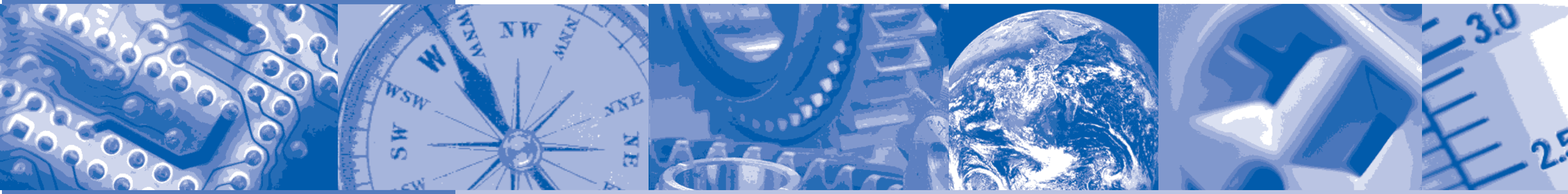
TECHNICAL REPORT

ISA-TR84.00.02-2002 - Part 3



Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of a SIF via Fault Tree Analysis

Approved 17 June 2002

ISA–The Instrumentation,
Systems, and
Automation Society

ISA-TR84.00.02-2002 – Part 3
Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques Part 3:
Determining the SIL of a SIF via Fault Tree Analysis

ISBN: 1-55617-804-2

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 3.

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

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.

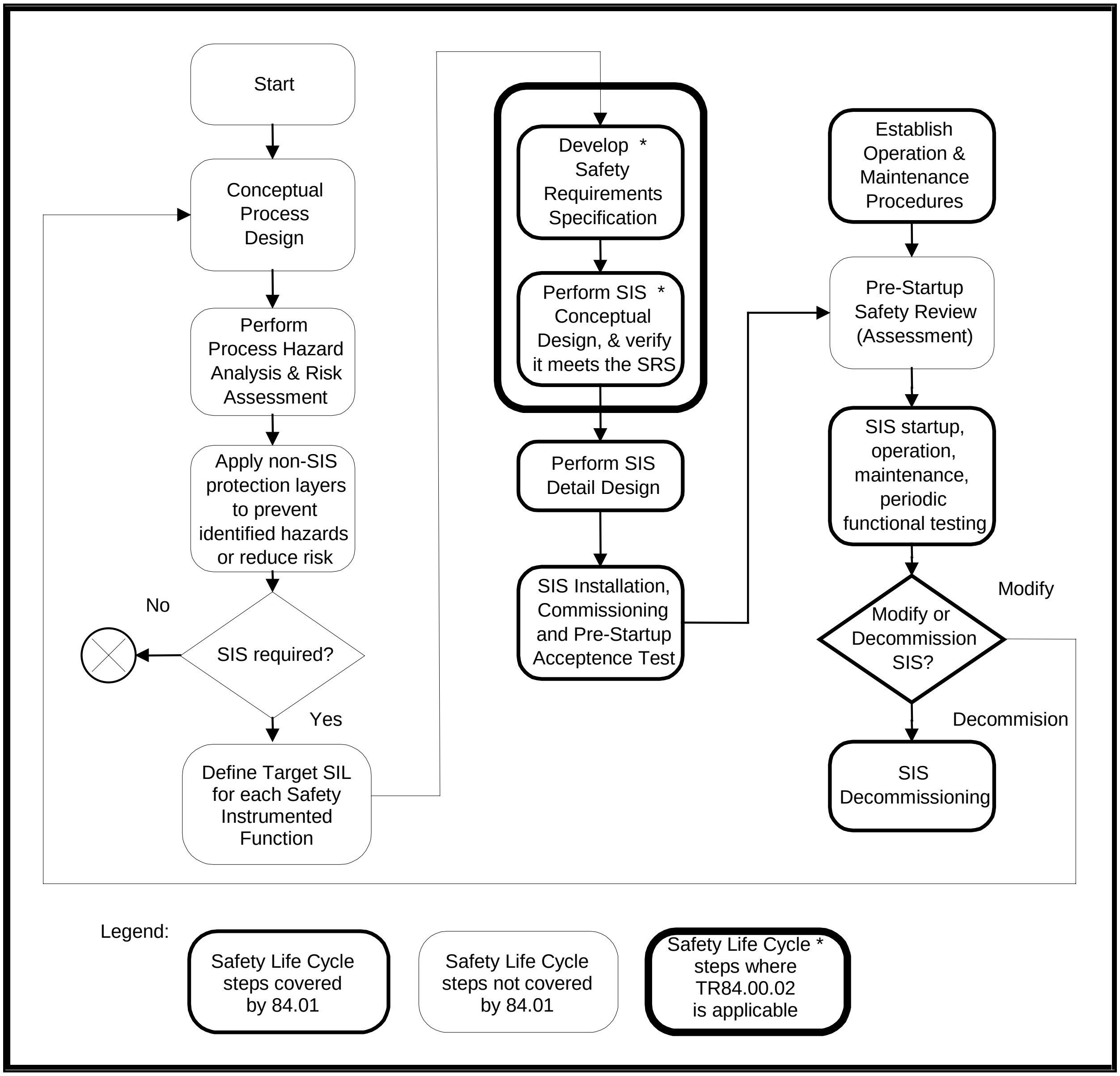

Start
Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
No
SIS required?
Yes
Define Target SIL for each Safety Instrumented Function
Develop * Safety Requirements Specification
Perform SIS * Conceptual Design, & verify it meets the SRS
Perform SIS Detail Design
SIS Installation, Commissioning and Pre-Startup Acceptence Test
Establish Operation & Maintenance Procedures
Pre-Startup Safety Review (Assessment)
SIS startup, operation, maintenance, periodic functional testing
Modify
Modify or Decommission SIS?
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

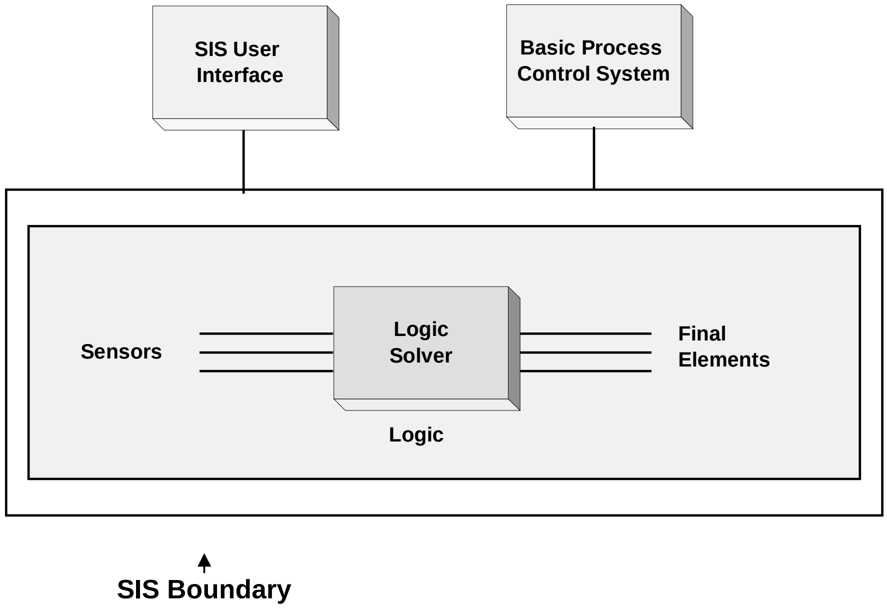


Figure I.2 — Definition of Safety Instrumented System (SIS)

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.

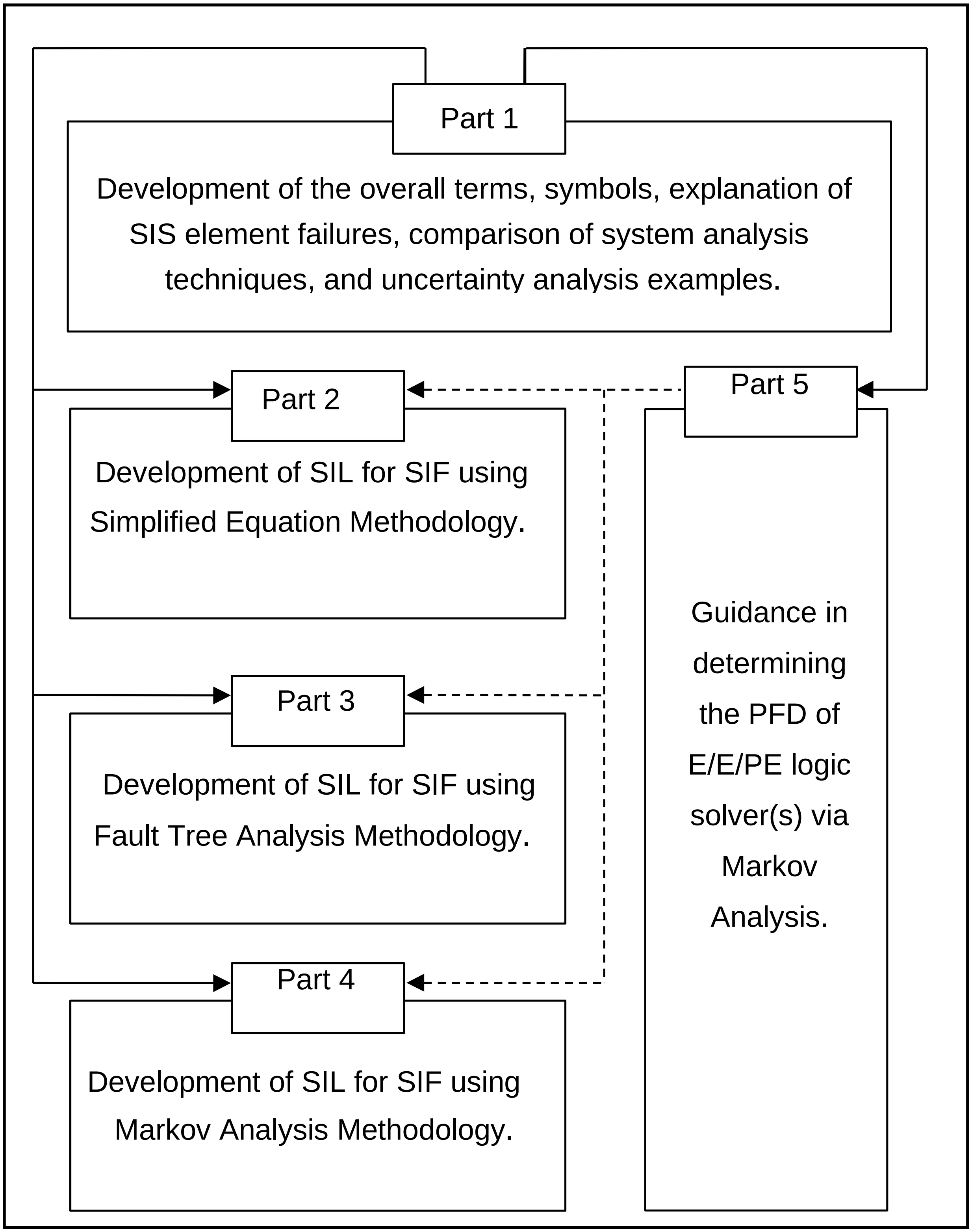

Part 1
Development of the overall terms, symbols, explanation of SIS element failures, comparison of system analysis techniques, and uncertainty analysis examples.
Part 2
Development of SIL for SIF using Simplified Equation Methodology.
Part 3
Development of SIL for SIF using Fault Tree Analysis Methodology.
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 3 is intended to be used only after achieving a thorough understanding of ISA-TR84.00.02-2002 – Part 1, which defines the overall scope. This technical report addresses:

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; and

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

1.2 ISA-TR84.00.02-2002 - Part 3 is considered informative and does not contain any mandatory requirements. The User should refer to ISA-TR84.00.02-2002 – Part 1, which defines the general requirements for the verification of SIL for SIF.

1.3 ISA-TR84.00.02-2002 - Part 3 is intended to provide guidance on the application of Fault Tree Analysis (FTA) to SIF. FTA is one possible technique for calculating SIL for a SIF installed per ANSI/ISA-84.01-1996(1).

1.4 ISA-TR84.00.02-2002 - Part 3 covers the analysis of a SIF application from the field sensors through the logic solver to the final elements.

1.5 Common cause failure and systematic failure are an example of important factors readily modeled in FTA.

1.6 Part 3 assumes that the complex analysis of the failure rate for a programmable logic solver is done by another method (see Part 5) or is provided by a vendor as an input PFD_L or $MTTF^{spurious}$ into this analysis (per Clause 7.3.2 of ANSI/ISA-84.01-1996, the failure rate of the logic solver should be supplied by the logic solver vendor). Calculation of the PFD_{avg} and $MTTF^{spurious}$ of electrical/electronic/ programmable electronic systems can be performed using FTA by applying the techniques presented in this part.

1.7 This part 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).

1.8 The ultimate goal for the FTA is to determine the following:

- The PFD_{avg}, Safety Integrity Level (SIL), and

- The $MTTF^{spurious}$ of the SIF

This analysis aids in the design of an effective SIF by allowing the User to determine where weaknesses exist within the SIF. This technique is applicable when the failure of the SIF can be caused by more than one pathway, when strong interactions exist between multiple SIF, or when several support systems (instrument air, cooling water, power, etc.) are involved.

2 References

1. ANSI/ISA-84.01-1996 “Application of Safety Instrumented Systems for the Process Industries," Instrumentation, Systems, and Automation Society, 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, Hiromitsu, IEEE Press, New York, New York, 1992.

7. “Guidelines for Chemical Process Quantitative Risk Analysis,” Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, New York, 1989.

8. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), IRRAS/SARA Version 5.12, U. S. Nuclear Regulatory Commission, 1996.

9. “Guidelines for Preventing Human Error in Process Safety,” Center of Chemical Process Safety, American Institute of Chemical Engineers, New York, New York, 1994.

10. “An Engineer’s View of Human Error,” Trevor A. Kletz, Gulf Publishing Company, Houston, Texas, 1991.

11. NUREG/DR-1278-F, “Handbook of Human Reliability Analysis for Emphasis on Nuclear Power Plant Applications,” Swain & Guttermann, 1983.

3 Introduction to Fault Tree Analysis

Fault Tree Analysis (FTA) originated in the 1960s at Bell Telephone Laboratories under the direction of H. A. Watson. FTA was developed to evaluate the safety of the Polaris missile project and was used to determine the probability of an inadvertent launching of a Minuteman missile. The methodology was extended to the nuclear industry in the 1970s for evaluating the potential for runaway nuclear reactors. Since the early 1980s, FTA has been used to evaluate the potential for incidents in the process industry, including the potential for failure of the safety instrumented function (SIF). FTA is a well-recognized and well-respected technique for determining the probability of events that occur due to failures of various equipment and components. The symbols used in Fault Tree Analysis are in Annex A, and the mathematics used are in Annex B.

FTA can be a rigorous and time-consuming methodology. It is a very structured, graphical technique that can be used to examine a single interlock or the interaction of multiple interlocks. Since FTA is used at the component and application specific event level, it should not be applied until the SIF design is well understood. In terms of the ANSI/ISA-84.01-1996 Life Cycle Model, the FTA should be performed only after the Safety Requirement Specification or Conceptual Design phases are complete.

WARNINGS —

3.1 FTA, similar to all the other methods in this report, cannot arrive at an absolute answer. FTA can only account for failure pathways that the person doing the analysis identifies and includes in the model. Furthermore, the failure rate values used in the assessment are based on large samples of industrial data. These failure rates must be adjusted with the knowledge of actual process operating conditions, external environmental conditions, operating history, maintenance history, and equipment age.

3.2 FTA, similar to all the other methods in this report, is not a replacement for good engineering design principles, but it is a good method to assess the SIL of the SIF design.

3.3 ANSI/ISA-84.01-1996, like other international standards describing the application of SIFs in the process industry, defines SIL in terms of PFD_{avg}. Unfortunately, it is difficult to obtain a PFD_{avg} value for an entire system due to the time-dependent, non-linear properties of most SIF logic. Calculation of the actual average can be performed by either a) deriving the instantaneous equation to describe the SIF logic and symbolically integrating the equation over the testing interval or b) numerically integrating the SIF logic using a large number of discrete time intervals over the testing interval.

As an alternative, many practitioners of FTA use an approximation to calculate PFD_{avg} in a single step. Using the approximation, the analyst integrates the instantaneous equation for each component over its testing interval to determine the PFD_{avg} for the component. Then, the individual component PFD_{avg} values are combined using Boolean algebra based on the fault tree logic to calculate the overall PFD_{avg}. Care should be exercised when employing this approximation. The deviation from the actual average when using this approximation can be substantial and the direction of the error is typically non-conservative (i.e., results in a lower PFD_{avg} than is actually achieved). When using this approximation, the analyst is cautioned to select conservative failure rates to account for non-conservative inaccuracies in the approximation technique.

The approaches described above are different and may not result in the same PFD_{avg}, depending on the configuration. Both approaches are discussed further in Annex B with a comparison of the numerical results. Section 7.0 also uses both solution techniques to solve the Base Case Example. **Due to the wide spread use of FTA, many software packages are available to facilitate the calculations. These software packages typically use the approximation technique for obtaining the PFD_{avg}. As with any software tool, the User is cautioned to understand the equations, mathematics, and any simplifying assumptions, restrictions, or limitations.**

4 Definition of terms and symbols

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

5 Assumptions for Fault Tree calculations for a SIF

The following assumptions were used in this part for Fault Tree calculations:

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

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

5.3 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.

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

5.5 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.

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

5.7 While dependent failures can be modeled using FTA, it is generally assumed that the failure of individual components is statistically independent of other component, that is, the failure of any component is in no way affected by the failure of any other component.

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

5.9 It is generally assumed that all repairs are perfect, that is, the repair results in the component being returned to its normal state. If review of the repair history identifies failures that have not been adequately repaired, FTA should be used to model imperfect maintenance and repair.

5.10 It is generally assumed that all testing is perfect, that is, the testing procedure will detect the covert failure of a component. If review of the testing procedures identifies failures that would not be detected by the testing procedure, the FTA should be used to model those failures.

5.11 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.

5.12 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.

5.13 The target PFD_{avg} and $MTTF^{spurious}$ is defined for each safety instrumented function implemented in the SIS.

5.14 ISA-TR84.00.02-2002 - Part 3 assumes that the User is familiar with FTA techniques and understands the principles behind construction of the fault trees. For further information on fault tree construction, please refer to *Probabilistic Risk Assessment*[(6)] and *Guidelines for Chemical Process Quantitative Risk Analysis*[(7)]*.*

6 Procedure

INTRODUCTION

FTA is generally an iterative process that involves modeling a SIF to determine the PFD, then modification of the SIF (and associated model) to achieve the target PFD. The fault tree analysis of a SIF can be broken down into 5 essential steps:

1. SIF Description and Application Information;

2. Top Event Identification;

3. Construction of the FTA;

4. Qualitative Examination of the Fault Tree Structure; and

5. Quantitative FTA Evaluation.

The following procedure summarizes the important aspects of how a SIF is modeled using FTA.

6.1 Step 1. SIF description and application information

Calculations to verify the SIF design meets the specified SIL are generally performed during the Conceptual Design phase of the Safety Life Cycle Model. Consequently, the information required for the FTA should be well understood and readily available. Critical information to the successful development of the fault trees is as follows:

- Instrumentation description
- Process description
- Support systems (instrument air, cooling water, hydraulic, electrical power, etc.) involved in SIF operations
- Testing frequency and whether testing is done on-line or off-line
- Testing procedures and equipment used and likelihood for SIF equipment to be compromised by testing
- Failure modes
- Failure rates
- Diagnostic coverage
- Repair intervals and whether repair is done on-line or off-line
- Maintenance procedures and likelihood of SIF equipment compromised by repair
- Management of change procedures, frequency of change, and likelihood of error introduced during change
- Operating and maintenance discipline, including an estimate of the frequency of human error and circumstances where incorrect bypassing could occur
- Administrative procedures
- Common cause failures
- Systematic failures
- Identify safety functions and their associated I/O and field components

Estimates for many of these factors are application or site specific.

6.2 Step 2. Top event identification

The FTA process begins with the determination of the Top Event. For SIL determination, the Top Event is the probability of the SIF to fail on process demand for a given safety function. Fault trees can also be constructed to determine the potential for the SIF to spurious trip. The structure of the fault tree is different for SIL determination and spurious tripping, so the Top Event to be modeled must be defined prior to proceeding with the fault tree analysis.

A process unit often has more than one safety function that will require SIL determination. Each safety function has a defined Top Event that is associated with a specific process hazard that has been identified by the Process Hazards Analysis (PHA). The Top Event will, in turn, have failure logic associated with the event that can be modeled in a Fault Tree. For instance, a furnace might have a tube rupture Top Event that can be detected with a pass flow measurement. The same furnace might have a firebox overpressure Top Event that is detected by burner pressure. The tube rupture and firebox overpressure safety functions would be modeled with separate fault trees, although they may share a logic solver and a fuel gas shutoff valve. The two safety functions might even have different SIL requirements.

<u>Only those sensors and final elements that prevent or mitigate the designated event are included in calculations</u>.

6.3 Step 3. Construction of the fault tree

Once the Top Event has been determined, the fault trees are constructed using appropriate failure logic. FTA models how the failure of a particular component or set of components can result in the Top Event. The SIF is analyzed by a top down procedure, in which the primary causes of the Top Event are identified. The fault tree construction continues by determining the failures that lead to the primary event failures. The fault tree is constructed using fault tree symbols and logic gates as described in Annex A.

The construction of the fault tree continues until all the basic events that influence the Top Event are evaluated. Ideally, all logic branches in the fault tree are developed to the point that they terminate in Basic events. At a minimum, the fault tree logic should include how failures of individual SIF components, including the various inputs, outputs, and the logic solver, affect the Top Event. SIF component failures that are Basic events include primary, common cause, and systematic failures.

Random Hardware Failures

Random hardware failures for SIF components are the immediate component failures, of a random nature. The random hardware failures are typically due to sensor, logic solver, or final element failure.

Common Cause Failures and Systematic Failures

Common cause failures and systematic failures can be due to a single failure event or to a combination of systematic failure, common cause failure, poor design practices, and/or poor operation/maintenance practices. If the potential for common cause failures and systematic failures is not evaluated, the PFD calculation may result in an overly optimistic assessment of the PFD.

When Should Common Cause Failures and Systematic Failures Be Modeled?

Systematic and common cause failures are important considerations in FTA, particularly for SIL 2 and above applications. When common cause failures and systematic failures are not evaluated, there is an implicit assumption that good practices for design, installation, operation, maintenance, and management of change are in place.

- Good practice can result in a low common cause failure and systematic failure rate, so that the modeling of only the random hardware failures provides a good estimate of the PFD_{avg} for the SIF.

- Poor practice can result in a high common cause failure and systematic failure rate, which can actually be equal to or greater than the calculated random hardware failure rate. Thus, the PFD_{avg} calculated from the modeling of the random hardware failures is too low.

The following situations are some examples for which common cause failures and systematic failures might be modeled:

- A SIF that involves unusual or complex design or maintenance features

- A site where there have been incidents of poor operating discipline

- A significant change in management practices, such as downsizing, that impacts SIF operating and maintenance practices

Part 1, Annex E provides a checklist for determining the potential causes of common cause failures and systematic failures.

How are common cause failures and systematic failures modeled?

The modeling of common cause failures and systematic failures is performed by including appropriate basic events in the fault tree.

An understanding of operating, maintenance, testing, and diagnostic information is key to identifying which common cause failures and systematic failures should be included in the fault tree as basic events or used as a factor in assessing the random hardware failure rate. The failure rates for any of these basic events can be estimated using plant data for frequency of common cause failures and systematic failures or with data from published sources. Human factor data is available in published literature. *Guidelines for Preventing Human Error in Process Safety*(9) provides data for the chemical industry and also describes the techniques utilized in evaluating and modeling human reliability. *An Engineer's View of Human Error*(10) provides a discussion on how human factors can affect the safe operation of process units.

Estimates should be made for the probability and duration of common cause failures and systematic failures of components. Plant operating experience and human factors data are used to estimate likelihoods and duration times. For example, an incorrect calibration of a sensor might occur 1 out of 100 times the task is done. If the calibration is routinely performed at the annual testing interval, the duration of failure would be one year.

There are two ways to account for common cause failures and systematic failures:

1. **Explicit model:**

- Identify the causes of common cause failures and systematic failures and add basic events to the fault tree using conservative failure rates for the common cause failures and systematic failures.

2. **Approximation techniques:**

- Compare qualitatively the current FTA with results from previous FTAs on similar SIF. Those common cause failures and systematic failures that were shown to be significant would then be put in the FTA.

- Evaluate the potential effects of common cause failures and systematic failures and use conservative failure rates for the random hardware failures to account for the potential common cause failures and systematic failures.

Common Cause

Common cause failures should normally be modeled as basic events that cause the failure of a component or a sub-system. It is important to recognize the same event (common cause) when it appears in two or more places in the fault tree. For example, instrument air failure that disables the primary transmitter can be the same instrument air failure that disables the redundant transmitter; in this case, both instances of instrument air should be modeled as the same basic event.

To account for undeveloped common cause sources, a basic event called "beta factor" may be included at a conservative probability (see Part 1, Annex A).

Problems in Constructing Models

The User should be cautioned to proceed with fault tree development carefully to ensure that the fault tree does not evolve into a functional logic description of the SIF.

A key point in the fault tree development is that the fault tree should model how failures in the SIF propagate into the Top Event (fail-safe or fail-dangerous conditions). In the initial stages of fault tree development, it is critical to address all known paths to SIF failure.

Basic events that are proven to be negligible in their effect on the probability of the Top Event may be omitted from the analysis at a later time.

6.4 Step 4. Qualitative review of the fault tree structure

After the fault tree is constructed, the fault tree should be reviewed. The fault tree review should include the process and instrumentation designers, operations, and risk assessment. This review confirms that the fault tree model has correctly captured:

- The Top Events and the safety functions specified in the PHA and the SRS
- The failure modes of the components
- The combinations of basic events leading to the Top Events
- All significant pathways to failure
- Common cause failures
- Systematic failures
- Other SIF complexities or interactions

For large and/or complex fault trees, the qualitative examination of the fault tree alone may not be sufficient to completely audit the structure of the fault tree. For these fault trees, a listing of the minimal cut sets should also be generated and reviewed for consistency with how the SIF functions. A cut set is a combination of basic events that give rise to the Top Event, that is, when the failure of the basic events in the cut set occurs, the Top Event will occur. A brief discussion of minimal cut sets is provided in Annex B.

6.5 Step 5. Quantitative evaluation of fault tree

Once the fault tree structure is fully developed, failure rate data is employed to quantify the fault tree. Failure rate data can be obtained from plant experience or from industry published data. A listing of the industry published data sources is provided in ISA-TR84.00.02-2002 - Part 1. The data must be obtained for all SIF components. Since the primary objective of the Fault Tree Analysis is to obtain a reasonable and conservative estimate of PFD_{avg}, it is better to use conservative failure rates for the field components, that is, conservative failure rates will result in a higher estimate of PFD_{avg}.

Fault tree analysis does involve the use of Boolean algebra for the mathematical quantification. An overview of the equations typically used in the assessment of safety instrumented functions is provided in Annex B. Hand calculations using these equations are possible but can become quite cumbersome. Therefore, it is recommended that a computer software program be used for quantification of the fault trees. There are several commercially available software tools.

As the tree is quantified, the results should be examined for consistency. A cut set report should be generated showing the order of importance of each cut set to the overall PFD_{avg}. The cut sets at the top and the bottom of the importance list should be examined to see if their presence in the importance list (influence on PFD_{avg}) makes sense in view of the practical knowledge of the facility and similar facilities.

Next, the calculated PFD_{avg} should be compared to the target PFD_{avg} specified in the Safety Requirements Specification (See ANSI/ISA-84.01-1996, Clause 5 and Clause 6.2.2) for each safety instrumented function (SIF). If the SIF has not met or exceeded the target $PFD_{avg,}$, apply risk reduction techniques and re-calculate to meet the target PFD_{avg}. Typical risk reduction techniques that might be addressed are as follows:

- Increase testing frequency for SIF components.
- Investigate the $MTTF^{D}$ and $MTTF^{spurious}$ of SIF components and consider replacing low integrity SIF components with types or models that have greater integrity.
- Consider modifying the SIF to include more redundancy or diversity.
- Increase the diagnostic capability of the SIF components.

Other risk reduction techniques require PHA team participation:

- Improve administrative procedures for design, operation, and maintenance, or
- Add other layers of SIF protection.

The fault tree model can be updated to calculate the new PFD_{avg} as these risk reduction techniques are applied.

6.6 Step 6. Documentation of FTA Results

The FTA Documentation may include, but is not limited to:

- SIF application (Company, Plant, Unit, Safety Function)
- Assumptions
- Reference to the SRS documents used in the FTA
- Data
- Model
- Cut sets and importances for each top event
- PFD_{avg}
- $MTTF^{spurious}$
- Sensitivity and what-if studies (A sensitivity study estimates the change in PFD_{avg} or $MTTF^{spurious}$ for estimates of uncertainty in the component failure rate data. A what-if study estimates the change in PFD_{avg} or $MTTF^{spurious}$ for changes in the SIF configuration.)
- Recommendations for improvement of SIF (if any)
- Calculation details:
  - The FTA analysis program used
  - Equations chosen
  - Hand calculations used to transform component failure rate data into program input format, if used
  - Software options selected (for example, cut off criteria)
  - Input and output files (on disk or electronic form)
  - Name of person doing the calculations
  - Date(s) work was done (completed)

7 Base case example calculation for an SIF using FTA - without common cause failures and systematic failures

NOTE This example is the base case example used in TR84.00.02-2002 - Parts 2 and 4, as well as this part to illustrate the different techniques for evaluating the SIF PFD_{avg}.

The example SIF configuration in Figure 7.1 is modeled to demonstrate the Fault Tree Analysis 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 safety function. 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 components 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. A one (1) year functional testing interval is assumed for the SIF components. Testing is assumed to be perfect.

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

9. For the Base Case Example, the effects of common cause and systematic errors are assumed to be negligible in the calculations.

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

11. 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 $MTTF^{spurious}$ for the individual components.

12. The $MTTF^D$ and $MTTF^{spurious}$ values used in the example are representative values taken from the Table 5.1 of ISA-TR84.00.02-2002 – Part 1. A summary of the $MTTF^D$ and $MTTF^{spurious}$ data used in this analysis is provided in Table 7.1.

13. Equations B.27 and B.34 (as shown in Annex B, TR84.00.02 - Part 3) was used for the PFD_{avg} example calculation when using the “Average Before Logic” technique and Equation B.18 was used for calculation when using the “Average After Logic” Technique.

14. **The MTTF numbers used in the example in Clause 7 are for illustrative purposes only and should not be used for actual evaluation of a specific SIF.**

7.1 Base case example SIF calculation

The Base Case Example SIF equipment is shown in Figure 7.1 and the schematic configuration is shown in Figure 7.2. This Base Case Example SIF is also shown in ISA-TR84.00.02-2002 - Parts 2 and 4. The equipment failure rate data used in the analysis is shown in Table 7.1

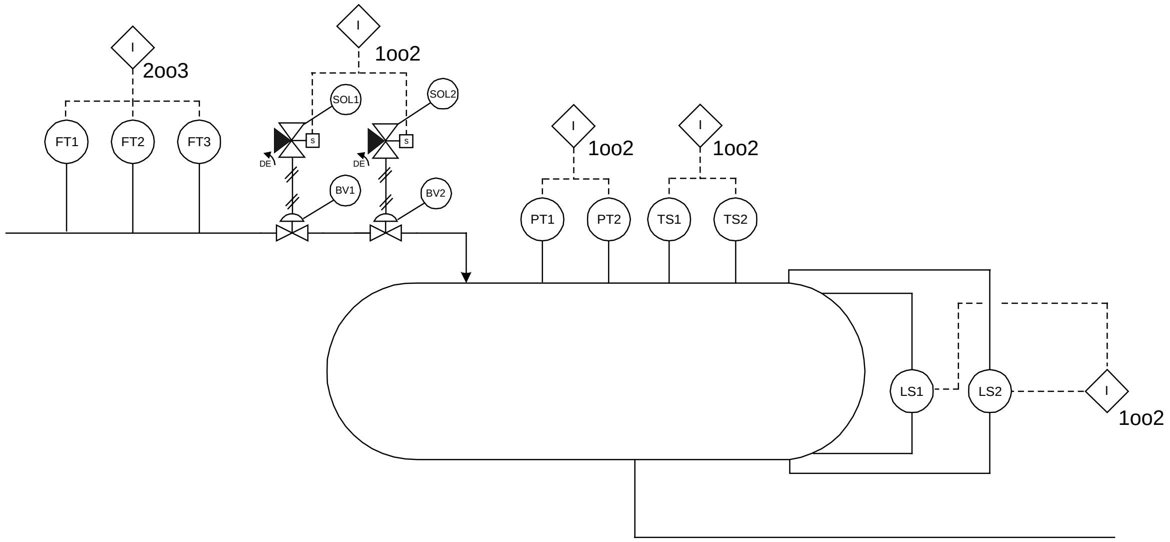


Figure 7.1 — Base case exam ple process diagram

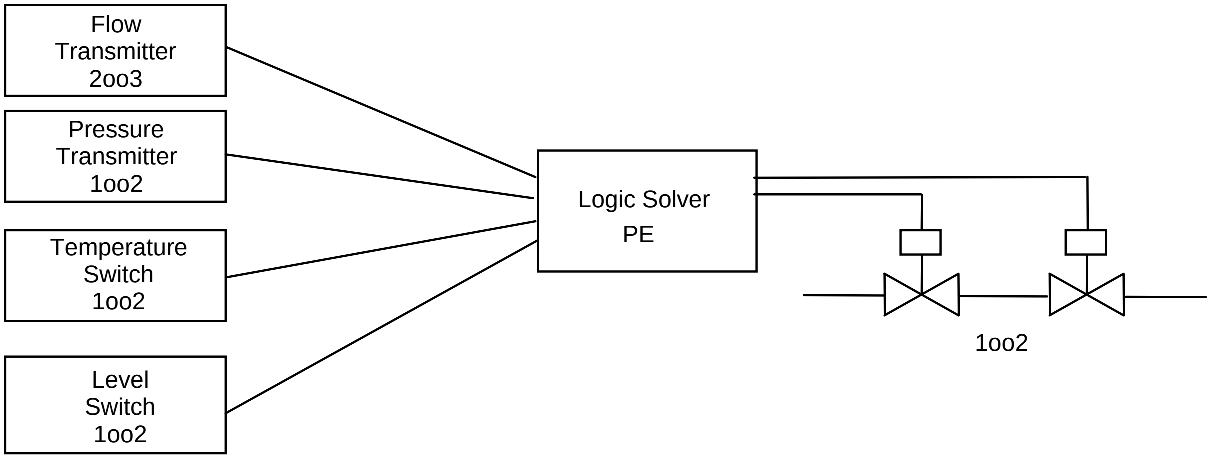


Figure 7.2 — Base case example SIF configuration

Table 7.1 — Data used in fault tree analysis

Devices	**MTTF^D** **(years)**	**MTTF^{spurious}** **(years)**
Flow Transmitters	40	20
Pressure Transmitters	50	25
Temperature Switch	15	5
Level Switch	25	10
Block Valves	50	25
Solenoid Valves	50	25

7.1.1 Determination of FTA logic and cut-sets

The SIF depicted in Figure 7.1 will fail on process demand if any of the following occurs:

- Any two of the three flow transmitters fail to detect the abnormal flow
- Both of the pressure transmitters fail to detect the high pressure
- Both of the temperature switches fail to detect the abnormal temperature
- Both of the level switches fail to detect the abnormal level
- Block valve 1 and block valve 2 fail to close
- Block valve 1 fails to close and solenoid valve 2 fails to vent

- Block valve 2 fails to close and solenoid valve 1 fails to vent
- Solenoid valve 1 and solenoid valve 2 fail to vent
- The logic solver fails to generate the correct outputs

The fault tree, which represents this failure logic, is shown in Figure 7.3.

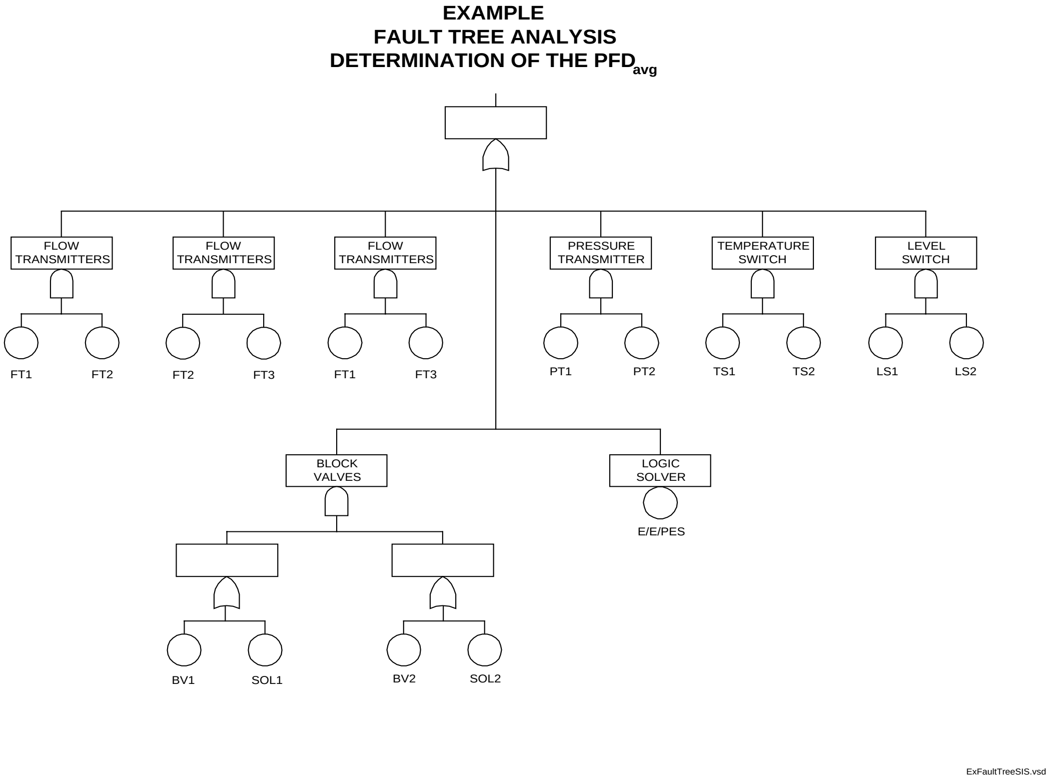


Figure 7.3 — Fault tree for the determination of PFD$_{avg}$

The minimal cut sets generated for the solution of this fault tree are shown in Table 7.2.

Table 7.2 — Fault tree cut sets

Cut set	Events
1	E/E/PES
2	TS1 and TS2
3	LS1 and LS2
4	FT1 and FT2
5	FT2 and FT3
6	FT1 and FT3
7	BV1 and BV2
8	BV1 and SOL1
9	BV2 and SOL2
10	SOL1 and SOL2
11	PT1 and PT2

7.1.2 Determination of PFDavg – Average before logic solution

For the quantification of the fault tree, the data in Table 7.1 is converted to a failure rate, λ, by

$$\lambda = 1/\text{MTTF}^D$$

Lambda is used with the testing interval for the components to determine the PFD_{avg} of the individual components.

Many FTA software programs allow the determination of the PFD_{avg} using the extended equation as provided in Equation B.27. Table 7.3 shows the values for λ and PFD_{avg}, calculated using extended equation.

Table 7.3 — Calculated data for each component

Devices	**MTTF^D** **(years)**	**Lambda** **(failures per year)**	**PFD$_{avg}$** $= 1+\dfrac{e^{-\lambda TI}-1}{\lambda TI}$
Flow Transmitters	40	0.025	1.26 x E-2
Pressure Transmitters	50	0.02	1.00 x E-2
Temperature Switch	15	0.067	3.26 x E-2
Level Switch	25	0.04	1.99 x E-2
Block Valves	50	0.02	1.00 x E-2
Solenoid Valves	50	0.02	1.00 x E-2

The logic shown in the fault tree determines how the PFD_{avg} of the individual components combine to determine the overall PFD_{avg}. The PFD_{avg} for each cut-set shown in Table 7.2 is determined as follows:

FT1 and FT2 = 0.0126 * 0.0126 = 1.59 x E-4

FT2 and FT3 = 0.0126 * 0.0126 = 1.59 x E-4

FT1 and FT3 = 0.0126 * 0.0126 = 1.59 x E-4

PT1 and PT2 = 0.01 * 0.01 = 1.00 x E-4

TS1 and TS2 = 0.0326 * 0.0326 = 1.06 x E-3

LS1 and LS2 = 0.0199 * 0.0199 = 3.95 x E-4

BV1 and BV2 = 0.01 * 0.01 = 1.00 x E-4

BV1 and SOL1 = 0.01 * 0.01 = 1.00 x E-4

BV2 and SOL1 = 0.01 * 0.01 = 1.00 x E-4

SOL1 and SOL2 = 0.01 * 0.01 = 1.00 x E-4

E/E/PES = 5 X E-3

Many FTA software programs use cut-set correction in the calculation of the results for the overall fault tree. This is performed using the following equation (generalized from Equation B.6 in Annex B), where $P_N(s)$ is the probability of success for the Nth cut-set:

$$PFD_{avg} = 1 - \prod_{1}^{N} (1 - P_N(s))$$

Therefore,

PFD_{avg} = 1-((1-1.59 x E-4)*(1-1.59 x E-4)*(1-1.59 x E-4)*(1-1.00 x E-4)*(1-1.06 x E-3)*(1-3.95 x E-4)*(1-1.00 x E-4)***(**1-1.00 x E-4)*(1-1.00 x E-4)*(1-1.00 x E-4)*(1-5.00 x E-3))

PFD_{avg} = 7.4 x E-3

Thus, the calculated PFD_{avg} is 7.4 x E-3. This is equivalent to SIL 2. The calculated PFD_{avg} should be compared to the target PFD_{avg} (SIL) specified in the SRS to ensure that the calculated PFD_{avg} for the SIF equals or exceed the target PFD_{avg}, as specified in the SRS.

The percent contribution of each cut set to the overall probability of failure on process demand can be calculated as follows:

$$\%\ \text{Contribution} = \frac{\text{Probability of Failure for the Cut Set}}{\sum \text{Probability of Failure for the Cut Sets}} \text{ x } 100$$

The percent contribution report for this example is shown in Table 7.4. If the SIF did not meet the target PFD_{avg}, the percent contribution report can be used to focus efforts for SIF modifications. This example shows that the logic solver contributes 67.6% to the overall PFD_{avg} for the SIF, while the temperature switches contribute 14.3%. Cases 7.2 and 7.3 illustrate techniques used to improve the PFD_{avg}.

Table 7.4 — Percent contribution to PFD_{avg} base case 7.1

Cut set	PFD_{avg} for the Cut sets	% Contribution to PFD_{avg}
E/E/PES	5.00 x E-3	67.6
TS1 and TS2	1.06 x E-3	14.3
LS1 and LS2	3.95 x E-4	5.3
FT1 and FT2	1.59 x E-4	2.1
FT2 and FT3	1.59 x E-4	2.1
FT1 and FT3	1.59 x E-4	2.1
BV1 and BV2	1.00 x E-4	1.3
BV1 and SOL1	1.00 x E-4	1.3
BV2 and SOL2	1.00 x E-4	1.3
SOL1 and SOL2	1.00 x E-4	1.3
PT1 and PT2	1.00 x E-4	1.3
PFD_{avg} 7.4 x E-3		

Alternatively, for hand calculations, Equation B.34 can be used to determine the PFD_{avg} for each component as shown in Table 7.5.

Table 7.5 — Calculated data for each component

Devices	$MTTF^D$ (years)	Lambda (failures per hour)	$PFD_{avg}=\lambda*TI/2$
Flow Transmitters	40	2.9 x E-6	1.25 x E-2
Pressure Transmitters	50	2.3 x E-6	1.00 x E-2
Temperature Switch	15	7.6 x E-6	3.33 x E-2
Level Switch	25	4.6 x E-6	2.00 x E-2
Block Valves	50	2.3 x E-6	1.00 x E-2
Solenoid Valves	50	2.3 x E-6	1.00 x E-2

FT1 and FT2 = 0.0125 * 0.0125 = 1.56 x E-4

FT2 and FT3 = 0.0125 * 0.0125 = 1.56 x E-4

FT1 and FT3 = 0.0125 * 0.0125 = 1.56 x E-4

PT1 and PT2 = 0.0100 * 0.0100 = 1.00 x E-4

TS1 and TS2 = 0.0333 * 0.0333 = 1.11 x E-3

LS1 and LS2 = 0.0200 * 0.0200 = 4.00 x E-4

BV1 and BV2 = 0.0100 * 0.0100 = 1.00 x E-4

BV1 and SOL1 = 0.0100 * 0.0100 = 1.00 x E-4

BV2 and SOL1 = 0.0100 * 0.0100 = 1.00 x E-4

SOL1 and SOL2 = 0.0100 * 0.0100 = 1.00 x E-4

E/E/PES = 5 X E-3

For hand calculations, the cut-set probabilities can be summed to yield conservative results.

PFD_{avg} = 1.56 x E-4 + 1.56 x E-4 + 1.56 x E-4 + 1.00 x E-4 + 1.11 x E-3 + 4.00 x E-4 + 1.00 x E-4 + 1.00 x E-4 + 1.00 x E-4 + 1.00 x E-4 + 5.00 x E-3

PFD_{avg} = 7.5 x E-3

Thus, the calculated PFD_{avg} is 7.5 x E-3. This is equivalent to SIL 2. Again, the calculated PFD_{avg} should be compared to the target PFD (SIL) specified in the SRS to ensure that the calculated PFD_{avg} for the SIS equals or exceed the target PFD_{avg}, as specified in the SRS.

7.1.3 Determination of PFD_{avg} – Average after logic solution

For the quantification of the fault tree, the data in Table 7.1 is converted to a failure rate, λ, by

$$\lambda = 1/MTTF^D$$

Lambda is used with the testing interval for the components to determine the PFD_{avg} of the individual components.

Table 7.6 shows the values used to calculate the Average After Logic solution. The left most column contains the time interval under consideration, and the column next to it contains the result of the fault tree for that time interval. The value in the Result column is calculated by using Equation B.6 with the eleven cut sets of the fault tree. The “Result” is calculated for each row, or time interval. The columns on the right side of the table contain the instantaneous PFD for each individual cut set for each time interval. The values calculated for each time interval were calculated using Equation B.18. The analysis shown in the table is performed for every one-hour interval of the 8760-hour (i.e., number of hours in one year) test interval under consideration. The final PFD_{avg} result is obtained by dividing the sum of all of the values in the Result column by the total number of time intervals considered, which is 8760.

Table 7.6 — Average after logic solution time series (excerpt)

Time	Result	1	2	3	4	5	6	7	8	9	10	11
0	0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0
1	1.14E-6	1.14E-6	5.79E-11	2.09E-11	8.14E-12	8.14E-12	8.14E-12	5.21E-12	5.21E-12	5.21E-12	5.21E-12	5.21E-12
2	2.28E-6	2.28E-6	2.32E-10	8.34E-11	3.26E-11	3.26E-11	3.26E-11	2.09E-11	2.09E-11	2.09E-11	2.09E-11	2.09E-11
…	…	…	…	…	…	…	…	…		…	…	
8758	1.97E-2	1.00E-2	4.44E-3	1.60E-3	6.25E-4	6.25E-4	6.25E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4
8759	1.97E-2	1.00E-2	4.44E-3	1.60E-3	6.25E-4	6.25E-4	6.25E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4
8760	1.98E-2	1.00E-2	4.44E-3	1.60E-3	6.25E-4	6.25E-4	6.25E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4	4.00E-4

The Average After Logic Solution for the fault tree yielded a PFD_{avg} of 8.3 x E-3. This is equivalent to SIL 2. The calculated PFD_{avg} should be compared to the target PFD_{avg} (SIL) specified in the SRS to ensure that the calculated PFD_{avg} for the SIF equals or exceed the target PFD_{avg}, as specified in the SRS.

7.1.4 Determination of $MTTF^{spurious}$

The SIF depicted in Figure 7.1 will spurious trip if any of the following occurs:

- Any two of the three flow transmitters fail such that the trip flow is transmitted.
- Either of the pressure transmitters fail, such that the trip pressure is transmitted.
- Either of the temperature switches fail, such that the trip temperature is transmitted.
- Either of the level switches fail, such that the trip level is transmitted.
- Block valve 1 or solenoid valve 1 fail, such that the valve closes.
- Block valve 2 or solenoid valve 2 fail, such that the valve closes.

- Electrical power fails, such that the final elements are de-energized.
- The logic solver fails, such that either valve closes.

The fault tree, which represents this failure logic, is shown in Figure 7.4.

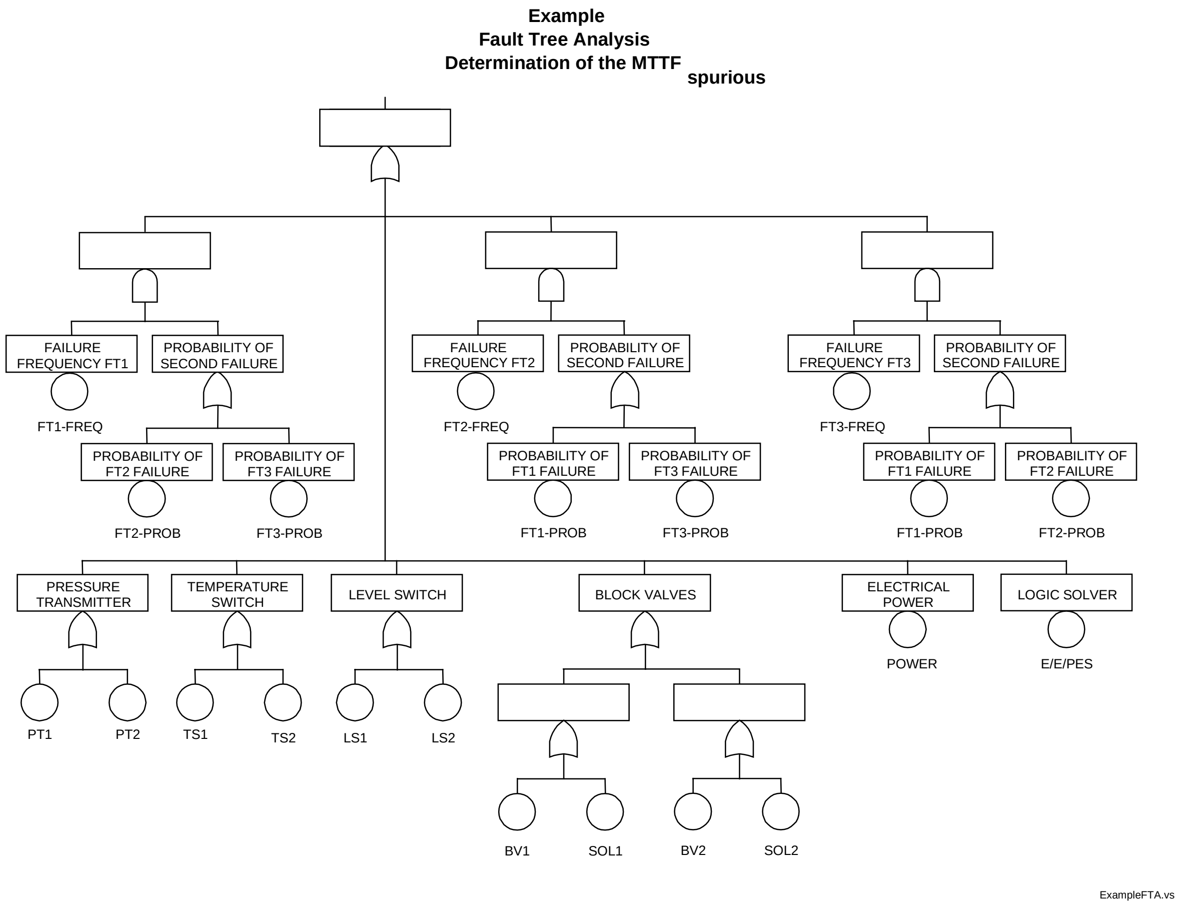


Figure 7.4 — Fault tree for the determination of MTTF^{spurious}

As in the PFD$_{avg}$ calculation, the fault tree analysis software, IRRAS[(8)], was used to determine the minimal cut sets and to perform the Boolean algebra for quantification of the cut sets. As with many FTA software programs, this program uses cut-set correction in the calculation of the results for the overall fault tree. This is performed using the following equation, where $F_N(s)$ is the frequency of success for the Nth cut-set:

$$STR_{SIF} = 1 - \prod_{1}^{N} (1 - F_N(s))$$

The calculated STR$_{SIF}$ is 0.65 per year. The MTTF^{spurious} is, therefore, 1.5 years. This MTTF^{spurious} calculation is also valid for Cases 7.2 and 7.3.

The percent contribution of each cut set can be calculated for the spurious trip rate. The percent contribution shown in Table 7.7 can be used to focus efforts for SIF modifications to reduce the spurious trip rate similar to the procedure for improving the PFD$_{avg}$ as described in Section 6.2.

Table 7.7 — Percent contribution to MTTF^{spurious}

Cut set	STR$_{SIF}$ for the Cut sets	% Contribution to STR$_{SIF}$
TS1	0.2	19.9
TS2	0.2	19.9
E/E/PES	0.1	10.0
LS1	0.1	10.0
LS2	0.1	10.0
POWER	0.05	5.0
SOL1	0.04	4.0
SOL2	0.04	4.0
PT1	0.04	4.0
PT2	0.04	4.0
BV1	0.04	4.0
BV2	0.04	4.0
FT1-FREQ and FT2-PROB	6.85 x E-6	0.2
FT1-FREQ and FT3-PROB	6.85 x E-6	0.2
FT2-FREQ and FT2-PROB	6.85 x E-6	0.2
FT2-FREQ and FT3-PROB	6.85 x E-6	0.2
FT3-FREQ and FT1-PROB	6.85 x E-6	0.2
FT3-FREQ and FT2-PROB	6.85 x E-6	0.2
STR$_{SIF}$ = 0.65 per year or MTTF^{spurious} = 1.5 years		

NOTE The STR$_{SIF}$ in Table 7.7 was calculated using cut-set correction. The STR$_{SIF}$ would have been 0.99 per year without the cut-set correction. Part 2, which does not use cut-set correction, also calculated 0.99 per year. This results in a conservative estimate of the STR$_{SIF}$.

7.2 Case 7.2 PFD$_{avg}$ calculation (more frequent functional test interval)

Step 5 of the FTA methodology (Part 3 Clause 6) provides a list of typical risk reduction techniques. To lower the PFD$_{avg}$ of the SIF, various SIF components could be tested more frequently. For instance, the temperature switches could be tested every 3 months rather than once per year.

When the higher testing frequency is used to calculate the failure rate for the temperature switches, the PFD$_{avg}$ for the SIF decreases to 6.4 x E-3 using the Average Before Logic solution. The percent contribution report would change as shown in Table 7.8. The temperature switches drop from the highest contributor to PFD$_{avg}$ to the lowest.

7.3 Case 7.3 PFD_{avg} calculation (logic solver with higher $MTTF^D$)

As an alternative to modification of the testing frequency, the evaluation could also examine the degree of improvement that could be obtained by replacing the SIF components with components that have a higher $MTTF^D$. For example, the E/E/PES logic solver used in the example had a PFD of 0.005. If the logic solver was replaced with one that had a PFD of 0.0005, the PFD_{avg} for the SIF decreases to 2.9 x E-3 using the Average Before Logic solution. The percent contribution report would change as shown in Table 7.9.

There are many combinations of the risk reduction techniques (Part 3 Clause 5) that could be used to improve the PFD_{avg}. This example only provides two possible modifications that could be made to the SIF to improve the PFD_{avg}. The choice of these two possible modifications does not indicate an order of preference for the selection of the risk reduction technique. The risk reduction techniques should be used as necessary to improve the PFD_{avg} within the constraints of the process design and the concurrence of the process hazard analysis team.

Table 7.8 — Case 7.2 percent contribution to PFD_{avg} (temperature switches tested every 3 months instead of annually)

Cut set	PFD_{avg} for the Cut sets	% Contribution to PFD_{avg}
E/E/PES	5.00 x E-3	78.2
LS1 and LS2	3.95 x E-4	6.1
FT1 and FT2	1.59 x E-4	2.4
FT2 and FT3	1.59 x E-4	2.4
FT1 and FT3	1.59 x E-4	2.4
BV1 and BV2	1.00 x E-4	1.5
BV1 and SOL1	1.00 x E-4	1.5
BV2 and SOL2	1.00 x E-4	1.5
SOL1 and SOL2	1.00 x E-4	1.5
PT1 and PT2	1.00 x E-4	1.5
TS1 and TS2	6.68 x E-5	1.0
PFD_{avg} 6.4 x E-3		

NOTE The PFD_{avg} in Table 7.8 was calculated using Average Before Logic and the cut-set correction

Table 7.9 — Case 7.3 percent contribution to PFD$_{avg}$ (logic solver with higher MTTFD)

Cut set	PFD$_{avg}$ for the Cut sets	% Contribution to PFD$_{avg}$
TS1 and TS2	1.06 x E-3	36.2
E/E/PES	5.00 x E-4	17.1
LS1 and LS2	3.95 x E-4	13.5
FT1 and FT2	1.59 x E-4	5.4
FT2 and FT3	1.59 x E-4	5.4
FT1 and FT3	1.59 x E-4	5.4
BV1 and BV2	1.00 x E-4	3.4
BV1 and SOL1	1.00 x E-4	3.4
BV2 and SOL2	1.00 x E-4	3.4
SOL1 and SOL2	1.00 x E-4	3.4
PT1 and PT2	1.00 x E-4	3.4
PFD$_{avg}$ 2.9 x E-3		

NOTE The PFD$_{avg}$ in Table 7.9 was calculated using Average Before Logic and the cut-set correction

8 Example FTA calculations for an SIF including common cause and systematic failure

This section presents two cases to illustrate modeling of common cause failures and systematic failures.

- Case 8.1 illustrates the effect of common cause failures and systematic failures on the SIF PFD$_{avg}$.
- Case 8.2 shows the application of a procedural safeguard to the common cause and systematic failure illustrated in Case 8.1.

The PFD$_{avg}$ calculation provided in this Clause is for illustrative purposes only and should not be used for actual evaluation of a specific SIF.

8.1 Case 8.1: SIF with incorrect transmitter calibration

The fault tree shown in Figure 8.1 illustrates the addition of a common cause failure and systematic failure to the example SIF modeled in Clause 7.

The random hardware failure for the two pressure transmitters was modeled by the “AND” relationship in the fault tree. A potential common cause failure and systematic failure associated with this set of transmitters would be the potential miscalibration of the transmitters during the annual test. The fault tree can be modified to include this potential common cause failure and systematic failure and is shown in Figure 8.1.

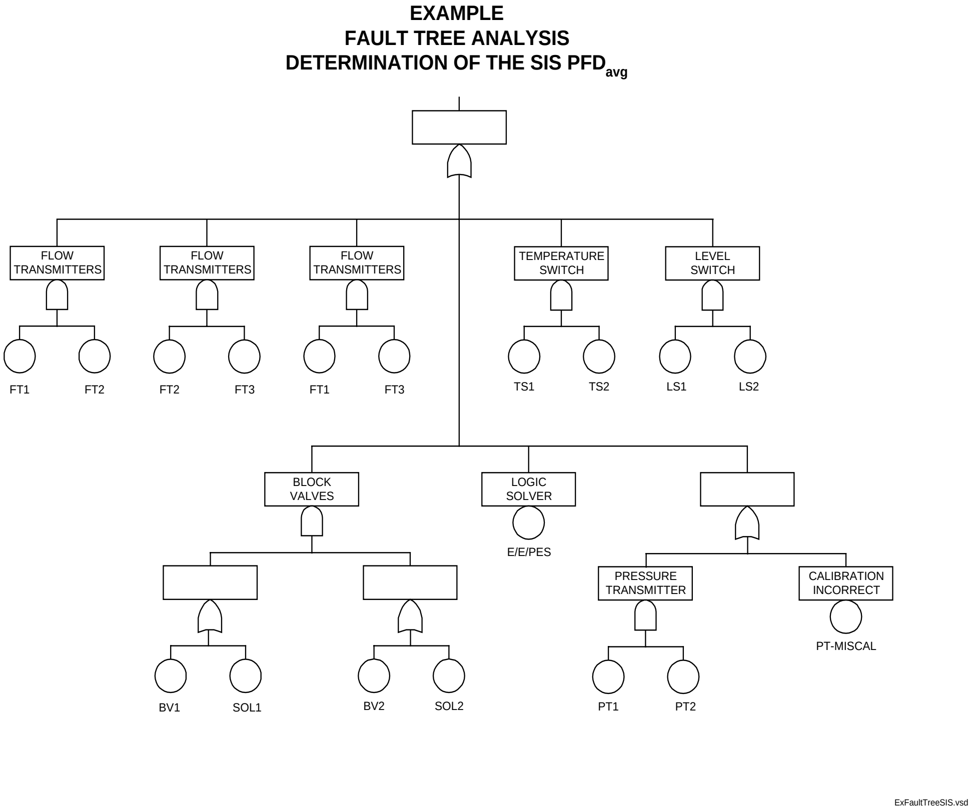


Figure 8.1 — Fault tree for the determination of PFD$_{avg}$ transmitter miscalibrated

The PFD$_{avg}$ for this fault tree can be calculated by making the same assumptions utilized in the example calculation of Part 3 Clause 6.3 and assuming a miscalibration occurrence of 1 in 100 calibrations. The PFD$_{avg}$ is calculated using the Average Before Logic solution. The percent contribution of the basic events to the SIF PFD$_{avg}$ is shown in Table 8.1.

Table 8.1 — Case 8.1 percent contribution to PFD_{avg} transmitter miscalibrated

Cut set	PFD_{avg} for the Cut sets	% Contribution to PFD_{avg}
PT-MISCAL	1.00 x E-2	57.7
E/E/PES	5.00 x E-3	28.8
TS1 and TS2	1.06 x E-3	6.1
LS1 and LS2	3.95 x E-4	2.2
FT1 and FT2	1.59 x E-4	0.9
FT2 and FT3	1.59 x E-4	0.9
FT1 and FT3	1.59 x E-4	0.9
BV1 and BV2	1.00 x E-4	0.5
BV1 and SOL1	1.00 x E-4	0.5
BV2 and SOL2	1.00 x E-4	0.5
SOL1 and SOL2	1.00 x E-4	0.5
PT1 and PT2	1.00 x E-4	0.5
PFD_{avg} 1.7 x E-2		

NOTE The PFD_{avg} in Table 8.1 was calculated using Average Before Logic and the cut-set correction.

For additional information on how to estimate human reliability, refer to NUREG/DR-1278-F, “Handbook of Human Reliability Analysis for Emphasis on Nuclear Power Plant Applications,” Swain & Guttermann, 1983.

The PFD_{avg} calculated by the fault tree would deteriorate substantially from 7.4 x E-3 for perfect calibration (Case 7.1) to 1.7 x E-2 (shown above). The potential for pressure transmitter miscalibration is now the greatest contributor to the SIF PFD_{avg}. The SIF does not meet the required SIL.

8.2 Case 8.2: SIF with incorrect transmitter calibration with procedural safeguard

Since the SIF in Case 8.1 does not meet requirements, the effect of the miscalibration of the pressure transmitters must be reduced.

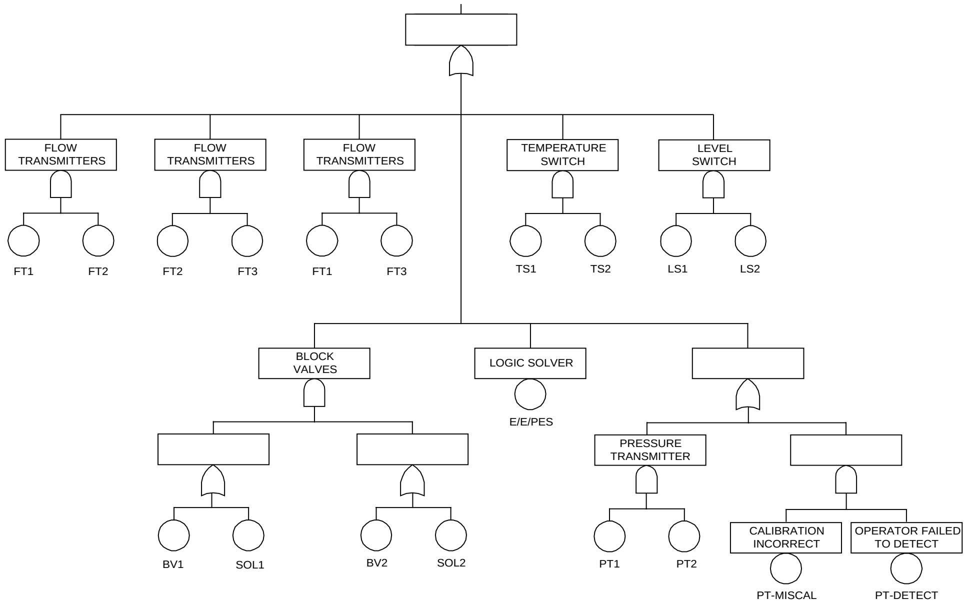
After review with the process hazard analysis team, it was determined that procedures can be written and personnel trained to verify that the pressure transmitter readings are within the expected operating range after calibration. Administrative or operation/maintenance procedures should also be adopted that would require that the operator/maintenance personnel respond promptly to the perceived incorrect reading by testing and re-calibrating.

The failure of the procedures and personnel could be modeled as separate failures or as a single basic event. For the purpose of this example, a single basic event will be modeled. The probability of not detecting the miscalibrated transmitter will be assumed to be 1 in 100. The fault tree shown in Figure 8.2 shows that the transmitters must be miscalibrated “AND” the detection of the miscalibrated transmitter has to fail in order for the SIF to fail on demand.

The PFD_{avg} is calculated using the Average Before Logic solution and is determined to be 7.5 x E-3. The SIF does meet the required SIL.

The percent contribution report for this fault tree is shown in Table 8.2. The miscalibrated transmitter was the largest contributor to PFD_{avg} in Case 8.1. Now, in Case 8.2, the miscalibration “AND” the failure to detect is a small contributor to the PFD_{avg}.

EXAMPLE
FAULT TREE ANALYSIS
DETERMINATION OF THE SIS PFD$_{avg}$



ExFaultTreeSIS1.vsd

Figure 8.2 — Case 8.2 fault tree for the determination of PFD$_{avg}$ transmitter calibration with procedural safeguard

Table 8.2 — Percent contribution to PFD_{avg}

Cut set	PFD_{avg} for the Cut sets	% Contribution to PFD_{avg}
E/E/PES	5.00 x E-3	66.6
TS1 and TS2	1.06 x E-3	14.1
LS1 and LS2	3.95 x E-4	5.2
FT1 and FT2	1.59 x E-4	2.1
FT2 and FT3	1.59 x E-4	2.1
FT1 and FT3	1.59 x E-4	2.1
BV1 and BV2	1.00 x E-4	1.3
BV1 and SOL1	1.00 x E-4	1.3
BV2 and SOL2	1.00 x E-4	1.3
SOL1 and SOL2	1.00 x E-4	1.3
PT1 and PT2	1.00 x E-4	1.3
PT-MISCAL and PT-DETECT	1.00 x E-4	1.3
PFD_{avg} 7.5 x E-3		

NOTE The PFD_{avg} in Table 8.2 was calculated using Average Before Logic and the cut-set correction.

This page intentionally left blank.

Annex A (informative) — Fault tree symbols and logic

This Annex shows examples of symbols typically used in Fault Tree Analysis[6,7,8] (Figure A.1) followed by a brief description.

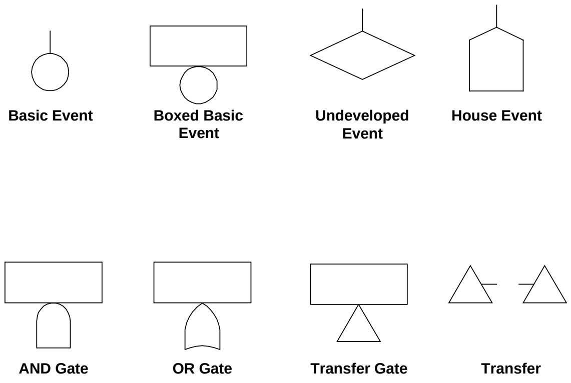


Figure A.1 — Examples of fault tree symbols

Each Fault Tree symbol represents specific logic:

A basic event is the limit to which the failure logic can be resolved. A basic event must have sufficient definition for determination of appropriate failure rate data and equation.

A boxed basic event is the same as a basic event. The box allows a text description to be placed above the basic event.

Undeveloped events are events that could be broken down into sub-components, but, for the purposes of the model under development, is not broken down further. An example of an undeveloped events may be the failure of the instrument air supply. An undeveloped event symbol and a single failure rate can be used to model the instrument air supply rather than model all of the components. FTA treats undeveloped events in the same way as basic events.

House events are events that are guaranteed to occur or guaranteed not to occur. House events are typically used when modeling SIF with sequential events or when operator action or inaction results in SIF failure (for example, over-rides).

“AND” gates are used to define a set of conditions or causes in which all the events in the set must be present for the gate event to occur. The set of events under an “AND” gate must meet the test of “necessary” and “sufficient."

“Necessary” means each cause listed in a set is required for the event above it to occur; if a “necessary” cause is omitted from a set, the event above will not occur.

“Sufficient” means the event above will occur if the set of causes is present; no other causes or conditions are needed.

“OR” gates define a set of events in which any one of the events in the set, by itself, can cause the gate event. The set of events under an “OR” gate must meet the test of “sufficient."

Transfer gates are used to relate multiple fault trees. The right or left transfer gates associate the results of the fault tree with a “transfer in” gate on another fault tree.

Annex B (informative) — Mathematics

This Annex provides a brief overview of the mathematics and equations used in fault tree analysis. The calculation of PFD_{avg} and $MTTF^{spurious}$ by fault tree analysis requires an understanding of set mathematics and Boolean algebra[6,8].

B.1 provides a brief introduction to the mathematical concepts that must be applied to the calculations. Furthermore, the equations used for the PFD_{avg} and $MTTF^{spurious}$ calculations are very important and warrant some explanation.

B.2 lists equations that can be used for modeling PFD_{avg}.

B.3 lists equations that can be used for modeling $MTTF^{spurious}$.

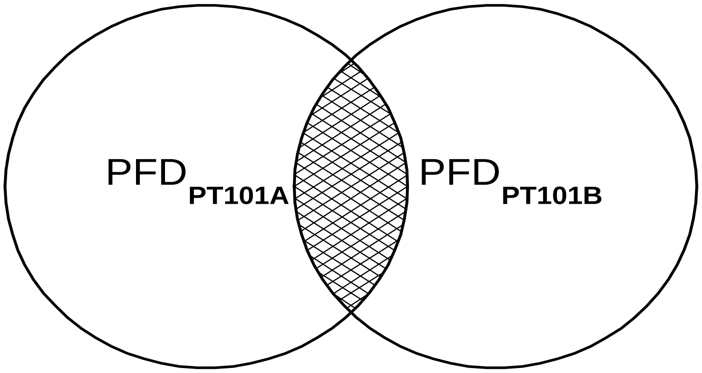
B.1 Fault tree mathematics

To understand the quantification of the fault trees, it is necessary to review some basic concepts of set mathematics, including Venn diagrams. B.1 will present the mathematics using the PFD_{avg} calculation as an example, but the mathematical relationships are also used for the $MTTF^{spurious}$ calculation. A fault tree is composed of basic events, which represent the failure logic for the SIF. The basic event probabilities are calculated using the equations that were listed above. These basic event probabilities are used to quantify the overall tree by following the logical relationships defined by the structure of the fault tree. The mathematics used to define the logical relationships is called Boolean after the mathematician George Boole.

B.1.1 “AND” gates

Consider two transmitters, PT101A and PT101B. If these two transmitters are voted 1oo2, the fault tree for the probability of failure of the sensor system would show that both components, PT101A “AND” PT101B, must fail in order for the trip to not occur.

For the two independent events, PT101A and PT101B, with a failure on demand probabilities of PFD_{PT101A} and PFD_{PT101B}, respectively, the failure on demand probability for the intersection of PT101A and PT101B can be represented in Venn diagram format as shown in Figure B.1.



Shaded Area Represents the Intersection of
PFD_{PT101A} AND PFD_{PT101B}

Figure B.1 — Intersection of PFD_{PT101A} and PFD_{PT101B}

The set logic for this intersection is

(Eq. B.1) $PFD_{PT101A} \cap PFD_{PT101B}$

The PFD for the intersection is calculated as

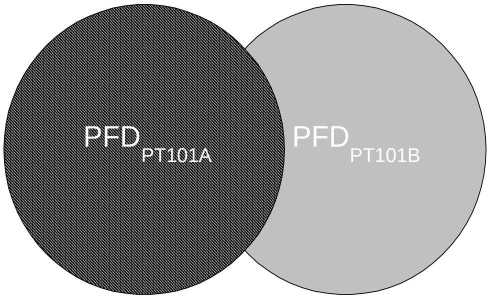
(Eq. B.2) $PFD_{PT101A \text{ and } PT101B} = PFD_{PT101A} * PFD_{PT101B}$

This can be generalized for N basic events as

(Eq. B.3) $PFD_{all} = PFD_1 * PFD_2 * PFD_3 \ldots. PFD_N$

B.1.2 “OR” gates

For 2oo2 voting transmitters, the failure logic of the transmitters would be PT101A “OR” PT101B, since the failure on demand of either transmitter results in a failure of the SIF. The logical relationship shows that the failure of only one of the transmitters is required to cause the SIF to trip. For the independent events, PT101A and PT101B, with PFD of PFD_{PT101A} and PFD_{PT101B}, respectively, the PFD for PT101A “OR” PT101B can be represented in Venn diagram format as shown in Figure B.2.



The total shaded area represents the union of PFD_{PT101A} and PFD_{PT101B}

Figure B.2 — The union of PF D_{PT101A} and PFD_{PT101B}

The set logic is

(Eq. B.4) $PFD_{PT101A} \cup PFD_{PT101B}$

This union is calculated as

(Eq. B.5) $PFD_{PT101A\ or\ PT101B} = PFD_{PT101A} + PFD_{PT101B} – (PFD_{PT101A} \ast PFD_{PT101B})$

This can be generalized for N basic events as

(Eq. B.6)

$PFD_{all} = PFD_1 + PFD_2 + PFD_3 + \ldots PFD_N - (PFD_1 \ast PFD_2) -$

$(PFD_1 \ast PFD_3) - \ldots (PFD_{N-1} \ast PFD_N) + (PFD_1 \ast PFD_2 \ast PFD_3) +$

$(PFD_1 \ast PFD_2 \ast PFD_4) + (PFD_{N-2} \ast PFD_{N-1} \ast PFD_N) + \ldots$

$(-1)^{N-1}(PFD_1 \ast PFD_2 \ast \ldots PFD_N)$

A cut set is a combination of basic events that give rise to the Top Event, that is, when the failure of the basic events in the cut set occurs, the Top Event will occur. When the fault tree is quantified, the cut set report is created which identifies all of the logical combinations (or intersections) of basic events that can cause the Top Event to occur.

Sometimes in complex SIFs, it is necessary to define the minimal cut sets. A minimum cut set is one that does not contain within itself another cut set. The mathematical technique for conducting the minimal cut set determination is called Boolean reduction, and it is performed to simplify the cut sets and remove redundant cut sets. Consider basic events, A, B, and C. If $A \cap B \cap C$ and $A \cap B$ are both cut sets, the minimal cut set is $A \cap B$. Thus, $A \cap B \cap C$ can be eliminated as a cut set.

B.2 PFD$_{avg}$ equations

This section presents the equations for obtaining the instantaneous PFD and the PFD$_{avg}$. The PFD$_{avg}$ equation is developed using Average Before Logic and Average After Logic solution techniques. Failure rate data for each basic event is used to quantify the PFD$_{avg}$ for the top event for the fault tree. There are many equations commonly used in fault tree analysis. A more thorough discussion of PFD calculation methodologies and equations can be found in *Probabilistic Risk Assessment*[(2)].

When software is utilized for the FTA calculation, the User is cautioned to understand the equations, mathematics, and any simplifying assumptions, restrictions, or limitations used in the software.

The equations for PFD can be derived by examining the transition of the component from the working state to the failed state. For standby equipment, there are only two states as shown in Figure B.3. State 1 represents the state where the component is available to perform its function. State 2 represents the state where the component is not available to perform its function. The transition between State 1 and State 2 is the product of the failure rate of the component and the time Δt.

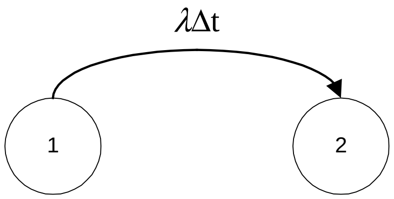


Figure B.3 — Representation of the states of a device

The probability of the component being in State 1 can be derived as follows:

(Eq. B.7) $$P_1(t+\Delta t) = P_1(t) - \lambda P_1(t)\Delta t$$

Rearranging,

(Eq. B.8) $$\frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} = -\lambda P_1(t)$$

Taking the limit as $\Delta t \to 0$

(Eq. B.9) $$\lim_{\Delta t \to 0} \frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} = -\lambda P_1(t)$$

(Eq. B.10) $$\frac{dP_1(t)}{dt} = -\lambda P_1(t)$$

Using the Laplace transform, the equation for $dP_1(t)/dt$ can be restated as:

(Eq. B.11) $$\frac{dP_1(t)}{dt} = sP_1(s) - P(0)$$

(Eq. B.12) $$sP_1(s) - P_1(0) = -\lambda P_1(s)$$

At the initial condition, t = 0, $P_1(0) = 1$. Therefore,

(Eq. B.13) $$sP_1(s) - 1 = -\lambda P_1(s)$$

Rearranging and solving for $P_1(s)$

(Eq. B.14) $$P_1(s) = \frac{1}{s+\lambda}$$

To convert from Laplace domain to time domain, the following functions are used:

(Eq. B.15) $$f(s) = \frac{1}{s-a}$$

(Eq. B.16) $$f(t) = e^{at}$$

Therefore, in the time domain, the probability of the component being in State 1 at any time t can be shown as

(Eq. B.17) $$P_1(t) = e^{-\lambda t}$$

For the evaluation of a SIF, the SIL is related to the probability of the component being in State 2, the unavailable state, where $P_2(t) = 1 - P_1(t)$.

(Eq. B.18) $$P_2(t) = PFD(t) = 1 - e^{-\lambda t}$$

NOTE Equation B.18 is the instantaneous PFD as a function of any selected time.

$$PFD(t) = 1 - e^{-\lambda t}$$

Sometimes, this equation is shown in its “rare event” form, which is applicable when λ t < 0.1. To determine the rare event form of the equation, the exponential series expansion is used for the exponential term,

(Eq. B.19) $$e^{-\lambda t} = 1 - \lambda t + \frac{\lambda^2 t^2}{2} - \frac{\lambda^3 t^3}{6} + \frac{\lambda^4 t^4}{24} - \ . \ . \ .$$

(Eq. B.20) $$PFD(t) = 1 - \left(1 - \lambda t + \frac{\lambda^2 t^2}{2} - \frac{\lambda^3 t^3}{6} + \ldots\right)$$

(Eq. B.21) $$PFD(t) = \lambda t - \frac{\lambda^2 t^2}{2} + \frac{\lambda^3 t^3}{6} - \ldots$$

When the “rare event” assumption is valid, the second order and higher terms become very small and can be neglected. In practice, the “rare event” approximation provides good results for most SIFs when $\lambda t < 0.1$. The instantaneous PFD can then be calculated as

(Eq. B.22) $$PFD(t) = \lambda t$$

> NOTE Equation B.22 is the rare event approximation of the instantaneous PFD as a function of any selected time.
>
> $$PFD(t) = \lambda t$$

To calculate the average PFD, the instantaneous PFD must be averaged over a defined time interval. For safety instrumented system evaluations, this time interval is the proof testing interval. The equation for PFD$_{avg}$ is derived by integrating the PFD(t) from time 0 to the testing interval, TI, assuming TI>>MTTR, and dividing by the test interval.

(Eq. B.23) $$PFD_{avg} = \frac{1}{TI}\int_0^{TI} 1 - e^{-\lambda t}dt$$

Integrating the terms,

(Eq. B.24) $$PFD_{avg} = \frac{1}{TI}\left(t - \frac{e^{-\lambda t}}{-\lambda}\right)\begin{matrix} TI \\ 0 \end{matrix}$$

Substituting the bounds of the integration,

(Eq. B.25) $$PFD_{avg} = \frac{1}{TI}\left[(TI - 0) + \left(\frac{e^{-\lambda TI} - e^{-\lambda(0)}}{\lambda}\right)\right]$$

Rearranging,

(Eq. B.26) $$PFD_{avg} = \frac{1}{TI}\left[TI + \left(\frac{e^{-\lambda TI} - 1}{\lambda}\right)\right]$$

This results in one of the most common forms of the PFD$_{avg}$ equation, describing standby components, such as those used in safety instrumented functions.

(Eq. B.27) $$PFD_{avg} = 1 + \frac{e^{-\lambda TI} - 1}{\lambda TI}$$

NOTE Equation B.27 is equation for the Average Probability to Fail on Demand for a Basic Event at the defined Testing Interval (TI).

$$PFD_{avg} = 1 + \frac{e^{-\lambda TI} - 1}{\lambda TI}$$

Sometimes, the rare event equation is used for the PFD$_{avg}$. As shown previously, the exponential series expansion is used for the exponential term:

(Eq. B.28) $$e^{-\lambda t} = 1 - \lambda t + \frac{\lambda^2 t^2}{2} - \frac{\lambda^3 t^3}{6} + \frac{\lambda^4 t^4}{24} - ...$$

(Eq. B.29) $$1 - e^{-\lambda t} = 1 - \left[1 - \lambda t + \frac{\lambda^2 t^2}{2} - \frac{\lambda^3 t^3}{6} + \frac{\lambda^4 t^4}{24} - ...\right]$$

(Eq. 30) $$PFD_{avg} = \frac{1}{TI}\int_0^{TI} \left[\lambda t - \frac{\lambda^2 t^2}{2} + \frac{\lambda^3 t^3}{6} - \frac{\lambda^4 t^4}{24} + ...\right]dt$$

(Eq. B.31) $$PFD_{avg} = \frac{1}{TI}\left[\frac{\lambda t^2}{2} - \frac{\lambda^2 t^3}{6} + \frac{\lambda^3 t^4}{24} - ...\right]\Big|_0^{TI}$$

Substituting the bounds of the integration,

(Eq. B.32) $$PFD_{avg} = \frac{1}{TI}\left[\frac{\lambda\left(TI^2 - 0^2\right)}{2} - \frac{\lambda^2\left(TI^3 - 0^3\right)}{6} + \frac{\lambda^3\left(TI^4 - 0^4\right)}{24} - ...\right]$$

For $\lambda TI < 0.1$, the third order and higher terms may be neglected. The rare event equation can be shown as

(Eq. B.33) $$PFD_{avg} = \frac{1}{TI}\left[\frac{\lambda TI^2}{2}\right]$$

(Eq. B.34) $$PFD_{avg} = \frac{\lambda TI}{2}$$

NOTE Equation B.34 is the rare event approximation for the Average Probability to Fail on Demand for a Basic Event at the defined Testing Interval (TI).

$$PFD_{avg} = \frac{\lambda TI}{2}$$

There are failures that occur in the SIF that cannot be readily described by the average PFD equations. For these failures, the PFD$_{avg}$ for components may be entered directly into the model as the PFD$_{avg.}$ This relationship can be shown in the fault tree as an undeveloped event. For example, SIFs that require operator intervention, the probability that an operator will not acknowledge an alarm must be included in the fault tree. The potential failure of the operator cannot be tested or repaired. A probability must be estimated for the operator and this is simply entered into the model as the average probability of failure on process demand.

The most common examples of events that will be used as a undeveloped event are as follows:

- Logic solvers
- Subsystems, such as cooling water, power, steam, hydraulic oil, and instrument air, and
- Human errors

B.2.1 Alternate methods for solving for the top event

The probability of the top event of a fault tree is obtained by combining the basic event probabilities using the probability math functions described in Annex B.1. The “logic” that a particular fault tree represents is a mathematical function that relates the input vector (i.e., the basic events) to the output (i.e., top event probability). PFD_{avg} reflects an average top event value over a time interval that is represented by the SIF’s test interval (TI). Calculating PFD_{avg} can be done in one of three ways, 1) Average Before Logic - Approximation, 2) Average After Logic – Symbolic Integration, 3) Average After Logic – Numerical Integration.

The Average Before Logic - Approximation is by far the most common method for solving for fault tree top event probability. This method’s popularity stems from its ease of use compared to the other methods. When using the Average Before Logic - Approximation, the PFD_{avg} of each individual component is calculated (using Equation B.27 or B.34) and used as the input to the fault tree logic function. The fault tree logic function is the probability addition (using Equation B.6) of the fault tree’s minimal cut sets. The fault tree logic function is only performed once using the average basic events as inputs. The resulting top event is a reasonable approximation of the PFD_{avg} of the system.

While the Average Before Logic - Approximation is the most popular method, it is only an approximation. The objective of the SIL verification process is to obtain a PFD_{avg} for the entire system, which is different from fault tree logic applied to average inputs if the function is non-linear (such as the function that results from a fault tree AND gate. Consider the non-linear function shown below.

(Eq. B.35) $$f(x) = x^2$$

For an input vector of three numbers, it can be shown by example that the average of the outputs of the function does not equal the output of the average of the inputs. As an example, consider an input vector X=<1,2,3>. If the vector X is input and the average is calculated after the function the result is 7, if the average is taken before the function, the result will be 4. It can be shown that for all non-linear functions averaging before the function will result in a different answer then averaging after the function. Since the desired result of SIF analysis is the PFD_{avg} of the overall system, the logic should be performed before averaging.

Average before function

(Eq. B.36) $$f(\overline{X}) = \left(\frac{1+2+3}{3}\right)^2 = 4.00$$

Average after function

(Eq. B.37) $$\overline{f(X)} = (\frac{1^2+2^2+3^2}{3}) = 4.67$$

While Average After Logic methods, both Symbolic and Numerical, provide more accurate results, they are rarely used in practice due to the increased effort and the acceptability of the error in Average Before Logic results to many analysts.

Solving for the PFDavg of a SIF using Average After Logic – Symbolic Integration requires the analyst to convert the logic being performed by the fault tree and the basic events into an equation. This equation is then symbolically integrated over the test interval to determine the equation for PFD_{avg} of the system using the same process that was used to develop Equation B.27 from Equation B.23. In practice, the symbolic integration method is never used because it is very cumbersome, and can only be done for very small and simple fault trees.

When the accuracy of Average After Logic is desired, results are usually obtained using Numerical Integration techniques. The Average After Logic – Numerical Integration technique is performed by solving the fault tree logic function for a large number of discrete time intervals and then averaging the results. As with Average Before Logic, the fault tree logic function is the probability addition (using Equation B.6) of the fault tree's minimal cut sets. In this case, each of the basic event probabilities is re-calculated for each discrete time interval using the instantaneous PFD formula (either B.18 or B.22). If a sufficient number of discrete time intervals are used, Numerical Integration and Symbolic Integration results will be identical.

Table B.1 provides a comparison of fault trees for small sub-systems of SIF being solved using both the Average Before Logic and Average After Logic methods. This table is presented to give the User an overview of the magnitudes of error that are possible for various typical SIF architectures. The difference between Average Before Logic and Average After Logic can become quite pronounced as the function becomes more non-linear. For example, the difference between Average Before Logic and Average After Logic is a factor of 4/3 for the 1oo2 configuration (i.e., 33% error in the non-conservative direction). This difference varies depending on the architecture or voting configuration. Although the table shows results calculated using Average After Logic - Symbolic Integration, identical results would be obtained using Numerical Integration.

Table B.1 — PFD$_{avg}$ comparison of average before logic and average after logic

Architecture (Voting Configuration)	Average Before Logic		Average After Logic		% Difference
	PFD$_{avg}$ Equation	PFD$_{avg}$ Value Obtained *	PFD$_{avg}$ Equation	PFD$_{avg}$ Value Obtained *	Between PFD$_{AVG}$ Results - Average After Logic Versus Average Before Logic
1oo1	$\frac{\lambda(TI)}{2}$	4.38 x E-2	$\frac{\lambda(TI)}{2}$	4.38 x E-2	0
1oo2	$\frac{\lambda^2(TI)^2}{4}$	1.92 X E-3	$\frac{\lambda^2(TI)^2}{3}$	2.56 X E-3	33
2oo2	$\lambda(TI)$	8.76 X E-2	$\lambda(TI)$	8.76 X E-2	0
1oo3	$\frac{\lambda^3(TI)^3}{8}$	8.40 X E-5	$\frac{\lambda^3(TI)^3}{4}$	1.68 X E-4	100
2oo3	$\frac{3\lambda^2(TI)^2}{4}$	5.76 X E-3	$\lambda^2(TI)^2$	7.67 X E-3	33
2oo4**	$\frac{\lambda^3(TI)^3}{2}$	3.36 X E-4	$\lambda^3(TI)^3$	6.72 X E-4	100

* Assuming $\lambda = \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 1$ X E-5 hrs^{-1} & TI for all components = 8760 hrs

** Assumes graceful degradation

B.3 MTTF^{spurious} equations

Spurious failures are random failures that are often self-revealing. Some spurious failures will not result in an immediate process impact or process interruption, e.g. the failure of a single component in a redundant 2oo2 configuration. Fortunately, fault trees may be drawn to model the spurious failure of the inputs, logic solver, final elements and the support system. The mathematics involved in quantifying these fault trees is different from PFD$_{avg}$, because the spurious trip rate is calculated as a rate rather than as a probability. The actual calculation methodology is different for “Or” gates and “And” gates. Therefore, these are discussed separately below.

B.3.1 “Or” gates

The spurious trip rate or STR for each component is calculated as:

(Eq. B.35) $STR_{component} = 1/MTTF^{spurious}$

The spurious trip rate for an “Or” gate is then calculated using B.6.

B.3.2 “And” gates

The spurious trip rate or STR for an “And” Gate must be calculated by examining the probability of one component failing and the frequency of the other component failing prior to the detection of the first failure. For two basic events, this would be calculated mathematically as:

Spurious Trip Rate = Probability of Device 1 Failing x Frequency of Device 2 Failing + Probability of Device 2 Failing x Frequency of Device 1.

The probability of each component failing is calculated using B.27. The frequency is calculated using B.35.

This page intentionally left blank.

Annex C — Index

This page intentionally left blank.

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: 1-55617-804-2