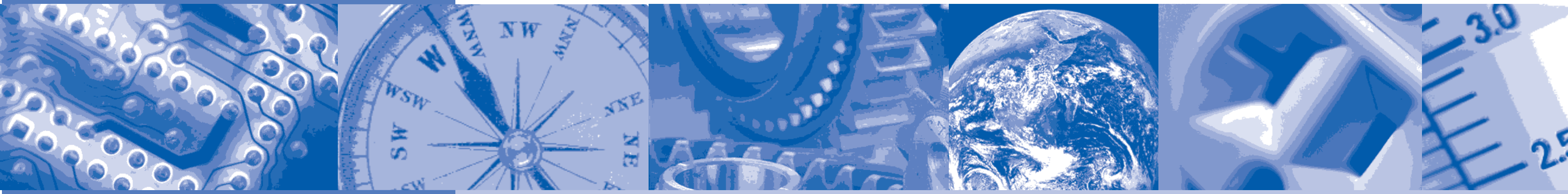
TECHNICAL REPORT

ISA-TR84.00.02-2002 - Part 2



Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations

Approved 17 June 2002

ISA–The Instrumentation,
Systems, and
Automation Society

ISA-TR84.00.02-2002 – Part 2
Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques Part 2:
Determining the SIL of a SIF via Simplified Equations

ISBN: 1-55617-803-4

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 2.

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	Cytec Industries Inc.
K. Schilowsky	Marathon Ashland Petroleum Company LLC
D. Sniezek	Lockheed Martin Federal Services
C. Sossman	WG-W Safety Management Solutions
R. Spiker	Yokogawa Industrial Safety Systems BV
P. Stavrianidis*	Factory Mutual Research Corporation
H. Storey	Equilon Enterprises LLC
A. Summers	SIS-TECH Solutions LLC
L. Suttinger	Westinghouse Savannah River Company
R. Szanyi	ExxonMobil Research Engineering
R. Taubert	BASF Corporation
H. Tausch	Honeywell Inc.
T. Walczak	GE FANUC Automation
M. Weber	System Safety Inc.
D. Zetterberg	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	Emerson Process Management
D. Bishop	David N Bishop, Consultant
D. Bouchard	Paprican
M. Cohen	Consultant
M. Coppler	Ametek, Inc.
B. Dumortier	Schneider Electric
W. Holland	Southern Company
E. Icayan	ACES Inc
A. Iverson	Ivy Optiks
R. Jones	Dow Chemical Company
V. Maggioli	Feltronics Corporation
T. McAvinew	ForeRunner Corporation
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Westinghouse Process Control Inc.
R. Reimer	Rockwell Automation
J. Rennie	Factory Mutual Research Corporation
H. Sasajima	Yamatake Corporation
I. Verhappen	Syncrude Canada Ltd.
R. Webb	POWER Engineers
W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	KEMA Consulting
M. Widmeyer	Stanford Linear Accelerator Center
C. Williams	Eastman Kodak Company
G. Wood	Graeme Wood Consulting

This page intentionally left blank.

Contents

This page intentionally left blank.

Safety Instrumented Functions (SIF)

— Safety Integrity Level (SIL) Evaluation Techniques

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

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 I, 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.

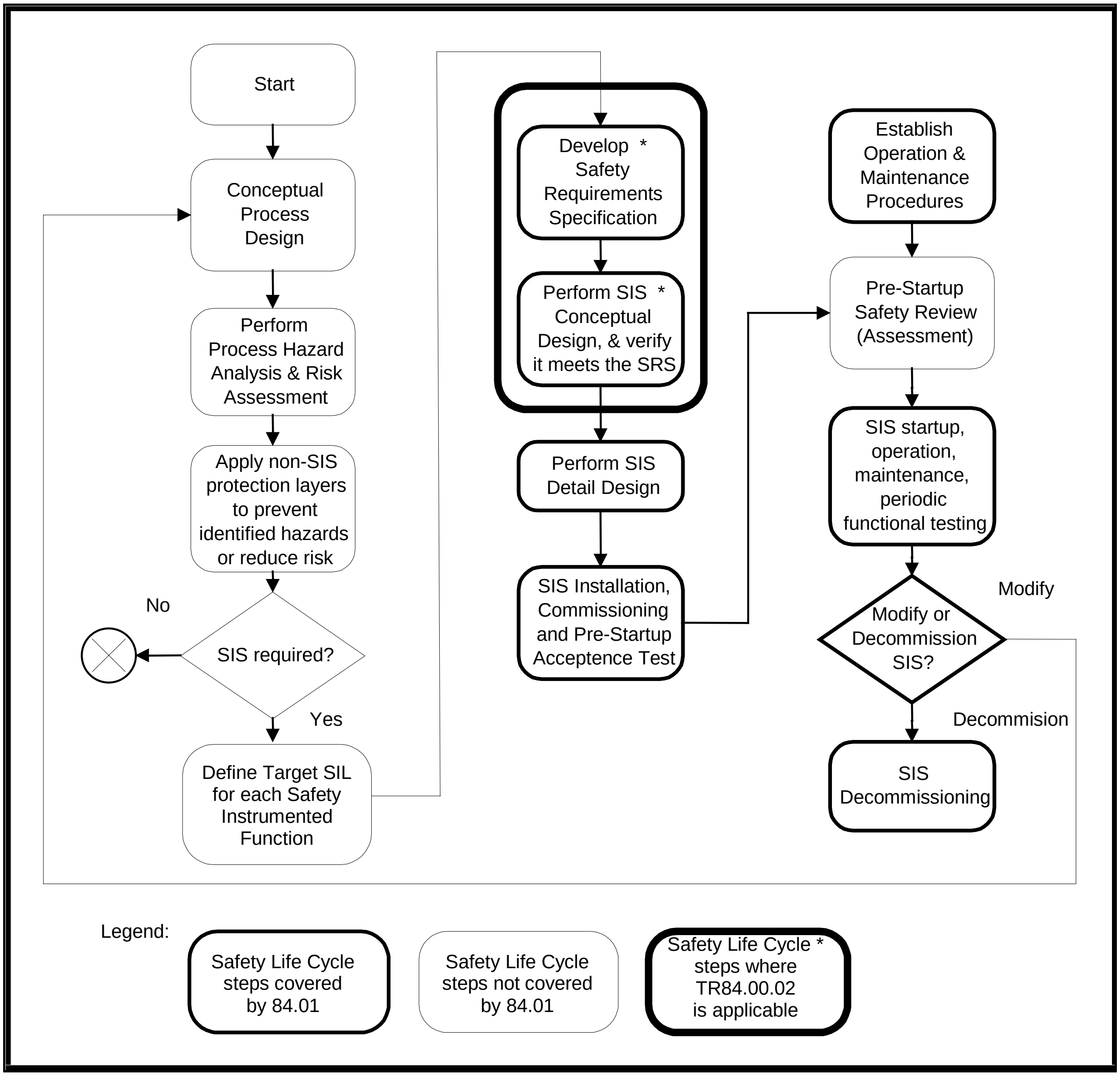

Start
Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
SIS required?
No
Yes
Define Target SIL for each Safety Instrumented Function
Develop * Safety Requirements Specification
Perform SIS * Conceptual Design, & verify it meets the SRS
Perform SIS Detail Design
SIS Installation, Commissioning and Pre-Startup Acceptance Test
Establish Operation & Maintenance Procedures
Pre-Startup Safety Review (Assessment)
SIS startup, operation, maintenance, periodic functional testing
Modify or Decommission SIS?
Modify
Decommision
SIS Decommissioning
Legend:
Safety Life Cycle steps covered by 84.01
Safety Life Cycle steps not covered by 84.01
Safety Life Cycle * steps where TR84.00.02 is applicable

Figure I.1 — Safety Lifecycle Model

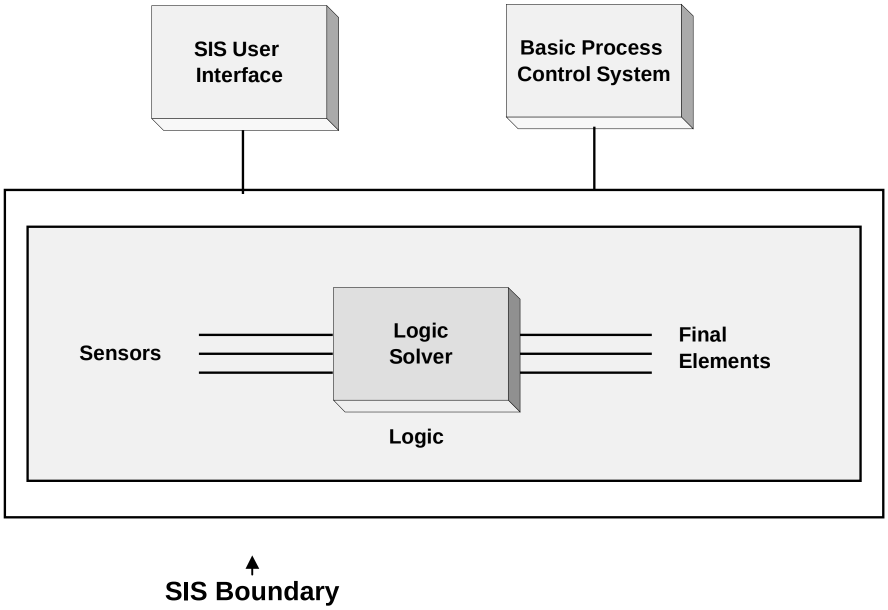


Figure I.2 — Definition of Safety Instrumented System (SIS)

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 **$\mathbf{PFD_{avg}}$** (average probability of failure to perform its design function on demand). **$\mathbf{PFD_{avg}}$** 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 ($\mathbf{MTTF^{spurious}}$).

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 ($\mathbf{PFD_{avg}}$) and the determination of $\mathbf{MTTF^{spurious}}$. 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.

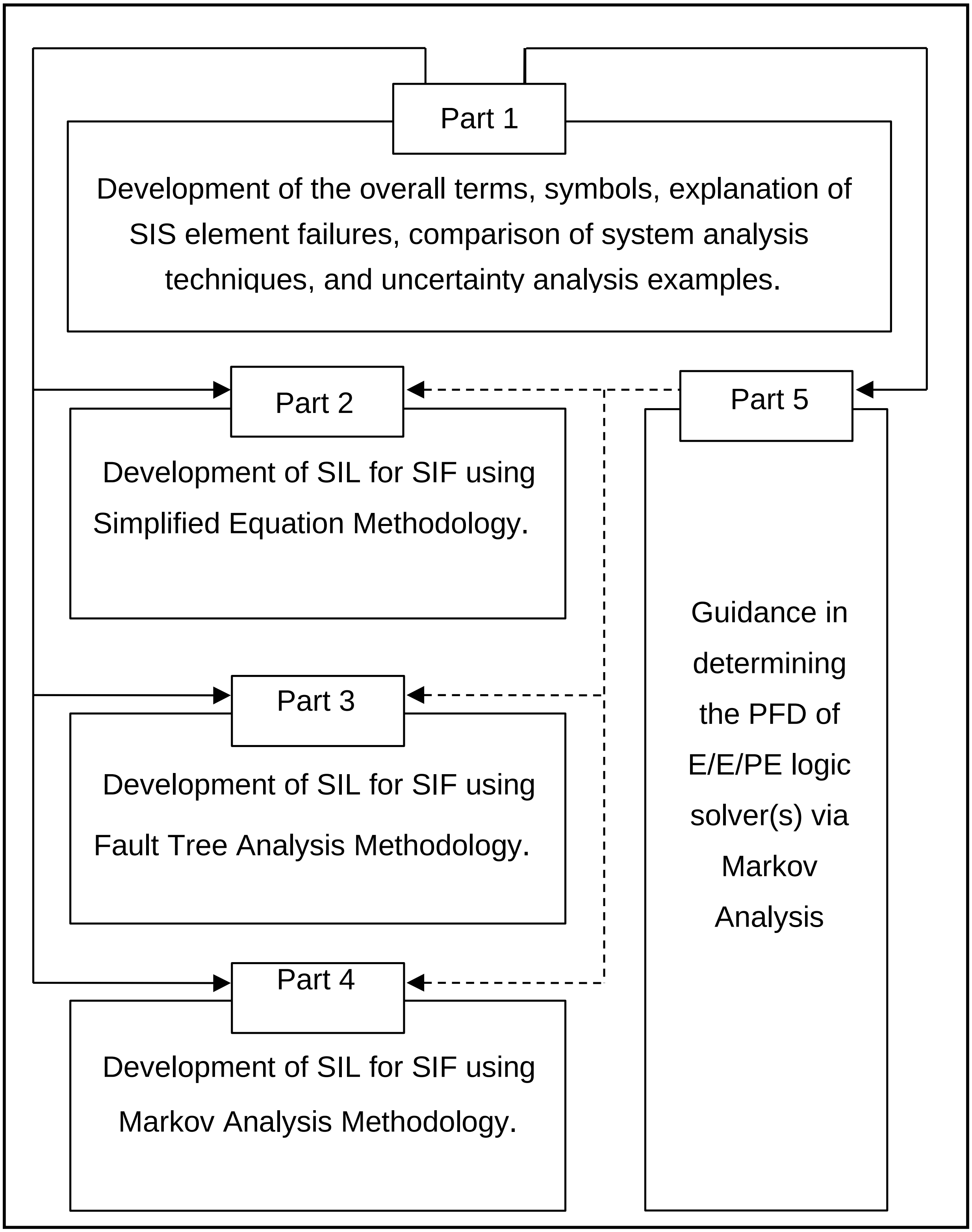

Part 1
Development of the overall terms, symbols, explanation of SIS element failures, comparison of system analysis techniques, and uncertainty analysis examples.
Part 2
Development of SIL for SIF using Simplified Equation Methodology.
Part 3
Development of SIL for SIF using Fault Tree Analysis Methodology.
Part 4
Development of SIL for SIF using Markov Analysis Methodology.
Part 5
Guidance in determining the PFD of E/E/PE logic solver(s) via Markov Analysis

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

1 Scope

1.1 ISA-TR84.00.02-2002 - Part 2 is informative and does not contain any mandatory requirements. This part of the technical report is intended to be used only after a thorough understanding of ISA-TR84.00.02-2002 – Part 1, which defines the overall scope. ISA-TR84.00.02-2002 - Part 2 provides:

a) technical guidance in Safety Integrity Level (SIL) Analysis;

b) ways to implement Safety Instrumented Functions (SIF) to achieve a specified SIL;

c) failure rates and failure modes of SIF components;

d) diagnostics, diagnostic coverage, covert faults, test intervals, redundancy of SIF components;

e) tool(s) for SIL verification of SIF.

1.2 ISA-TR84.00.02-2002 - Part 2 provides one possible technique for calculating PFD_{avg} values for Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA-84.01-1996, “Application of Safety Instrumented Systems for the Process Industries”.

1.3 ISA-TR84.00.02-2002 - Part 2 provides the engineer(s) performing design for a SIF with a relatively simple technique generally following the simplified equation approach for assessing the capability of the designed SIF.

1.4 The procedures outlined in ISA-TR84.00.02-2002 - Part 2 provide the engineer with steps to follow in estimating a mathematical value for PFD_{avg} for typical configurations of SIF designed according to ANSI/ISA-84.01-1996. This procedure is appropriate for SIL 1 and SIL 2 SIFs. This procedure should not be used for SIL 3 SIFs unless the User has a thorough understanding of the SIL Verification mathematics and fully understands the limitations of the simplified equations.

1.5 ISA-TR84.00.02-2002 - Part 2 does not cover modeling of external communications or operator interfaces. The SIL analysis includes the SIF envelope as defined by ANSI/ISA-84.01-1996 (see Figure I.2).

2 References

1. ANSI/ISA-84.01-1996 “Application of Safety Instrumented Systems for the Process Industries”, Instrumentation, Systems, and Automation Society, 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 PFD 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” by David J. Smith, 4th Edition, 1993, Butterworth-Heinemann, ISBN 82-515-0188-1.

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. “Probabilistic Risk Assessment, Henley, Ernest J. and Kumamoto, Kiromitsu, IEEE Press, New York, New York, 1992.

3 Definitions

Definitions and terminology used in this part are defined in ISA-TR84.00.02-2002 – Part 1.

4 Assumptions used in the calculations

The following assumptions were used in this Part for Simplified Equation calculations:

4.1 The SIF being evaluated will be designed, installed, and maintained in accordance with ANSI/ISA-84.01-1996.

4.2 Component failure and repair rates are assumed to be constant over the life of the SIF.

4.3 Once a component has failed in one of the possible failure modes it cannot fail again in one of the remaining failure modes. It can only fail again after it has first been repaired. This assumption has been made to simplify the modeling effort.

4.4 The equations assume similar failure rates for redundant components.

4.5 The sensor failure rate includes everything from the sensor to the input module of the logic solver including the process effects (e.g., plugged impulse line to transmitter).

4.6 The logic solver failure rate includes the input modules, logic solver, output modules and power supplies. These failure rates typically are supplied by the logic solver vendor.

NOTE ISA-TR84.00.02-2002 - Part 5 illustrates a suggested method to use in developing failure rate data for the logic solver.

4.7 The final element failure rate includes everything from the output module of the logic solver to the final element including the process effects.

4.8 The failure rates shown in the formulas for redundant architectures are for a single ‘leg’ or ‘slice’ of a system (e.g., if 2oo3 transmitters, the failure rate used is for a single transmitter, not three (3) times the single transmitter value.)

4.9 The Test Interval (TI) is assumed to be much shorter than the Mean Time To Failure (MTTF).

4.10 Testing and repair of components in the system are assumed to be perfect.

4.11 All SIF components have been properly specified based on the process application. For example, final elements (valves) have been selected to fail in the safe direction depending on their specific application.

4.12 All equations used in the calculations based on this part are based on Reference 3.

4.13 All power supply failures are assumed to be to the de-energized state.

4.14 It is assumed that when a dangerous detected failure occurs, the SIS will take the process to a safe state or plant personnel will take necessary action to ensure the process is safe (operator response is assumed to be before a demand occurs, i.e., instantaneous, and PFD of operator response is assumed to be 0).

NOTE If the action depends on plant personnel to provide safety, the user is cautioned to account for the probability of failure of personnel to perform the required function in a timely manner.

4.15 The target PFD_{avg} and $MTTF^{spurious}$ is defined for each SIF implemented in the SIS.

4.16 The Beta model is used to treat possible common cause failures.

NOTE A detailed explanation of the Beta model is given in Annex A of Part 1.

4.17 The equations developed in this part assume a graceful degradation path, i.e., 2oo4 system is assumed to degrade as 4-3-2-0.

4.18 ISA-TR84.00.02-2002 - Part 2 assumes that the User is familiar with the SIF verification techniques and has a general understanding of the principles behind data collection, failure modes, and effects and analysis, and common cause and diagnostic coverage assessment.

5 Calculation procedures

Evaluation of a SIS or a portion of a SIS involves estimating both the PFD_{avg} and the anticipated mean time to spurious trip or Mean Time to Failure - Spurious ($MTTF^{spurious}$) of a single SIF. Both factors may be important in the final system selection and design. The following steps are carried out in this evaluation:

Step No.

1. Identify the hazardous event for which the SIS is providing a layer of protection and the specific individual components that protect against the event.

2. Identify the Safety Integrity Level (SIL) of each SIF required for each hazardous event.

3. List the components that have an impact on each SIF. This will typically be those sensors and final elements identified in the process hazard analysis (PHA) process. The associated SIFs are assigned a SIL by the PHA team.

4. Using the SIS architecture being considered, calculate the PFD_{avg} for each SIF by combining the contributions from the sensors, logic solver, final elements, power supply, and any other components that impact that SIF.

5. Determine if the PFD_{avg} meets the Safety Requirements Specification for each SIF.

6. If required, modify SIS (hardware configuration, test interval, hardware selection, etc.) and re-calculate to meet the requirements specified in the Safety Requirements Specifications (See ANSI/ISA-84.01-1996, Clause 5 and Clause 6.2.2) for each SIF.

7. If SIS reliability impacts the consequence of concern, determine the expected Spurious Trip Rate (STR) for system components and combine to obtain $MTTF^{spurious}$ for the SIS.

8. If the calculated $MTTF^{spurious}$ is unacceptable, modify configuration (add redundancy, use components with better reliability, etc.) and re-calculate to meet requirements in the Safety Requirements Specifications. This will require re-calculation of the PFD_{avg} value for each SIF as well.

9. When the PFD_{avg} and $MTTF^{spurious}$ values meet or exceed those specified in the Safety Requirements Specifications, the calculation procedure is complete.

5.1 PFD_{avg} calculations

The PFD_{avg} is determined by calculating the PFD for all the components in each SIF which provide protection against a process hazardous event and combining these individual values to obtain the SIF PFD value. This is expressed by the following:

(Eq. No. 1) $$\mathrm{PFD}_{\mathrm{SIS}} = \sum \mathrm{PFD}_{\mathrm{Si}} + \sum \mathrm{PFD}_{\mathrm{Ai}} + \sum \mathrm{PFD}_{\mathrm{Li}} + \sum PFD_{PSi}$$

where,

PFD_A is the final element PFD_{avg} for a specific SIF,

PFD_S is the sensor PFD_{avg} for a specific SIF,

PFD_L is the logic solver PFD_{avg},

PFD_{PS} is the power supply PFD_{avg}, and

PFD_{SIS} is the PFD_{avg} for the specific SIF in the SIS.

i represents the number of each type of components that is a part of the specific SIF

Each element of the calculation is discussed in the following sections.

5.1.1 Determining the PFD_{avg} for sensors

The procedure for determining the PFD_{avg} for sensors is as follows:

1. Identify each sensor that detects the out of limits condition that could lead to the event the SIF is protecting against. Only those sensors that prevent or mitigate the designated event are included in PFD calculations**.**

2. List the $MTTF^{DU}$ for each sensor.

3. Calculate the PFD for each sensor configuration using the $MTTF^{DU}$ and the equations in 5.1.5 with appropriate consideration for redundancy.

4. Sum the PFD values for the sensors to obtain the PFD_S component for the SIF being evaluated. This step is only required if multiple sensor inputs are required in the SIF being evaluated.

Combined sensor PFD_{avg} component for SIF:

$PFD_S = \sum PFD_{Si}$ (values for individual sets of sensors)

5.1.2 Determining the PFD_{avg} for Final Elements

The procedure for determining the PFD_{avg} for final elements is as follows:

1. Identify each final element that protects against the out of limits condition that could lead to the event the SIS is protecting against. Only those final elements that prevent or mitigate the designated event are included in PFD calculations.

2. List the MTTF^{DU} for each final element.

3. Calculate the PFD_{avg} for each final element configuration using the MTTF^{DU} and the equations in 5.1.5 with appropriate consideration for redundancy. (*See Figures 5.1 through 5.5 for configuration details.)*

4. Sum the PFD values for the final elements to obtain the PFD_A component for the SIF being evaluated. This step is only required if multiple final elements are required in the SIF being evaluated.

Combined final element PFD_{avg} component for SIF:

$$PFD_A = \sum PFD_{Ai} \text{ (values for individual sets of final elements)}$$

5.1.3 Determining the PFD for the logic solver

NOTE A common logic solver may provide the logic for several SIFs.

The procedure for determining the PFD_{avg} for the logic solver is as follows:

1. Identify the type of logic solver hardware used.

2. Select the MTTF^{DU} for the logic solver (typically obtained from logic solver manufacturer).

NOTE Since the PFD_{avg} for the logic solver is a non-linear function, the user should request the MTTF^{DU} for a number of functional test intervals of interest and use the one that matches the system requirements.

3. Calculate the PFD_{avg} for the logic solver portion of SIF using equations in 5.1.5 with appropriate consideration for redundancy. (Note that this step is only required when the manufacturer does not supply the PFD_{avg} for the fully integrated logic solver system.)

4. If the user must determine the PFD for a PES logic solver, refer to Part 5 of ISA-TR84.00.02-2002 for an approach that can be used.

5.1.4 Determining PFD_{avg} for power supply

If the SIS is designed for de-energize to trip, the power supply does not impact the SIF PFD_{avg} because a power supply failure will result in action taking the process to a safe state. If the SIS is energize to trip, the power supply PFD_{avg} is determined by the following:

1. List the MTTF^{DU} for each power supply to the SIS.

2. Calculate the PFD_{avg} for the power supplies using the appropriate redundancy and the equations in 5.1.5.

5.1.5 System equations

The following equations cover the typical configurations used in SIS configurations. To see the derivation of the equations listed, refer to Reference 3 or ISA-TR84.0.02 - Part 5.

Converting MTTF to failure rate, λ:

(Eq. No. 2) $$\lambda^{DU} = \frac{1}{MTTF^{DU}}$$

Equations for typical configurations:

(Eq. No. 3) 1oo1

$$\mathrm{PFD_{avg}} = \left[\lambda^{DU} \times \frac{\mathrm{TI}}{2}\right] + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

where $\lambda^{\mathbf{DU}}$ is the undetected dangerous failure rate

λ_F^D is the dangerous systematic failure rate, and

TI is the time interval between manual functional tests of the component.

NOTE The equations in ISA-TR84.00.02-2002 - Part 1 model the systematic failure as an error that occurred during the specification, design, implementation, commissioning, or maintenance that resulted in the SIF component being susceptible to a random failure. Some systematic failures do not manifest themselves randomly, but exist at time 0 and remain failed throughout the mission time of the SIF. For example, if the valve actuator is specified improperly, leading to the inability to close the valve under the process pressure that occurs during the hazardous event, then the average value as shown in the above equation is not applicable. In this event, the systematic failure would be modeled using $\lambda \times TI$. When modeling systematic failures, the reader must determine which model is more appropriate for the type of failure being assessed.

1oo2

(Eq. No. 4A)

$$\mathrm{PFD_{avg}} = \left[\left((1-\beta)\times\lambda^{DU}\right)^2 \times \frac{TI^2}{3}\right] + \left[(1-\beta)\times\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

For simplification, 1-β is generally assumed to be one, which yields conservative results. Consequently, the equation reduces to

(Eq. No. 4B)

$$\mathrm{PFD_{avg}} = \left[\left(\lambda^{DU}\right)^2 \times \frac{TI^2}{3}\right] + \left[\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

where MTTR is the mean time to repair

λ^{DD} is dangerous detected failure rate, and

β is fraction of failures that impact more than one channel of a redundant system (common cause).

The second term represents multiple failures during repair. This factor is typically negligible for short repair times (typically less than 8 hours). The third term is the common cause term. The fourth term is the systematic error term.

1oo3

(Eq. No. 5)

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^{3} \times \frac{TI^{3}}{4}\right] + \left[\left(\lambda^{DU}\right)^{2} \times \lambda^{DD} \times MTTR \times TI^{2}\right] + \left[\beta \times \left(\lambda^{DU} \times \frac{TI}{2}\right)\right] + \left[\lambda_{F}^{D} \times \frac{TI}{2}\right]$$

The second term accounts for multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term and the fourth term is the systematic error term.

<u>2oo2</u>

(Eq. No. 6)

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU} \times TI\right] + \left[\beta \times \lambda^{DU} \times TI\right] + \left[\lambda_{F}^{D} \times \frac{TI}{2}\right]$$

The second term is the common cause term and the third term is the systematic error term.

<u>2oo3</u>

(Eq. No. 7)

$$\mathrm{PFD}_{\mathrm{avg}} = \left[(\lambda^{DU})^{2} \times (TI)^{2}\right] + \left[3\lambda^{DU} \times \lambda^{DD} \times MTTR \times TI\right] + \left[\beta \times \lambda^{DU} \times \frac{TI}{2}\right] + \left[\lambda_{F}^{D} \times \frac{TI}{2}\right]$$

The second term in the equation represents multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term. The fourth term is the systematic error term.

<u>2oo4</u>

(Eq. No. 8)

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^{3} \times (TI)^{3}\right] + \left[4\left(\lambda^{DU}\right)^{2} \times \lambda^{DD} \times MTTR \times (TI)^{2}\right] + \left[\beta \times \lambda^{DU} \times \frac{TI}{2}\right] + \left[\lambda_{F}^{D} \times \frac{TI}{2}\right]$$

The second term in the equation represents multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term. The fourth term is the systematic error term.

For configurations other than those indicated above, see Reference 3 or ISA-TR84.00.02-2002 - Part 5.

The terms in the equations representing common cause (Beta factor term) and systematic failures are typically not included in calculations performed in the process industries. These factors are usually accounted for during the design by using components based on plant experience.

Common cause includes environmental factors, e.g., temperature, humidity, vibration, external events such as lightning strikes, etc. Systematic failures include calibration errors, design errors, programming errors, etc. If there is concern related to these factors, refer to ISA-TR84.00.02-2002 - Part 1 for a discussion of their impact on the $\mathrm{PFD}_{\mathrm{avg}}$ calculations.

If systematic errors (functional failures) are to be included in the calculations, separate values for each sub-system, if available, may be used in the equations above. An alternate approach is to use a single value for functional failure for the entire SIF and add this term as shown in Equation 1a in 5.1.6.

NOTE Systematic failures are rarely modeled for SIF Verification calculations due to the difficulty in assessing the failure modes and effects and the lack of failure rate data for various types of systematic failure. However, these failures are extremely important and can result in significant impact to the SIF performance. For this reason, ANSI/ISA-84.01-1996, IEC 61508, and IEC 61511 provide a lifecycle process that incorporates design and installation concepts, validation and testing criteria, and management of change. This lifecycle process is intended to support the reduction in the systematic failures. SIL Verification is therefore predominantly concerned with assessing the SIS performance related to random failures.

The simplified equations without the terms for multiple failures during repair, common cause and systematic errors reduce to the following for use in the procedures outlined in 5.1.1 through 5.1.4.

1oo1

(Eq. No. 3a) $$PFD_{avg} = \lambda^{DU} \times \frac{TI}{2}$$

1oo2

(Eq. No. 4a) $$PFD_{avg} = \frac{\left[\left(\lambda^{DU}\right)^2 \times TI^2\right]}{3}$$

1oo3

(Eq. No. 5a) $$PFD_{avg} = \frac{\left[\left(\lambda^{DU}\right)^3 \times TI^3\right]}{4}$$

2oo2

(Eq. No. 6a) $$PFD_{avg} = \lambda^{DU} \times TI$$

2oo3

(Eq. No. 7a) $$PFD_{avg} = \left(\lambda^{DU}\right)^2 \times TI^2$$

2oo4

(Eq. No. 8a) $$PFD_{avg} = \left(\lambda^{DU}\right)^3 \times (TI)^3$$

5.1.6 Combining components' PFDs to obtain SIF PFD_{avg}

Once the sensor, final element, logic solver, and power supply (if applicable) portions are evaluated, the overall PFD_{avg} for the SIF being evaluated is obtained by summing the individual components. The result is the PFD_{avg} for the SIF for the event being protected against.

(Eq. No. 1a) $$\mathrm{PFD_{SIS}} = \sum \mathrm{PFD_{Si}} + \sum \mathrm{PFD_{Ai}} + \sum \mathrm{PFD_{Li}} + \sum PFD_{PSi} + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

NOTE The last term in the equation, the systematic failure term, is only used when systematic error has not been accounted for in individual component PFD and the user desires to include an overall value for the entire SIF.

5.1.7 PFD improvement techniques

Where adjustments are required to decrease PFD_{avg}, additional redundancy may be used on components, the functional test interval may be decreased, the SIS configuration may be changed, or components with lower failure rates may be considered.

5.2 Mean time to failure spurious ($\text{MTTF}^{\text{spurious}}$) calculations

A safe failure of a component may cause a spurious trip of the system. Mean time to a safe failure is referred to as Mean Time to Failure Spurious ($\text{MTTF}^{\text{spurious}}$) that is the estimated time between safe failures of a component or system.

If trips of the SIS caused by failures of system components are a concern, the anticipated spurious trip rate may be calculated to determine if additional steps are justified to improve SIS reliability. The procedures for making these calculations are presented in the sections that follow.

In ISA-TR84.00.02-2002, the term Spurious Trip Rate (STR) refers to the rate at which a nuisance or spurious trip might occur in the SIS.

NOTE All components that can cause a SIS trip even though not directly related to a specific hazardous event must be considered in this evaluation.

5.2.1 Determining the STR for sensors

The procedure for determining the spurious trip rate caused by sensors is as follows:

1. Identify each sensor that is an initiator in the SIS.
2. List the $\text{MTTF}^{\text{spurious}}$ for each sensor.
3. List the MTTR for each sensor.
4. Calculate the spurious trip rate for each sensor using the equations in 5.2.5 with appropriate consideration for redundancy.
5. Sum the individual trip rates to determine the SIS trip rate based on sensors.

Combined sensor, $\text{STR}_\text{S} = \sum STR_{Si}$ (values for individual sensor configurations)

5.2.2 Determining the STR for final elements

The procedure for determining the spurious trip rate for final elements used in the SIS is as follows:

1. Identify each final element controlled or driven by the SIS.
2. List the $\text{MTTF}^{\text{spurious}}$ for each final element.
3. List the MTTR for each final element.
4. Calculate the spurious trip rate for each final element using the equations in 5.2.5 with appropriate consideration for redundancy.

5. Sum the individual trip rates to determine the SIS trip rate based on final elements.

Combined final element.- STR $_A$ = $\sum \mathrm{STR}_{\mathrm{Ai}}$ (values for individual final element configurations)

5.2.3 Determining the STR for logic solver(s)

The procedure for determining the spurious trip rate for logic solver(s) is as follows:

1. Identify each logic solver in the SIS.

2. List the MTTF$^{\text{spurious}}$ for each logic solver (Typically obtained from manufacturer).

NOTE Since the MTTF$^{\text{spurious}}$ for the logic solver is a non-linear function, the user should request the MTTF$^{\text{spurious}}$ as a function of MTTR. The user should specify the range of MTTR that is acceptable.

3. List the MTTR for each logic solver.

4. Calculate the spurious trip rate for each logic solver using the equations in 5.2.5 with appropriate consideration for redundancy.

   Note: This step is only required for a PES logic solver when the manufacturer does not supply the spurious trip rate value for the fully integrated logic solver system.

5. Sum the individual trip rates to determine the SIS spurious trip rate based on logic solver.

Combined logic solver - STR $_L$ = $\sum \mathrm{STR}_{\mathrm{Li}}$ (values for individual logic solver configurations)

5.2.4 Determining the STR for power supplies

NOTE The power supplies referred to here are those power sources external to the SIS. These typically are UPS, diesel generators, or alternate power sources. The power supplies internal to the logic solver must also be considered if their failure rate is not taken into account in the logic solver failure rate itself. Unless otherwise noted, the internal power supplies are assumed to be included in the logic solver failure rate for the calculations which follow.

The procedure for determining the spurious trip rate for power supplies is as follows:

1. Identify each power supply that impacts the SIS.

2. List the MTTF^S for each power supply.

3. List the MTTR for each power supply.

4. Calculate the spurious trip rate for the power supply using the equations in 5.2.5 with appropriate consideration for redundancy.

Combined power supply - STR $_{PS}$ = $\sum \mathrm{STR}_{\mathrm{PSi}}$ (values for multiple individual power supplies)

5.2.5 System equations for evaluating MTTF$^{\text{spurious}}$

The following equations cover the typical configurations used in SIS configurations. To see the derivation of the equations listed, refer to Reference 3 or ISA-TR84.00.02-2002 - Part 5.

The MTTF$^{\text{spurious}}$ for the individual SIS elements is converted to failure rate by, (Eq. No. 9) $\lambda^{S} = \dfrac{1}{MTTF^{spurious}}$

1oo1

(Eq. No. 10) $STR = \lambda^{S} + \lambda^{DD} + \lambda_{F}^{S}$

Where λ^{S} is the safe or spurious failure rate for the component,

λ^{DD} is the dangerous detected failure rate for the component, and

λ_{F}^{S} is the safe systematic failure rate for the component.

The second term in the equation is the dangerous detected failure rate term and the third term is the systematic error rate term. The dangerous detected failure term is included in the spurious trip calculation when the detected dangerous failure puts that channel (of a redundant system) or system (if it is non-redundant) in a safe (de-energized) state. This can be done either automatically or by human intervention. If dangerous detected failure does not place the channel or system into a safe state, this term is not included in Equations 10 through 15.

1oo2

(Eq. No. 11) $STR = \left[2 \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \left[\beta \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \lambda_{F}^{S}$

The second term is the common cause term and the third term is the systematic error rate term.

1oo3

(Eq. No. 12) $STR = \left[3 \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \left[\beta \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \lambda_{F}^{S}$

The second term is the common cause term and the third term is the systematic error rate term.

2oo2

(Eq. No. 13) $STR = \left[2 \times \lambda^{S}\left(\lambda^{S} + \lambda^{DD}\right) \times MTTR\right] + \left[\beta \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \lambda_{F}^{S}$

The second term is the common cause term and the third term is the systematic error rate term. This equation, as well as Equations 14 and 15, assumes that safe failures can be detected on-line. If safe failures can only be detected through testing or inspection, the testing (or inspection) interval TI should be substituted for MTTR.

2oo3

(Eq. No. 14) $STR = \left[6 \times \left(\lambda^{S}\right) \times \left(\lambda^{S} + \lambda^{DD}\right) \times MTTR\right] + \left[\beta \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \lambda_{F}^{S}$

The second term is the common cause term, and the third term is the systematic error rate term.

2oo4

(Eq. No. 15) $STR = \left[12 \times \left(\lambda^{S} + \lambda^{DD}\right)^{3} \times MTTR^{2}\right] + \left[\beta \times \left(\lambda^{S} + \lambda^{DD}\right)\right] + \lambda_{F}^{S}$

The second term is the common cause term, and the third term is the systematic error rate term.

NOTE The above equations apply to elements with the same failure rates. If elements with different failure rates are used, appropriate adjustments must be made (See ISA-TR84.00.02-2002, Part 5 for method).

SIS in the process industry typically must be taken out of service to make repairs when failures are detected unless redundancy of components is provided. Accounting for additional failures while repairs are being made is typically not considered due to the relatively short repair time. Common cause and systematic error are handled as described in 5.1.5. Therefore, the equations above can be reduced to the following:

<u>1oo1</u>

(Eq. No. 10a) $STR = \lambda^S$

<u>1oo2</u>

(Eq. No. 11a) $STR = 2 \times \lambda^S$

<u>1oo3</u>

(Eq. No. 12a) $STR = 3 \times \lambda^S$

<u>2oo2</u>

(Eq. No. 13a) $STR = 2 \times \left(\lambda^S\right)^2 \times MTTR$

<u>2oo3</u>

(Eq. No. 14a) $STR = 6 \times \left(\lambda^S\right)^2 \times MTTR$

<u>2oo4</u>

(Eq. No. 15a) $STR = 12 \times \left(\lambda^S\right)^3 \times MTTR^2$

5.2.6 Combining spurious trip rates for components to obtain SIS MTTF$^{\text{spurious}}$

Once the sensor, final element, logic solver, and power supply portions are evaluated, the overall MTTF$^{\text{spurious}}$ for the SIS being evaluated is obtained as follows:

(Eq. No. 16) $STR_{SIS} = \sum STR_{Si} + \sum STR_{Ai} + \sum STR_{Li} + \sum STR_{PSi} + \lambda_F^S$

NOTE The last term in the equation, the systematic failure term, is only used when systematic error has not been accounted for in individual component STR and the user desires to include an overall value for the entire system.

(Eq. No. 17) $MTTF^{spurious} = \dfrac{1}{STR_{SIS}}$

The result is the MTTF$^{\text{spurious}}$ for the SIS.

5.2.7 Techniques for reducing spurious trip rate

Where the spurious trip rate is not acceptable, additional redundancy may be added to system components or more reliable components may be used. This will require re-evaluating the system PFD_{avg} to confirm that it still meets the requirements of the Safety Requirements Specifications.

5.3 Final element configurations

The following figures illustrate how different valve configurations should be treated with respect to redundancy in the calculations:

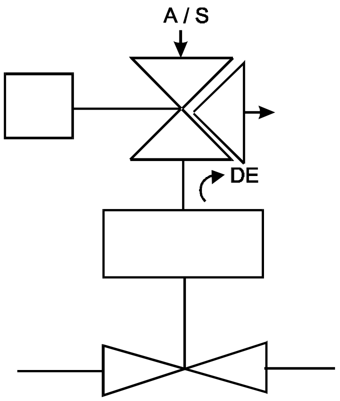


Figure 5.1 — 1oo1 final element

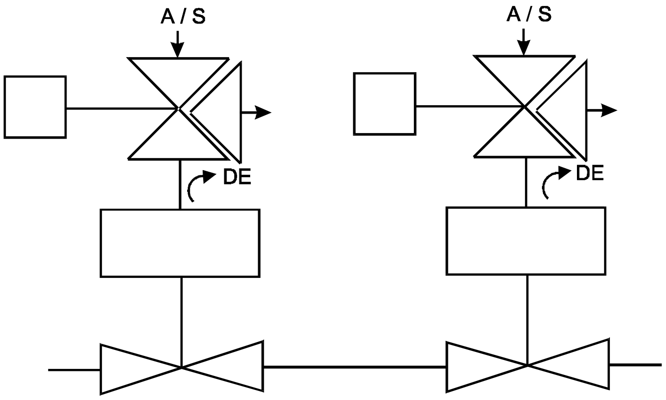


Figure 5.2 — 1oo2 final element

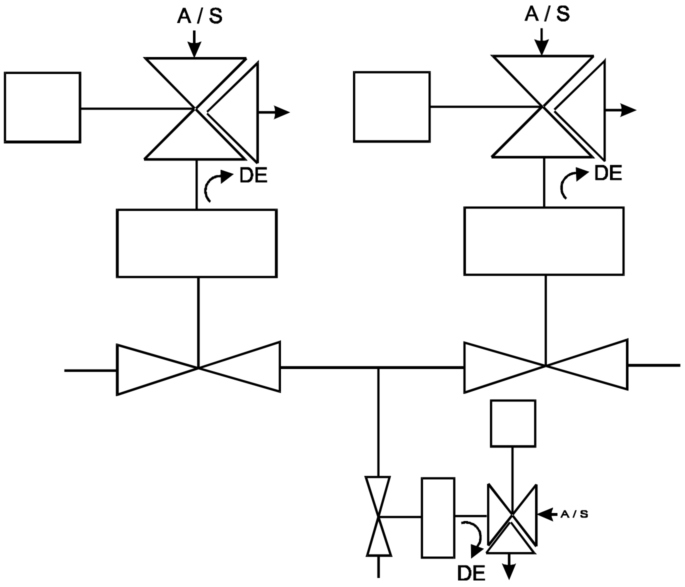


Figure 5.3 — 1oo2 final element (alternate)

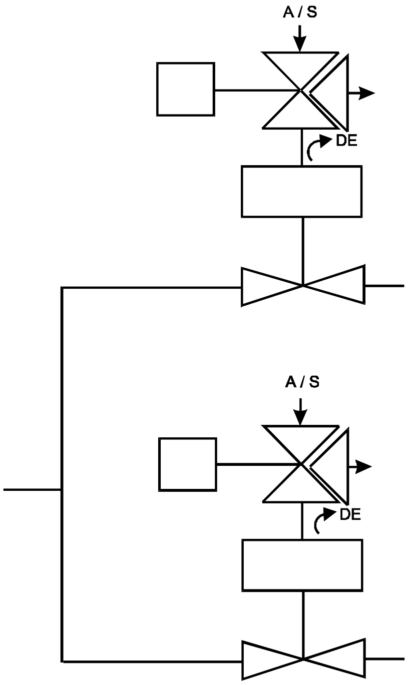


Figure 5.4 — 2oo2 final element

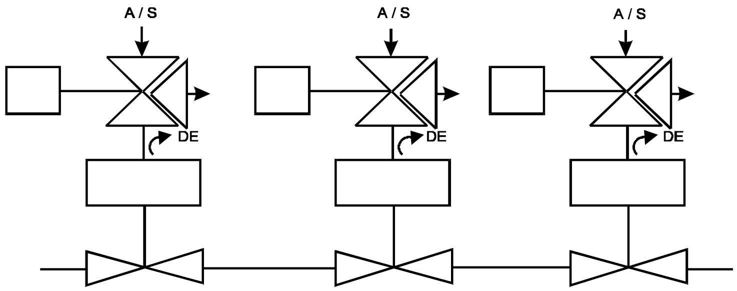


Figure 5.5 — 1oo3 final element

6 Base case example calculation for a SIF using simplified equations

NOTE This example is the base case example used in ISA-TR84.00.02-2002 - Parts 3 and 4 , as well as this part to illustrate the different techniques for evaluating the SIF PFD_{avg}.

The example SIS configuration shown in Figure 6.1 is modeled to demonstrate the Simplified Equation procedure for determining the safety integrity level and spurious trip rate of a SIF. **The PFD_{avg} and spurious trip rate calculation provided in this Clause is for illustrative purposes only and should not be used without review for the appropriateness for the specific installation.** The following assumptions are made relative to this example and the SIF components:

1. All inputs and outputs in the example are assumed to be part of the same SIF. Therefore a single PFD_{avg} and a single $MTTF^{spurious}$ are calculated for the entire SIF.

2. In a process hazard analysis, it was determined that the SIF should have a SIL 2.

3. The SIF is designed as de-energize to trip and will go to a safe state on loss of power. The $MTTF^{spurious}$ of the power supply is assumed to be 20 years.

4. Redundant AC power supplies (2) are provided external to the system.

5. All redundant devices are assumed to have the same failure rate.

6. The logic solver is a PES with output redundancy to prevent unsafe failure of an output and has an external watchdog circuit. The PFD_L and $MTTF^{spurious}$ for the logic solver are assumed values. The PFD_{avg} is 0.005 and the $MTTF^{spurious}$ is 10 years.

   CAUTION — THE USER SHOULD OBTAIN PFD_L FROM THE LOGIC SOLVER VENDOR FOR THE ACTUAL FUNCTIONAL TEST INTERVAL.

7. It is generally assumed that when a dangerous detected failure occurs, the SIF will take the process to a safe state or plant personnel will take necessary action to ensure the process is safe (operator response is assumed to be before a demand occurs and PFD of operator response is assumed to be 0).

   NOTE If the action depends on plant personnel to provide safety, the user is cautioned to account for the probability of failure of personnel to perform the required function in a timely manner.

8. A one (1) year functional test interval is assumed for the SIF components. Testing is assumed to be perfect.

9. The mean time to repair is assumed to be 8 hours, and the repair is assumed to be perfect.

10. The effects of common cause and systematic errors are assumed to be negligible in the calculations.

11. The use of diagnostics outside the normal design of the devices is not modeled in this example. It is assumed that spurious failures are detected on-line.

12. For simplicity, other possible contributions to PFD and STR such as loss of instrument air are not included in the example calculations. They are incorporated into the MTTF^{DU} and $\text{MTTF}^{spurious}$ for the individual components.

13. The MTTF^{D} and $\text{MTTF}^{spurious}$ values used in the example are representative values taken from the Table 5.1 of ISA-TR84.00.02-2002 – Part 1.

14. **The MTTF numbers used in the example in Clause 6 are for illustrative purposes only and should not be used for actual evaluation of a specific SIF.**

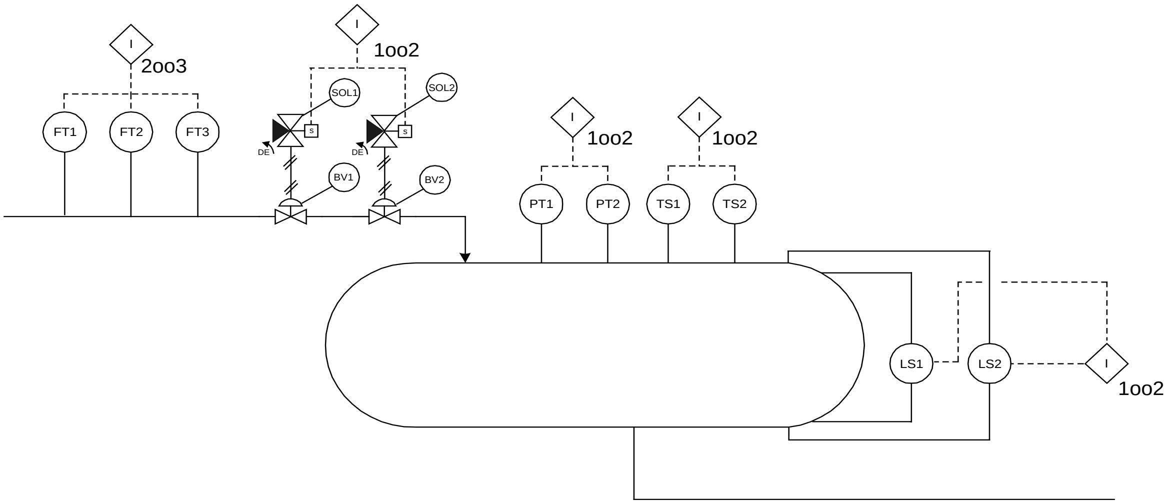


Figure 6.1 — Process diagram of example

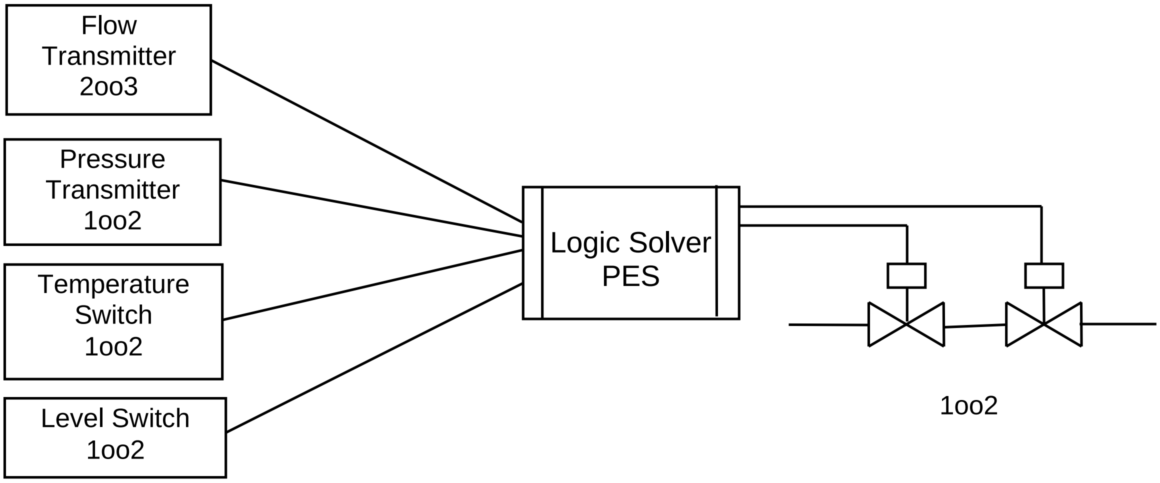


Figure 6.2 — Example SIS configuration

6.1 Calculations for PFD_{avg}

Calculations for the example SIS are as follows.

6.1.1 PFD for sensors

Sensor	**$MTTF^{DU}$**	**PFD_{avg}**	**(Eq. No.)**
Flow Transmitter (head type) (2oo3)	40	6.25 x E-4	7a
Pressure Transmitter (1oo2)	50	1.33 x E-4	4a
Temperature Switch (1oo2)	15	1.48 x E-3	4a
Level Switch (1oo2)	25	5.33 x E-4	4a
$\sum PFD_{Si}$		2.77 x E-3	

NOTE $\lambda^{DU} = 1/MTTF^{DU}$

6.1.2 PFD for final elements

Block Valve $MTTF^{DU}$ is 50 years, $\lambda^{DU} = 1/MTTF^{DU} = 0.02$

Solenoid Valve $MTTF^{DU}$ is 50 years, $\lambda^{DU} = 1/MTTF^{DU} = 0.02$

Combined λ^{DU} for block valve and solenoid valve is 0.02 + 0.02 = 0.04

Final Element configuration is 1oo2.

Using Eq. No. 4a, PFD_A = 5.33 x E-4

6.1.3 PFD for logic solver

$MTTF^{DU}$ for logic solver is 100 (provided by manufacturer and includes the WDT)

PFD_{avg} for logic solver is 0.005 (provided by the manufacturer)

6.1.4 PFD_{avg} for power supply

Since the SIS is de-energize to trip, the power supply does not impact the system PFD.

6.1.5 PFD_{avg} for system

(Eq. No. 1) PFD_{SIS} = 2.77 x E-3 + 5.33 x E-4 + 5 x E-3 = 8.3 x E-3

The calculated SIL should be compared to the SIL specified in the SRS to ensure that the calculated SIL for this SIS equals or exceeds the required SIL, as specified from the risk assessment. Therefore, this SIS meets the requirements of a SIL 2 system (SIL 2 PFD_{avg} range is 0.01 - 0.001).

6.2 Calculations for $MTTF^{spurious}$

The calculations for the spurious trip frequency of the example system follow:

6.2.1 STR for sensors

Sensors	**MTTF ^{S}** Years	**STR** Per year	**Eq. No.**
Flow Transmitter (head type) (2oo3)	20	4.1 x E-5	14a
Pressure Transmitter (1oo2)	25	8.0 x E-2	11a
Temperature Switch (1oo2)	5	4.0 x E-1	11a
Level Switch (1oo2)	10	2.0 x E-1	11a
$\sum STR_{Si}$		6.8 x E-1	

6.2.2 STR for final elements

Final Elements	**$MTTF^{S}$** years	**STR** Per year	**Eq. No.**
Double block valves (1oo2)	25	8.0 x E-2	11a
Solenoid valves (1oo2)	25	8.0 x E-2	11a
$\sum STR_{Ai}$		1.6 x E-1	

6.2.3 STR for logic solver(s)

$MTTF^{S}$ for logic solver is 10 years (provided by manufacturer)

STR_{l} for logic solver is 1.0 x E-1 per year (provided by manufacturer)

6.2.4 STR for power supply

$MTTF^{S}$ for power supply is 20 years.

(Eq. No. 13a) $STR_{PS} = 5 \times E\text{-}2$ per year

6.2.5 $MTTF^{spurious}$ for system

$STR_{SIS} = 6.8 \times E\text{-}1 + 1.6 \times E\text{-}1 + 1.0 \times E\text{-}1 + 5 \times E\text{-}2 = 9.9 \times E\text{-}1$ per year

(Eq. No. 16) $$MTTF_{SIS} = \frac{1}{STR_{SIS}} = 1/0.99 = 1.01 \text{ years}$$

This means that there will be about one (1) spurious trip per year for the SIS configuration. If this is not acceptable, consider changing the voting or redundancy of the system components to reduce spurious trips. Of course, any configuration changes must be re-verified to ensure that the PFD_{avg} requirement is maintained.

This page intentionally left blank.

7 Index

Developing and promulgating sound consensus standards, recommended practices, and technical reports is one of ISA's primary goals. To achieve this goal the Standards and Practices Department relies on the technical expertise and efforts of volunteer committee members, chairmen and reviewers.

ISA is an American National Standards Institute (ANSI) accredited organization. ISA administers United States Technical Advisory Groups (USTAGs) and provides secretariat support for International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) committees that develop process measurement and control standards. To obtain additional information on the Society's standards program, please write:

ISA
Attn: Standards Department
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

ISBN: 1-55617-803-4