
5.1 Physical failures.....	44
5.2 Hardware common cause failures.....	44
5.3 Systematic failures	44
5.4 Partitioning of SIF element failures	46
5.5 Modeling of field devices	49
5.6 Modeling of elements in PES arithmetic/logic solvers.....	50
5.7 System modeling.....	54
5.8 Failure rate data for commonly used field instrumentation	54
5.9 Statistical data analysis methods	57
6 Comparison of system analysis techniques	62
Annex A (informative) — Methodology for quantifying the effect of hardware-related common cause failures in Safety Instrumented Functions.....	67
Annex B (informative) — Fault simulation test procedure	79
Annex C (informative) — SIL quantification of SIS – Advisory software packages.....	83
Annex D (informative) — Failure mode effect, hazard and criticality analysis	85
Annex E (informative) — Common cause failures and systematic failure checklist.....	91
Annex F — Index	93



This page intentionally left blank.

Copyright The Instrumentation, Systems, and Automation Society

Safety Instrumented Systems (SIS)

— Safety Integrity Level (SIL) Evaluation Techniques

Part 1: Introduction

Foreword

The information contained in ISA-TR84.00.02-2002 is provided for information only and is not part of the ANSI/ISA-84.01-1996 Standard ⁽¹⁾ requirements.

The purpose of ISA-TR84.00.02-2002 ⁽²⁾ is to provide the process industry with a description of various methodologies that can be used to evaluate the Safety Integrity Level (SIL) of Safety Instrumented Functions (SIF).

ANSI/ISA-84.01-1996 provides the minimum requirements for implementing a SIS given that a set of functional requirements have been defined and a SIL requirement has been established for each safety instrumented function. Additional information of an informative nature is provided in the Annexes to ANSI/ISA-84.01-1996 to assist the designer in applying the concepts necessary to achieve an acceptable design. However, Standards Project 84 (SP84) determined that it was appropriate to provide supplemental information that would assist the user in evaluating the capability of any given SIF design to achieve its required SIL. A secondary purpose of this document is to reinforce the concept of the performance based evaluation of SIF. The performance parameters that satisfactorily service the process industry are derived from the SIL and reliability evaluation of SIF, namely the probability of the SIF to fail to respond to a demand and the probability that the SIF creates a nuisance trip. Such evaluation addresses the design elements (hardware, software, redundancy, etc.) and the operational attributes (inspection/maintenance policy, frequency and quality of testing, etc.) of the SIF. The basis for the performance evaluation of the SIF is safety targets determined through hazard analysis and risk assessment ⁽⁶⁾ of the process. This document demonstrates methodologies for the SIL and reliability evaluation of SIF.

The document focuses on methodologies that can be used without promoting a single methodology. It provides information on the benefits of various methodologies as well as some of the drawbacks they may have.

THE METHODOLOGIES ARE DEMONSTRATED THROUGH EXAMPLES (SIS ARCHITECTURES) THAT REPRESENT POSSIBLE SYSTEM CONFIGURATIONS AND SHOULD NOT BE INTERPRETED AS RECOMMENDATIONS FOR SIS. THE USER IS CAUTIONED TO CLEARLY UNDERSTAND THE ASSUMPTIONS AND DATA ASSOCIATED WITH THE METHODOLOGIES IN THIS DOCUMENT BEFORE ATTEMPTING TO UTILIZE THE METHODS PRESENTED HEREIN.

The users of ISA-TR84.00.02-2002 include:

- Process Hazards Analysis teams that wish to develop understanding of different methodologies in determining SIL
- SIS designers who want a better understanding of how redundancy, diagnostic coverage, diversity, etc., fit into the development of a proper SIS architecture
- Logic solver and field device suppliers

- National and International standard bodies providing guidance in the use of reliability techniques for SIS architectures
- Reliability engineers (or any engineer performing this function) can use this information to develop better methods for determining SIL in the rapidly changing SIS field
- Parties who do not have a large installed base of operating equipment sufficient to establish appropriate statistical analysis for PFD_{avg} and $MTTF^{spurious}$ for SIS components
- Operations and maintenance personnel

ISA-TR84.00.02-2002 consists of the following parts, under the general title "Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques."

Part 1: Introduction

Part 2: Determining the SIL of a SIF via Simplified Equations

Part 3: Determining the SIL of a SIF via Fault Tree Analysis

Part 4: Determining the SIL of a SIF via Markov Analysis

Part 5: Determining the PFD of Logic Solvers via Markov Analysis

Introduction

ANSI/ISA-84.01-1996 describes a safety lifecycle model for the implementation of risk reduction measures for the process industry (Clause 4). The standard then proceeds to provide specific guidance in the application of SIS, which may be one of the risk reduction methods used. The standard defines three levels of safety integrity (Safety Integrity Levels, SIL) that may be used to specify the capability that a safety instrumented function must achieve to accomplish the required risk reduction. ISA-TR84.00.02-2002 provides methodologies for evaluating SIF to determine if they achieve the specific SIL. This may be referred to as a probability of failure on demand (PFD) evaluation of the SIF.

ISA-TR84.00.02-2002 only addresses SIF operating in demand mode.

The evaluation approaches outlined in this document are performance-based approaches and do not provide specific results that can be used to select a specific architectural configuration for a given SIL.

THE READER IS CAUTIONED TO CLEARLY UNDERSTAND THE ASSUMPTIONS ASSOCIATED WITH THE METHODOLOGY AND EXAMPLES IN THIS DOCUMENT BEFORE DERIVING ANY CONCLUSIONS REGARDING THE EVALUATION OF ANY SPECIFIC SIF.

The evaluation processes described in this document take place before the SIS detailed design phase of the life cycle (see Figure I.1, Safety Lifecycle Model).

This document assumes that a SIS is required. It does not provide guidance in the determination of the need for a SIS. The user is referred to ANSI/ISA-84.01-1996 Annex A for methodologies that might be used in making this determination.

This document involves the evaluation of the whole SIF from the sensors through the logic solver to the final elements. Process industry experience shows that sensors and final elements are major contributors to loss of SIS integrity (high PFD). When evaluating the performance of sensors and final elements, issues such as component technology, installation, and maintenance should be considered.

Frequently multiple safety instrumented functions are included in a single logic solver. The logic solver should be carefully evaluated since a problem in the logic solver may adversely impact the performance of all of the safety instrumented functions (i.e., the logic solver could be the common cause failure that disables all of the SIFs.).

This principle (i.e., common cause) applies to any

- element of a SIS that is common to more than one safety instrumented function; and
- redundant element with one or more safety instrumented function.

Each element should be evaluated with respect to all the safety instrumented functions with which it is associated

- to ensure that it meets the integrity level required for each safety instrumented function;
- to understand the interactions of all the safety instrumented functions; and
- to understand the impact of failure of each component.

This document does not provide guidance in the determination of the specific SIL required (e.g., SIL 1, 2, and 3) for the SIS. The user is again referred to ANSI/ISA-84.01-1996 or to other references.

The primary focus of this document is on evaluation methodologies for assessing the capability of the SIS. The SIS lifecycle model is defined in ANSI/ISA-84.01-1996. Figure I.2 shows the boundaries of the SIS and how it relates to other systems.

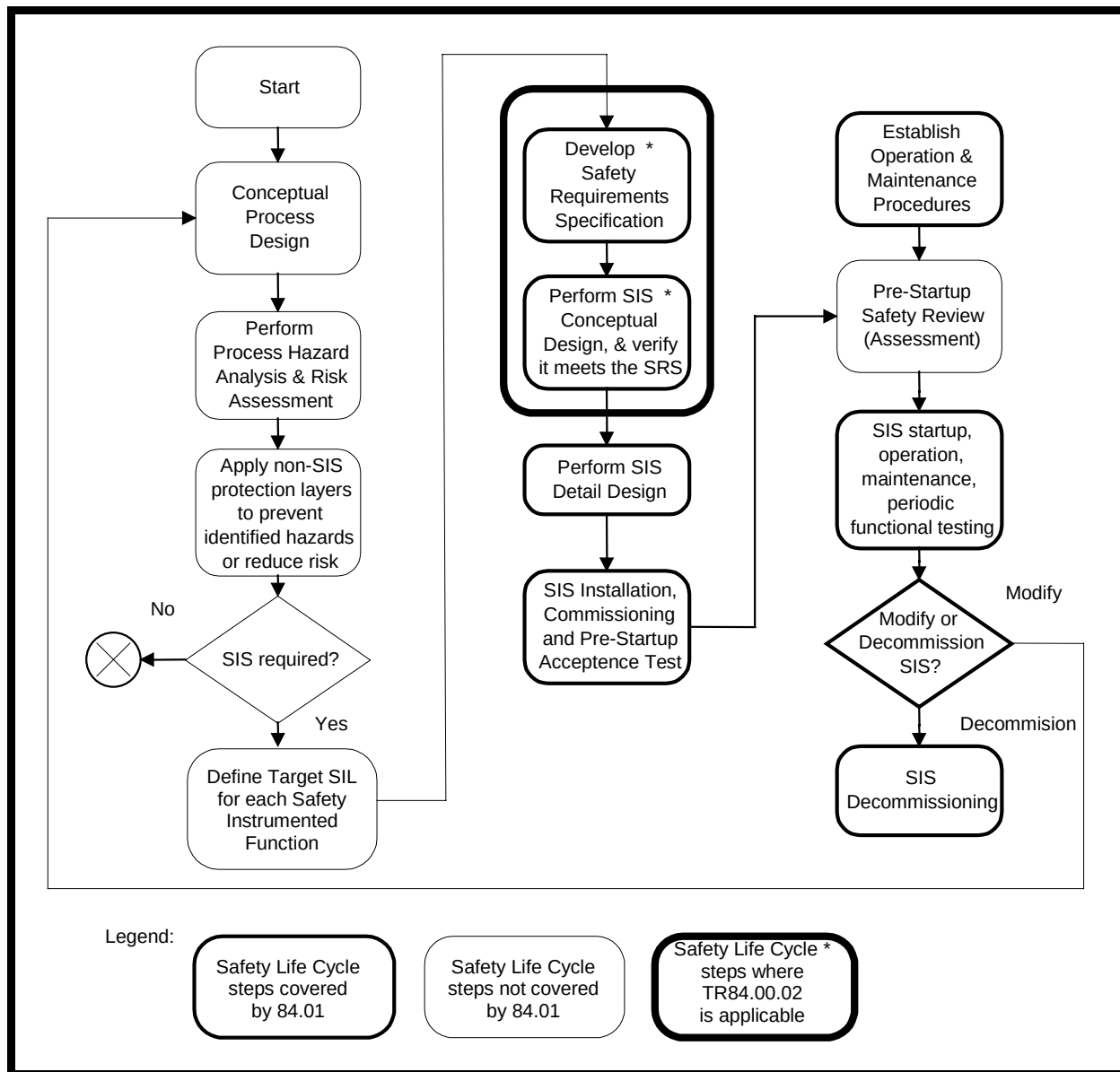


Figure I.1 — Safety lifecycle model

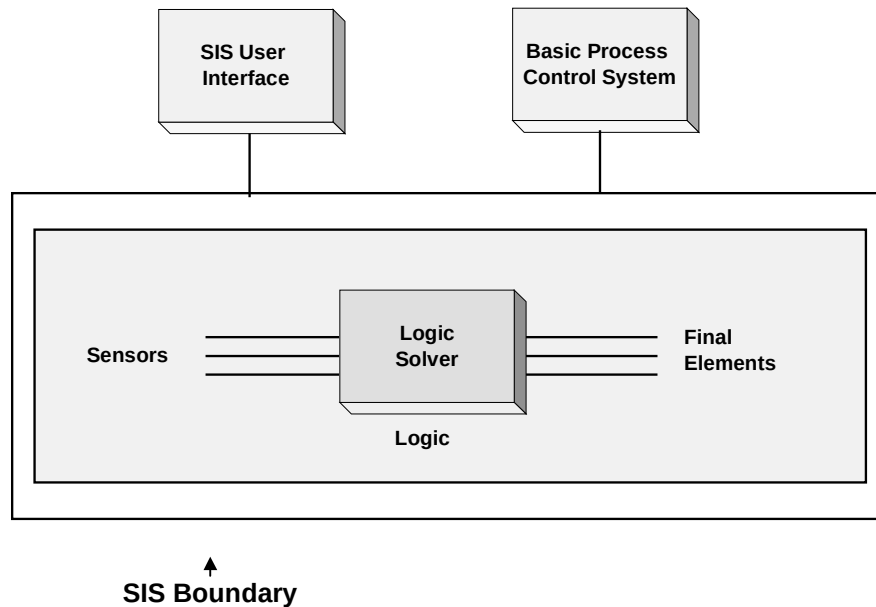


Figure I.2 — Definition of Safety Instrumented System (SIS)

The safety requirements specification addresses the design elements (hardware, software, redundancy, etc.) and the operational attributes (inspection/maintenance policy, frequency and quality of testing, etc.) of the SIS. These elements affect the PFD of each safety instrumented function.

The PFD of these systems can be determined using historical system performance data (e.g., statistical analysis). Where systems, subsystems, components, etc. have not been in use for a sufficiently long time and in large enough numbers to have a statistically significant population available for the evaluation of their performance solely based on actuarial data, a systematic evaluation of the performance of a system may be obtained through the use of PFD analysis techniques.

PFD analysis techniques employ systematic methodologies that decompose a complex system to its basic components. The performance and interactions of these basic components are merged into reliability models (such as simplified equations, fault trees, Markov models) to determine the overall system safety availability.

This document provides users with a number of PFD evaluation techniques that allow a user to determine if a SIF meets the required safety integrity level.

Safety integrity is defined as “The probability of a Safety Instrumented Function satisfactorily performing the required safety functions under all stated conditions within a stated period of time.” Safety integrity consists of two elements: 1) hardware safety integrity and 2) systematic safety integrity. Hardware safety integrity which is based upon random hardware failures can normally be estimated to a reasonable level of accuracy. ANSI/ISA-84.01-1996 addresses the hardware safety integrity by specifying target failure measures for each SIL. For SIF operating in the demand mode the target failure measure is PFD_{avg} (average probability of failure to perform its design function on demand). PFD_{avg} is also commonly referred to as the average probability of failure on demand. Systematic integrity is difficult to quantify due to the diversity of causes of failures; systematic failures may be introduced during the specification, design, implementation, operational and modification phase and may affect hardware as well as software. ANSI/ISA-84.01-1996 addresses systematic safety integrity by specifying procedures, techniques, measures, etc. that reduce systematic failures.

An acceptable safe failure rate is also normally specified for a SIF. The safe failure rate is commonly referred to as the false trip, nuisance trip, or spurious trip rate. The spurious trip rate is included in the evaluation of a SIF, since process start up and shutdown are frequently periods where chances of a hazardous event are high. Hence in many cases, the reduction of spurious trips will increase the safety of the process. The acceptable safe failure rate is typically expressed as the mean time to a spurious trip (**MTTF^{spurious}**).

NOTE In addition to the safety issue(s) associated with spurious trips the user of the SIS may also want the acceptable **MTTF^{spurious}** to be increased to reduce the effect of spurious trips on the productivity of the process under control. This increase in the acceptable **MTTF^{spurious}** can usually be justified because of the high cost associated with a spurious trip.

The objective of this technical report is to provide users with techniques for the evaluation of the hardware safety integrity of SIF (**PFD_{avg}**) and the determination of **MTTF^{spurious}**. Methods of modeling systematic failures are also presented so a quantitative analysis can be performed if the systematic failure rates are known.

ISA-TR84.00.02-2002 shows how to model complete SIF, which includes the sensors, the logic solver and final elements. To the extent possible the system analysis techniques allow these elements to be independently analyzed. This allows the safety system designer to select the proper system configuration to achieve the required safety integrity level.

ISA-TR84.00.02-2002 - Part 1 provides

- a detailed listing of the definition of all terms used in this document. These are consistent with the ANSI/ISA-84.01-1996, IEC 61508 and IEC 61511 standards.
- the background information on how to model all the elements or components of a SIF. It focuses on the hardware components, provides some component failure rate data that are used in the examples calculations and discusses other important parameters such as common cause failures and functional failures.
- a brief introduction to the methodologies that will be used in the examples shown in this document. They are Simplified equations ⁽³⁾, Fault Tree Analysis ⁽⁴⁾, and Markov Analysis ⁽⁵⁾.

ISA-TR84.00.02-2002 - Part 2 provides simplified equations for calculating the SIL values for Demand Mode Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA-84.01-1996, "Applications of Safety Instrumented Systems for the Process Industries." Part 2 should not be interpreted as the only evaluation technique that might be used. It does, however, provide the engineer(s) performing design for a SIS with an overall technique for assessing the capability of the designed SIF.

ISA-TR84.00.02-2002 - Part 3 provides fault tree analysis techniques for calculating the SIL for Demand Mode Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA-84.01-1996, "Applications of Safety Instrumented Systems for the Process Industries." Part 3 should not be interpreted as the only evaluation technique that might be used. It does, however, provide the engineer(s) performing design for a SIS with an overall technique for assessing the capability of the designed SIF.

ISA-TR84.00.02-2002 - Part 4 provides Markov analysis techniques for calculating the SIL values for Demand Mode Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA-84.01-1996, "Applications of Safety Instrumented Systems for the Process Industries." Part 4 should not be interpreted as the only evaluation technique that might be used. It does, however, provide the engineer(s) performing design for a SIS with an overall technique for assessing the capability of the designed SIF.

ISA-TR84.00.02-2002 - Part 5 addresses the logic solver only, using Markov Models for calculating the PFD of E/E/PE logic solvers because it allows the modeling of maintenance and repairs as a function of time, treats time as a model parameter, explicitly allows the treatment of diagnostic coverage, and models the systematic failures (i.e., operator failures, software failures, etc.) and common cause failures.

Figure I.3 illustrates the relationship of each part to all other parts.

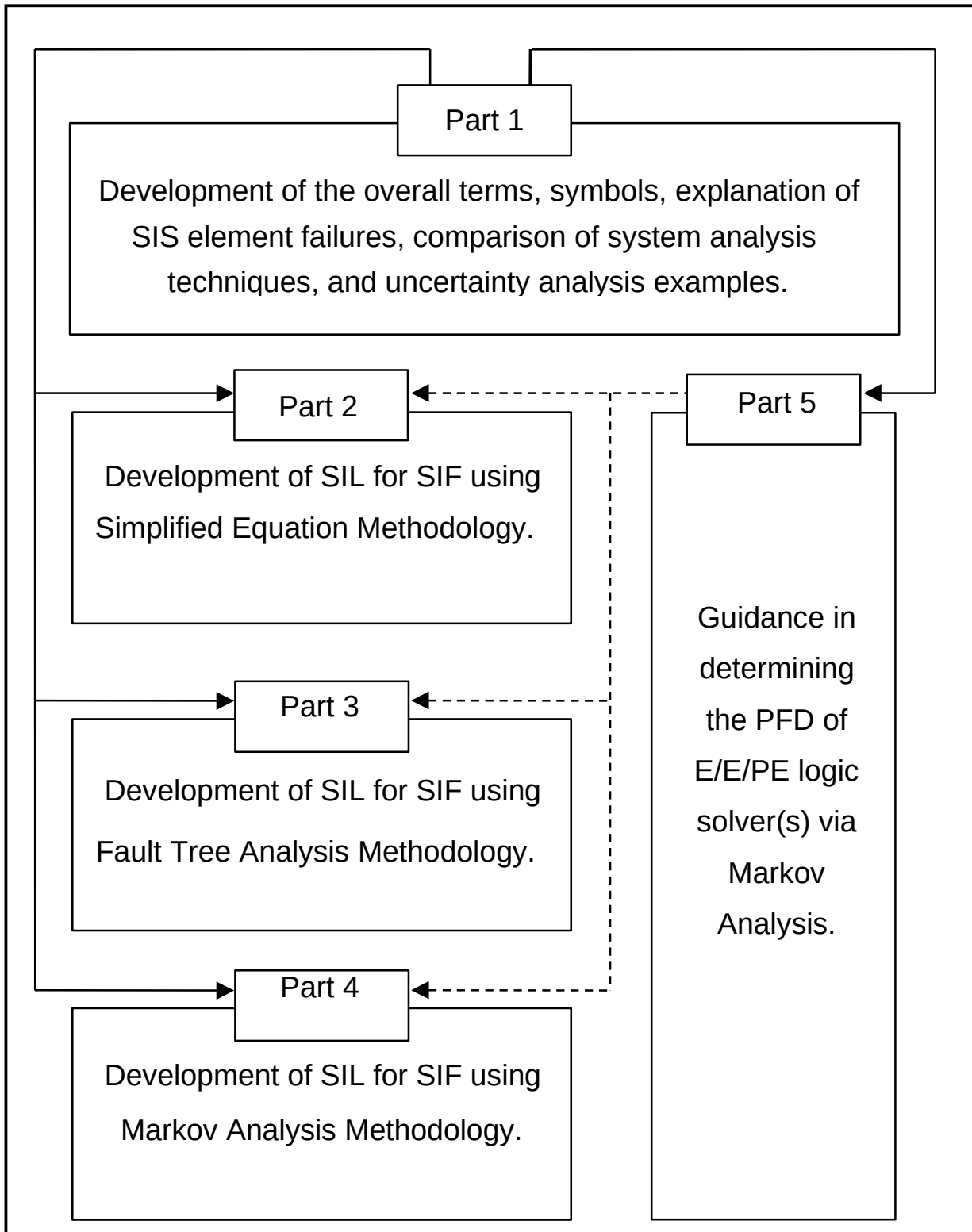


Figure I.3 — ISA-TR84.00.02-2002 Overall Framework

1 Scope

1.1 ISA-TR84.00.02-2002 - Part 1 is informative and does not contain any mandatory clauses. ISA-TR84.00.02-2002 is intended to be used only with a thorough understanding of ANSI/ISA-84.01-1996 (see Figure I.1). Prior to proceeding with use of ISA-TR84.00.02-2002 in a safety application, the Hazards and Risk Analysis must have been completed and the following information provided

- a) It is determined that a SIS is required.
- b) Each safety instrumented function to be carried out by the SIS(s) is defined.
- c) The SIL for each safety instrumented function is defined.

1.2 ISA-TR84.00.02-2002 - Part 1 provides

- a) guidance in Safety Integrity Level analysis;
- b) methods to implement Safety Instrumented Functions (SIF) to achieve a specified SIL;
- c) discussion of failure rates and failure modes (Annex D) of SIS and their components;
- d) discussion of diagnostic coverage, covert faults, common cause, systematic failures, redundancy of SIF;
- e) tool(s) for verification of SIL; and
- f) discussion of the effect of functional test interval.

1.3 The objective of ISA-TR84.00.02-2002 - Part 1 is to introduce the reader to the performance based approach for evaluating the reliability of SIF and to present system reliability methodologies that can be used to evaluate the system performance parameters, namely, the probability that the SIF fails to respond to a demand and the probability that the SIF creates a nuisance trip. ISA-TR84.00.02-2002 - Part 1 serves as an introduction for all other parts.

2 References

1. ANSI/ISA-84.01-1996 "Application of Safety Instrumented Systems for the Process Industries," ISA, Research Triangle Park, NC, 27709, February 1996.
2. ISA-TR84.00.02-2002, "Safety Instrumented Functions (SIF) – Safety Integrity Level Evaluation Techniques, Part 1: Introduction; Part 2: Determining the SIL of a SIF via Simplified Equations; Part 3: Determining the SIL of a SIF via Fault Tree Analysis; Part 4: Determining the SIL of a SIF via Markov Analysis; Part 5: Determining the PFDavg of SIS Logic Solvers via Markov Analysis," Instrumentation, Systems and Automation Society, Technical Report, Research Triangle Park, NC, 27709, 2002.
3. Reliability, Maintainability and Risk (Practical Methods for Engineers), 4th Edition, D.J. Smith, Butterworth-Heinemann, 1993, ISBN 0-7506-0854-4.
4. "Guidelines for Safe Automation of Chemical Processes," Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY 10017, 1993
5. "Evaluating Control Systems Reliability", W. M. Goble, Instrument Society of America, Research Triangle Park, NC, 27709, 1992.

6. "Introduction to Reliability Engineering," E.E. Lewis, John Wiley & Sons, New York, NY 10158, 1987.
7. "Assurance Technologies - Principles and Practices," D.G. Raheja, McGraw and Hill Inc., New York, NY, 1991.
8. "Safeware - System Safety and Computers," N.G. Levenson, Addison-Wesley Publishing Co., Reading, MA, 1995.
9. "Reliability by Design," A.C. Brombacher, John Wiley & Sons, New York, NY 10158, 1992.
10. "Software Reliability Handbook," P. Rook, Elsevier Science Press, New York, NY 10010, 1990.
11. "Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical Process Safety, New York, NY, American Institute of Chemical Engineers, 1989.
12. "The 'Why's' of Grounding Isolated Ground Planes and Power Supplies, ISBN 0-941247-00-7, Licensing Division, Bell Communications Research, Inc., 290 W. Mt. Pleasant Ave., Livingston, NJ 07039-2729, 1989.
13. "Reliability Evaluation of Engineering Systems," R. Billinton, R.N. Allan, Pitman Advanced Publishing Program, Marshfield, MA 02050, 1983.
14. OREDA-92 (Offshore Reliability Data) DNV Industry, 1992, ISBN 82-515-0188-1.
15. Guidelines For Process Equipment Reliability Data With Data Tables, American Institute of Chemical Engineers, Center for Chemical Process Safety, 1989, ISBN 8169-0422-7.
16. IEEE Std 500-1984, Equipment Reliability Data for Nuclear Power Generating Stations, IEEE and John Wiley & Sons, 1974, ISBN 471-80785-0.
17. RAC, Reliability Analysis Centre-1991, NSN7540-01-280-5500.
18. MIL-Handbook-217, Reliability Prediction of Electronic Equipment.
19. Programmable electronic systems in safety-related applications, Part 2: General technical guidelines, Health and Safety Executive, HMSO, ISBN 0 11 883906 3, 1987.
20. Assigning a numerical value to the beta factor common cause evaluation, Humphreys, R. A., Reliability '87.
21. UPM3.1: A pragmatic approach to dependent failures assessment for standard systems, AEA Technology, ISBN 085 356 4337.
22. G. Apostolakis, S. Kaplan, "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants," Technical Report, Pickard, Lowe and Garrick Inc., 1981.
23. G. Apostolakis, J.S. Wu and D. OKrent, "Uncertainties in System Reliability: Probabilistic versus Nonprobabilistic Theories," Reliability Engineering and System Safety, Vol. 30, 1991.
24. M. Evans, N. Hastings and B. Peacock, "Statistical Distributions," 2nd edition, John Wiley & Sons, NY, 1993.
25. G. Fishman, "Concepts and Methods in Discrete Event Simulation," John Wiley & Sons, NY, 1983.

26. P. Stavrianidis, "Reliability and Uncertainty Analysis of Hardware Failures of a Programmable Electronic System," Reliability Engineering and System Safety Journal, Special Issue, 1992.
27. A.L. Sweet, "On the Hazard Rate of Lognormal Distribution," IEEE Transactions on Reliability, Vol. 39, 1990.
28. A.C. Brombacher, Reliability by Design, John Wiley & Sons, New York, NY 10158, 1992.
29. R. Spence, Tolerance Design of Electronic Circuits (Electronic Systems Engineering Series), Addison-Wesley Pub Co, June 1998.
30. R. Spence, R. Singh Soin, Tolerance Design of Electronic Circuits, Harvill Pr, March 1997.
31. Montgomery D.C., Runger G.C., Montgomery D., Applied Statistics and Probability for Engineers, John Wiley and Sons, January 1994.
32. Rouvroye J.L., Robust Design Toolbox Reference Manual, Toolbox version 2.3. Eindhoven University of Technology, 1997.
33. Henley, Ernest J. and Kumamoto, Hiromitsu, Probabilistic Risk Assessment, IEEE Press, New York, New York, 1992.
34. "What Went Wrong? Case Histories of Process Plant Disasters," Trevor A. Kletz, Gulf Publishing Company, Houston, Texas, 1988.
35. "Learning From Disaster: How Organizations Have No Memory," Trevor A. Kletz, Gulf Publishing Company, Houston, Texas, 1993.

3 Definitions of terms and symbols

3.1 Definition of terms

3.1.1 application program:
see "application software."

3.1.2 application software:
see "software."

3.1.3 architecture:
the arrangement of hardware and/or software elements in a system e.g., (1) arrangement of safety instrumented system (SIS) subsystems; (2) internal structure of a SIS subsystem; (3) arrangement of software programs; (4) voting.

3.1.4 availability:
see "safety availability."

3.1.5 Basic Process Control System (BPCS):
a system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1 . 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 the Process Control System.

3.1.6 channel:

a channel is an element or a group of elements that independently perform(s) a function. The elements within a channel could include input/output(I/O) modules, logic system, sensors, and final elements. The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

NOTE A dual channel (i.e., a two channel) configuration is one with two channels that independently perform the same function.

3.1.7 common cause:

3.1.7.1. common cause fault:

a single fault that will cause failure in two or more channels of a multiple channel system. The single source may be either internal or external to the system.

3.1.7.2 common cause failure:

a failure, which is the result of one or more events causing coincident failures of two or more separate channels in a multiple channel system, leading to a system failure.

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."

3.1.10 overt:

see "undetected."

3.1.11 Cumulative Distribution Function (CDF):

the integral, from zero to infinity, of the failure rate distribution and takes values between zero and one.

3.1.12 dangerous failure:

a failure which has the potential to put the safety instrumented function in a hazardous or fail-to-function state.

NOTE Whether or not the potential is realised may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall hazardous or fail-to-function state.

3.1.13 decommissioning:

the permanent removal of a complete SIS from active service.

3.1.14 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.

3.1.15 demand:

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

3.1.16 detected:

in relation to hardware and software, detected by the diagnostic tests, or through normal operation.

NOTE 1 For example, physical inspection and manual tests, or through normal operation.

NOTE 2 These adjectives are used in detected fault and detected failure.

NOTE 3 Synonyms include: revealed and overt.

3.1.17 diagnostic coverage:

the diagnostic coverage of a component or subsystem is the ratio of the detected failure rates to the total failure rates of the component or subsystem as detected by automatic diagnostic tests.

NOTE 1 Diagnostic coverage factor is synonymous with diagnostic coverage.

NOTE 2 The diagnostic coverage is used to compute the detected (λ_D) and undetected failure rates (λ_U) from the total failure rate (λ_T) as follows: $\lambda_D = DC \times \lambda_T$ and $\lambda_U = (1-DC) \times \lambda_T$

NOTE 3 Diagnostic coverage is applied to components or subsystems of a safety instrumented system. For example the diagnostic coverage is typically determined for a sensor, final element, or a logic solver.

NOTE 4 For safety applications the diagnostic coverage is typically applied to the safe and dangerous failures of a component or subsystem. For example the diagnostic coverage for the dangerous failures of a component or subsystem is $DC = \lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rates and λ_{DT} is the total dangerous failure rate.

3.1.18 diverse:

use of different technologies, equipment or design methods to perform a common function with the intent to minimize common cause faults.

3.1.19 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.

3.1.20 Electronic (/E):

see “E/E/PES.”

3.1.21 embedded software:

see “software.”

3.1.22 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.

3.1.23 Equipment Under Control (EUC):

equipment, machinery, operations or plant used for manufacturing, process, transportation, medical or other activities. In IEC 61511, the term “process” is used instead of Equipment Under Control to reflect process sector usage.

3.1.24 fail-to-danger:

the state of a SIF in which the SIF cannot respond to a demand. Fail-to-function is used in this document (see fail-to-function).

3.1.25 fail-to-function:

the state of a SIF during which the SIF cannot respond to a demand.

3.1.26 fail-safe:

the capability to go to a predetermined safe state in the event of a specific malfunction.

3.1.27 failure:

the termination of the ability of a functional unit to perform a required function.

NOTE 1 Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

NOTE 2 Failures are either random or systematic.

3.1.28 failure rate:

the average rate at which a component could be expected to fail.

3.1.29 fault:

an abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

3.1.30 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.

3.1.31 field devices:

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

3.1.32 final element:

the part of a safety instrumented system which implements the physical action necessary to achieve a safe state.

NOTE 1 Examples are valves, switch gear, motors including their auxiliary elements e.g., a solenoid valve and actuator if involved in the safety instrumented function.

NOTE 2 This definition is process sector specific only.

3.1.33 firmware:

special purpose memory units containing embedded software in protected memory required for the operation of programmable electronics.

3.1.34 functional safety:

the ability of a safety instrumented system or other means of risk reduction to carry out the actions necessary to achieve or to maintain a safe state for the process and its associated equipment.

NOTE 1 This term is not used in ANSI/ISA-84.01-1996. It is used in the IEC 61508 and IEC 61511 standards.

NOTE 2 This definition is from IEC 61511 and it deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.35 functional safety assessment:

an investigation, based on evidence, to judge the functional safety achieved by one or more protection layers.

NOTE 1 This term is not used in ANSI/ISA-84.01-1996. It is used in the IEC 61508 and IEC 61511 standards.

NOTE 2 This definition is from IEC 61511 and it deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.36 functional safety audit:

a systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives.

NOTE A functional safety audit may be carried out as part of a functional safety assessment.

3.1.37 functional testing:

periodic activity to verify that the devices associated with the SIS are operating per the Safety Requirements Specification. May also be called the proof testing or full function testing.

3.1.38 hardware configuration:

see “architecture.”

3.1.39 harm:

physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment.

3.1.40 hazard:

potential source of harm.

NOTE The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long term effect on a person's health (for example, release of a toxic substance).

3.1.41 Hazard and Operability Study (HAZOP):

a systematic qualitative technique to identify process hazards and potential operating problems using a series of guide words to study process deviation. A HAZOP is used to examine every part of the process to discover that deviations from the intention of the design can occur and what their causes and consequences may be. This is done systematically by applying suitable guidewords. This is a systematic detailed review technique for both batch or continuous plants which can be applied to new or existing process to identify hazards.

3.1.42 input function:

a function which monitors the process and its associated equipment in order to provide input information for the logic solver

NOTE 1 An input function could be a manual function.

NOTE 2 This definition is process sector specific only.

3.1.43 input/output modules:

3.1.43.1 input module:

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

3.1.43.2 output module:

E/E/PES or subsystem that acts as the interface to external devices and converts output signals into signals that can actuate field devices.

3.1.44 logic function:

a function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions). Logic functions provide the transformation from one or more input functions to one or more output functions.

3.1.45 logic solver:

that portion of either a BPCS or SIS that performs one or more logic function(s).

NOTE 1 In ANSI/ISA-84.01-1996 and IEC 61511 the following logic systems are used:

- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- PE logic systems for programmable electronic systems.

NOTE 2 Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, hydraulic systems, etc. Sensors and final elements are not part of the logic solver.

NOTE 3 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.46 mean time to fail - spurious ($MTTF^{spurious}$):

the mean time to a failure of the SIS which results in a spurious or false trip of the process or equipment under control (EUC).

3.1.47 mean time to repair (MTTR):

the mean time to repair a module or element of the SIS. This mean time is measured from the time the failure occurs to the time the repair is completed and device returned to service (see $MTTR_{OT}$).

3.1.48 off-line:

process, to which the SIS is connected, is shutdown.

3.1.49 on-line:

process, to which the SIS is connected, is operating.

3.1.50 output function:

function which controls the process and its associated equipment according to final actuator information from the logic function.

NOTE This definition is process sector specific only.

3.1.51 overt:

see "detected."

3.1.52 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.

3.1.53 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 PFD_{avg} . PFD equals 1 minus Safety Availability. It is also referred to as safety unavailability or fractional dead time.

3.1.54 Probability to Fail Safe (PFS):

a value that looks at all failures and indicates the probability of those failures that are in a safe mode.

3.1.55 process Industries:

refers to those industries with processes involved in, but not limited to, the production, generation, manufacture, and/or treatment of oil, gas, wood, metals, food, plastics petrochemicals, chemical, steam, electric power, pharmaceuticals and waste material(s). The various process industries together make up the process sector – a term used in IEC standards.

3.1.56 programmable electronics (PE):

electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units.

NOTE 1 This term covers micro-electronic devices based on one or more central processing units (CPUs) together with associated memories, etc. Examples of process sector programmable electronics include:

- smart sensors;
- programmable electronic logic solvers including:
- programmable controllers;
- programmable logic controllers (PLC) (see figure 3.1);
- distributed control system (DCS);
- loop controllers; and
- smart final elements.

NOTE 2 This term differs from the definition in IEC 61508-4 to reflect differences in the process sector.

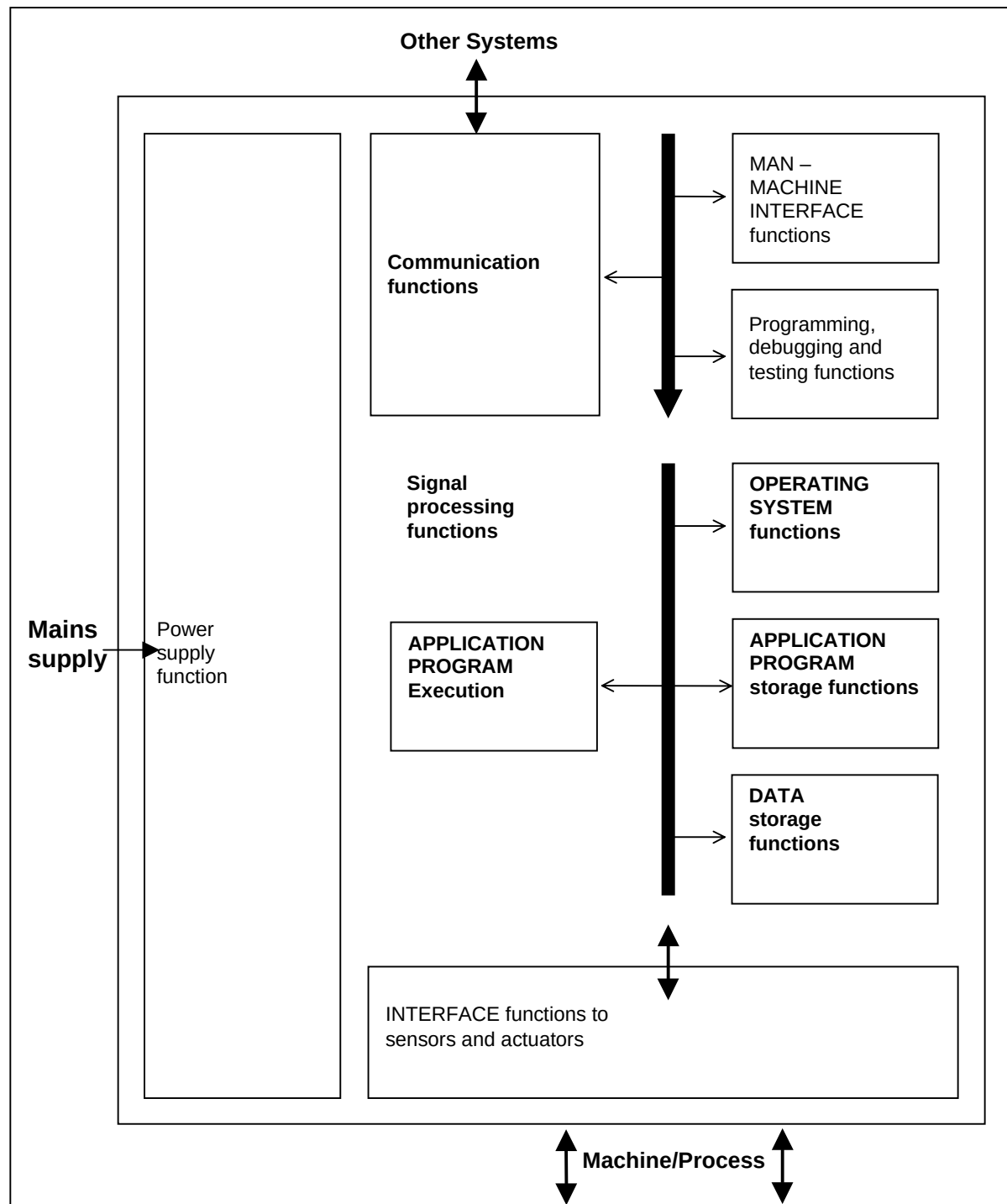


**Figure 3.1 – Structure and function of PLC system
(copied from IEC 61131)**

3.1.57 programmable electronic system (PES):

a system *for control, protection or monitoring* based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices (see Figure 3.2).

NOTE The structure of a PES is shown in Figure 3.2 (A). (B) illustrates the way in which a PES is represented with the programmable electronics shown as a unit distinct from sensors and actuators on the process and their interfaces but the programmable electronics could exist at several places in the PES. (C) illustrates a PES with two discrete units of programmable electronics. (D) illustrates a PES with dual programmable electronics (i.e., two channels) but with a single sensor and a single actuator. (E) illustrates a system based on non-programmable hardware.

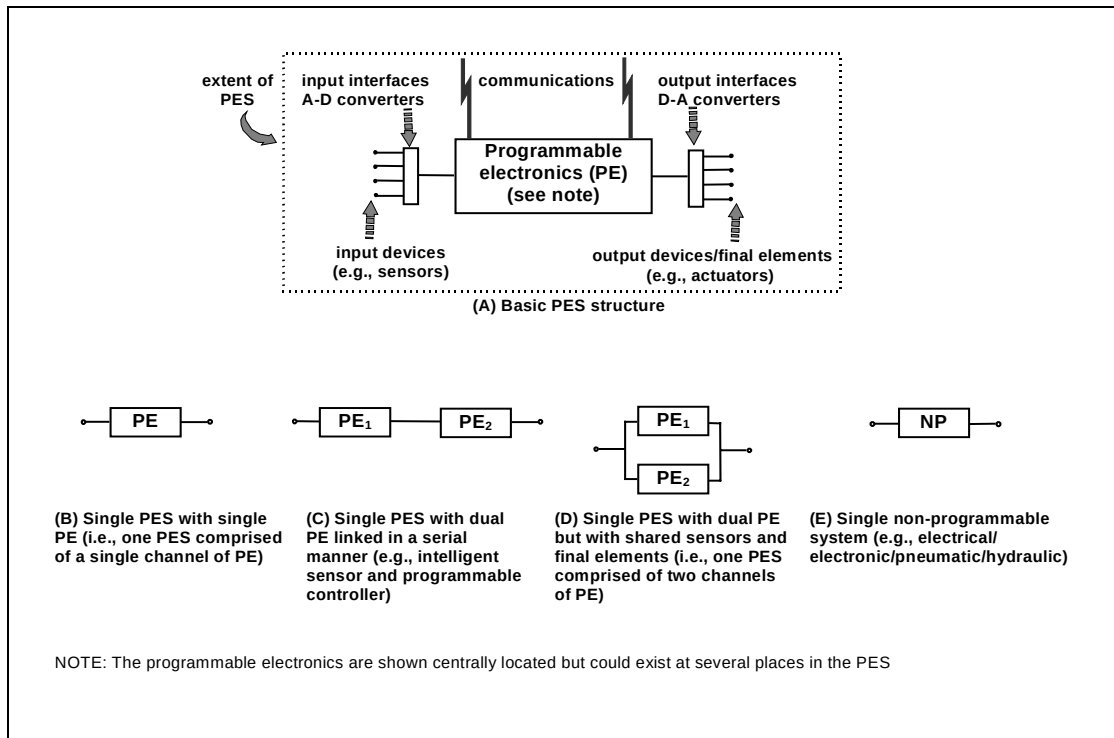


Figure 3.2 – Programmable electronic system (PES): structure and terminology

3.1.58 proof testing:
see “functional testing.”

3.1.59 protection layer:
any independent mechanism that reduces risk by control, prevention or mitigation.

NOTE 1 It could be a process engineering mechanism, such as the size of vessels containing hazardous chemicals; a mechanical engineering mechanism, such as a relief valve; a safety instrumented system; or an administrative procedure, such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

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

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

3.1.62 random hardware failure:

failure occurring at random time, which results from one or more of the possible degradation mechanisms in the hardware.

NOTE 1 There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

NOTE 2 A major distinguishing feature between random hardware failures and systematic failures (see definition below), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

3.1.63 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).

NOTE 1 Examples are the use of duplicate functional components and the addition of parity bits.

NOTE 2 Redundancy is used primarily to improve reliability or availability.

3.1.64 reliability:

probability that a system can perform a defined function under stated conditions for a given period of time.

3.1.65 reliability block diagram:

the reliability block diagram can be thought of as a flow diagram from the input of the system to the output of the system. Each element of the system is a block in the reliability block diagram and, the blocks are placed in relation to the SIS architecture to indicate that a path from the input to the output is broken if one (or more) of the elements fail.

3.1.66 risk:

the combination of the probability of occurrence of harm and the severity of that harm.

3.1.67 risk assessment:

process of making risk estimates and using the results to make decisions.

3.1.68 safe failure:

a failure which does not have the potential to put the safety instrumented function in a dangerous or fail-to-function state.

NOTE Other used names for safe failures are: nuisance failure, spurious failure, false trip failure or fail to safe failure.

3.1.69 safe failure fraction (SFF):

the fraction of the overall failure rate of a device that results in either a safe failure or a detected unsafe failure.

3.1.70 safety:

freedom from unacceptable risk.

3.1.71 safe state:

state of the process when safety is achieved.

NOTE 1 In going from a potentially hazardous condition to the final safe state the process may have to go through a number of intermediate safe-states. For some situations a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.



NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.72 safety availability:

probability that a SIS is able to perform its designated safety service when the process is operating. The average Probability of Failure on Demand (PFD_{avg}) is the preferred term. (PFD equals 1 minus Safety Availability).

3.1.73 safety function:

a function to be implemented by a SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event.

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.74 safety instrumented function (SIF):

an E/E/PE safety function with a specified safety integrity level which is necessary to achieve functional safety.

NOTE This definition is process sector specific only.

3.1.75 safety instrumented system (SIS):

implementation of one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s) (e.g., see Figure 3.3) Other terms commonly used include Emergency Shutdown System (ESD, ESS), Safety Shutdown System (SSD), and Safety Interlock System.

NOTE SIS may or may not include software.

SIS architecture and safety instrumented function example with different devices shown.

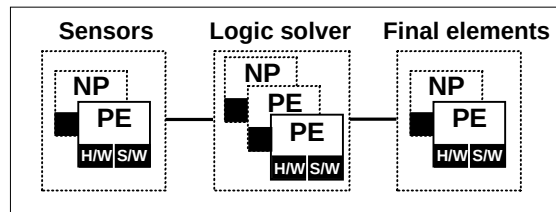


Figure 3.3 – Example SIS architecture

3.1.76 safety integrity:

the probability of a SIF satisfactorily performing the required safety functions under all stated conditions within a stated period of time.

NOTE 1 The higher the level of safety integrity of the safety instrumented function (SIF), the lower the probability that the SIF should fail to carry out the required safety instrumented functions.

NOTE 2 ANSI/ISA-84.01-1996 recognizes three levels of safety integrity for safety instrumented functions. IEC 61508 and IEC 61511 recognize four levels of safety integrity.

NOTE 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included; for example, hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety instrumented function failing to operate on demand.

However, the safety integrity of a SIF also depends on many factors, which cannot be accurately quantified but can only be considered qualitatively.

NOTE Safety integrity comprises hardware safety integrity and systematic safety integrity.

3.1.77 safety integrity level (SIL):

discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

NOTE 1 ANSI/ISA-84.01-1996 recognizes only three Safety Integrity Levels. The above definition is used in this document to provide compatibility with IEC 61508 and IEC 61511.

NOTE 2 The target failure measures for the safety integrity levels are specified in Table 3.1.

NOTE 3 It is possible to use several lower safety integrity level systems to satisfy the need for a higher level function (e.g., using a SIL 2 and a SIL 1 system together to satisfy the need for a SIL 3 function). See IEC 61511-2 for guidance on how to apply this principle.

NOTE 4 This term differs from the definition in IEC 61508-4 to reflect differences in the process sector.

Table 3.1 — Safety integrity level (SIL) target ranges

Safety Integrity Level (SIL)	Target Range Probability of Failure on Demand Average (PFD _{avg})
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}
4	10^{-4} to 10^{-5}

3.1.78 safety lifecycle:

the necessary activities involved in the implementation of safety instrumented function(s), occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.

NOTE The term “functional safety lifecycle “ is strictly more accurate, but the adjective “functional” is not considered necessary in this case within the context of this technical report.

3.1.79 safety requirements specification:

the specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems.

3.1.80 sensor:

a device or combination of devices, which measure the process condition (e.g., transmitters, transducers, process switches, position switches, etc.).

NOTE This definition is process sector specific only.

3.1.81 separation:

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

3.1.82 SIS components:

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

3.1.83 software:

an intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system.

NOTE Software is independent of the medium on which it is recorded.

3.1.84 software languages in SIS subsystems:

3.1.84.1 fixed program language (FPL):

this type of language is represented by the many proprietary, dedicated-function systems which are available as standard process industry products.

The functional specification of the FPL should be documented either in the suppliers' data sheets, user manual or the like.

The user should be unable to alter the function of the product, but limited to adjust a few parameters (e.g., range of the pressure transmitter).

NOTE Typical example of systems with FPL: smart sensor (e.g., pressure transmitter), sequence of events controller, dedicated smart alarm box, small data logging systems.

3.1.84.2 limited variability language (LVL):

this type of language is a more flexible language which provides the user with some capability for adjusting it to his own specific requirements. The safety instrumented functions are configured by the use of an application-related language and the specialist skills of a computer programmer are not required.

The documentation of the LVL should consist of a comprehensive specification which defines the basic functional components and the method of configuring them into an application program. In addition an engineering tool and a library of application specific functions should be given together with a user manual.

The user should be able to configure/program the required application functions according to the functional requirement specification.

NOTE 1 Typical examples of LVL are ladder logic, function block diagram and sequential function chart.

NOTE 2 Typical example of a system using LVL is a standard programmable logic controller (PLC) performing burner management.

3.1.84.3 full variability language (FVL):

this type of language is general-purpose computer-based, equipped with an operating system which usually provides system resource allocation and a real-time multi-programming environment. The language is tailored for a specific application by computer specialists, using high level languages.

The FVL application will often be unique for a specific application. As a result most of the specification will be special-to-project.

NOTE 1 Typical example of a system using FVL is a personal computer which performs supervisory control or process modeling.

NOTE 2 In the process sector FVL is found in embedded software and rarely in application software.

NOTE 3 FVL examples include: ADA, C, Pascal.

NOTE 4 This definition is process sector specific only.

3.1.85 software program types:

3.1.85.1 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. In general, it contains logic sequences, permissives, limits, expressions, etc., that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. See fixed and limited variability software language.

3.1.85.2 system software:

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

3.1.85.3 utility software:

software tools for the creation, modification, and documentation of application programs. These software tools are not required for the operation of the SIS.

NOTE This definition is process sector specific only.

3.1.86 software lifecycle:

the activities occurring during a period of time that starts when software is conceived and ends when the software is permanently disused.

NOTE 1 A software lifecycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

NOTE 2 Software cannot be maintained; rather, it is modified.

3.1.87 spurious trip:

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

3.1.88 Spurious Trip Rate (STR):

the expected rate (number of trips per unit time) at which a trip of the SIF can occur for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, electrical fault, transient, ground plane interference⁽¹²⁾, etc.). Other terms used include nuisance trip rate and false shutdown rate.

3.1.89 systematic failure:

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

NOTE 1 Corrective maintenance without modification should usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

NOTE 3 Example causes of systematic failures include human error in:

- the safety requirements specification;
- the design, manufacture, installation and operation of the hardware;
- the design, implementation, etc. of the software.

3.1.90 Test Interval (TI):

time between functional tests. Test interval is the amount of time that lapses between functional tests performed on the SIS or a component of the SIS to validate its operation.

3.1.91 undetected:

in relation to hardware and software, not found by the diagnostic tests or during normal operation.

NOTE 1 For example, physical inspection and manual tests, or through normal operation.

NOTE 2 These adjectives are used in undetected fault and undetected failure.

NOTE 3 Synonyms include: unrevealed and covert.

NOTE 4 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.1.92 utility software:

see “software.”

3.1.93 verification:

process of confirming for certain steps of the Safety Life Cycle that the objectives are met.

3.1.94 voting system:

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

3.1.95 watchdog:

a combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic (PE) device and taking action upon detection of an incorrect operation.

NOTE 1 The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (e.g., hardware electronic watchdog timer) by an output device controlled by the software.

NOTE 2 The watchdog can be used to de-energize a group of safety outputs when dangerous failures are detected in order to put the process into a safe state. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver.

NOTE 3 This definition is process sector specific only.

3.2 Definition of symbols

NOTE Symbols specific to the analysis of the logic solver portion are included in ISA-TR84.00.02-2002 - Part 5.

β is the fraction of single module or circuit failures that result in the failure of an additional module or circuit. Hence two modules or circuits performing the same function fail. This parameter is used to model common cause failures that are related to hardware failures.

β_D is the fraction of a single module or circuit failures that result in the failure of an additional module or circuit taking diagnostic coverage into account.