

ISA-TR84.00.02-2002 - Part 5



Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 5: Determining the PFD of SIS Logic Solvers via Markov Analysis

NOTICE OF COPYRIGHT

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



ISA—The Instrumentation,
Systems, and
Automation Society

Approved 17 June 2002



Documents
Document Sharing Hub

ISA-TR84.00.02-2002 – Part 5

Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques Part 5:
Determining the PFD of SIS Logic Solvers via Markov Analysis

ISBN: 1-55617-806-9

Copyright © 2002 by The Instrumentation, Systems, and Automation Society. All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.02-2002 – Part 5.

This document has been prepared as part of the service of ISA—the Instrumentation, Systems, and Automation Society—toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

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

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE STANDARD, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE STANDARD OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

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

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

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

PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS STANDARD.

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

The following people served as members of ISA Committee SP84:

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



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

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

* One vote per company.

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

NAME

COMPANY

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

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



This page intentionally left blank.

Contents

Foreword	9
Introduction	11
1 Scope	17
2 References	17
3 Definitions	18
4 Logic solver modeling using Markov analysis	18
4.1 Probability of Failure on Demand (PFD)	18
4.2 Markov modeling methodology	19
4.3 Assumptions and limitations	21
4.4 Basic Markov model description	22
5 Procedures for quantification of logic solver performance	23
5.1 Assumptions and limitations	23
5.2 Calculations and reports	25
6 Logic solver Markov models calculation results	25
6.1 Description and results of the reliability calculation for three E/E/PE logic solver configurations including input data tables	26
6.2 Configuration drawings, Markov diagrams and calculation results	27
Annex A (informative) — Markov model development and quantification	49
Annex B (informative) — Logic solver model input data	91
Annex C — Index	99

This page intentionally left blank.



Documents
Document Sharing Hub

Safety Instrumented Functions (SIF)

— Safety Integrity Level (SIL) Evaluation Techniques

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

Foreword

The information contained in ISA-TR84.00.02-2002 – Part 5 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 Systems (SIS).

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 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 SIS design to achieve its required SIL. A secondary purpose of this document is to reinforce the concept of the performance based evaluation of SIS. The performance parameters that satisfactorily service the process industry are derived from the SIL and reliability evaluation of SIS, namely the probability of the SIS to fail to respond to a demand and the probability that the SIS 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 SIS. The basis for the performance evaluation of the SIS is safety targets determined through hazard analysis and risk assessment⁽⁶⁾ of the process. This document demonstrates methodologies for determining the SIL and the probability of spurious trip of the SIS.

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 Systems (SIS) — 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 SIS Logic Solvers via Markov Analysis

Introduction

ANSI/ISA-84.01-1996 describes a safety life cycle 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 function must achieve to accomplish the required risk reduction. ISA-TR84.00.02-2002 provides methodologies for evaluating SIS to determine if they achieve the specific SIL. This may be referred to as a probability of failure on demand (PFD) evaluation of the SIS.

ISA-TR84.00.02-2002 only addresses SIS 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 SIS.

The evaluation processes described in this document take place before the SIS detailed design phase of the life cycle (see Figure I.1, Safety Life Cycle 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 SIS 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 functions are included in a single logic solver. Generally, the safety function case with the highest SIL requirement will be the case that determines whether the logic solver meets performance requirements. When multiple safety function cases have the same SIL, select the case with the largest number of I/O, number of I/O channels, etc., to determine whether the logic solver meets performance requirements. The logic solver should be carefully evaluated since a problem in the logic solver may adversely impact the performance of all of the safety functions (e.g., common cause).

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

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

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

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

This document does not provide guidance in the determination of the specific SIL required (e.g., SIL 1, 2, 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. To understand what is meant by the SIS, refer to the model defined in ANSI/ISA-84.01-1996 and repeated in Figure I.2 defining the boundaries of the SIS.

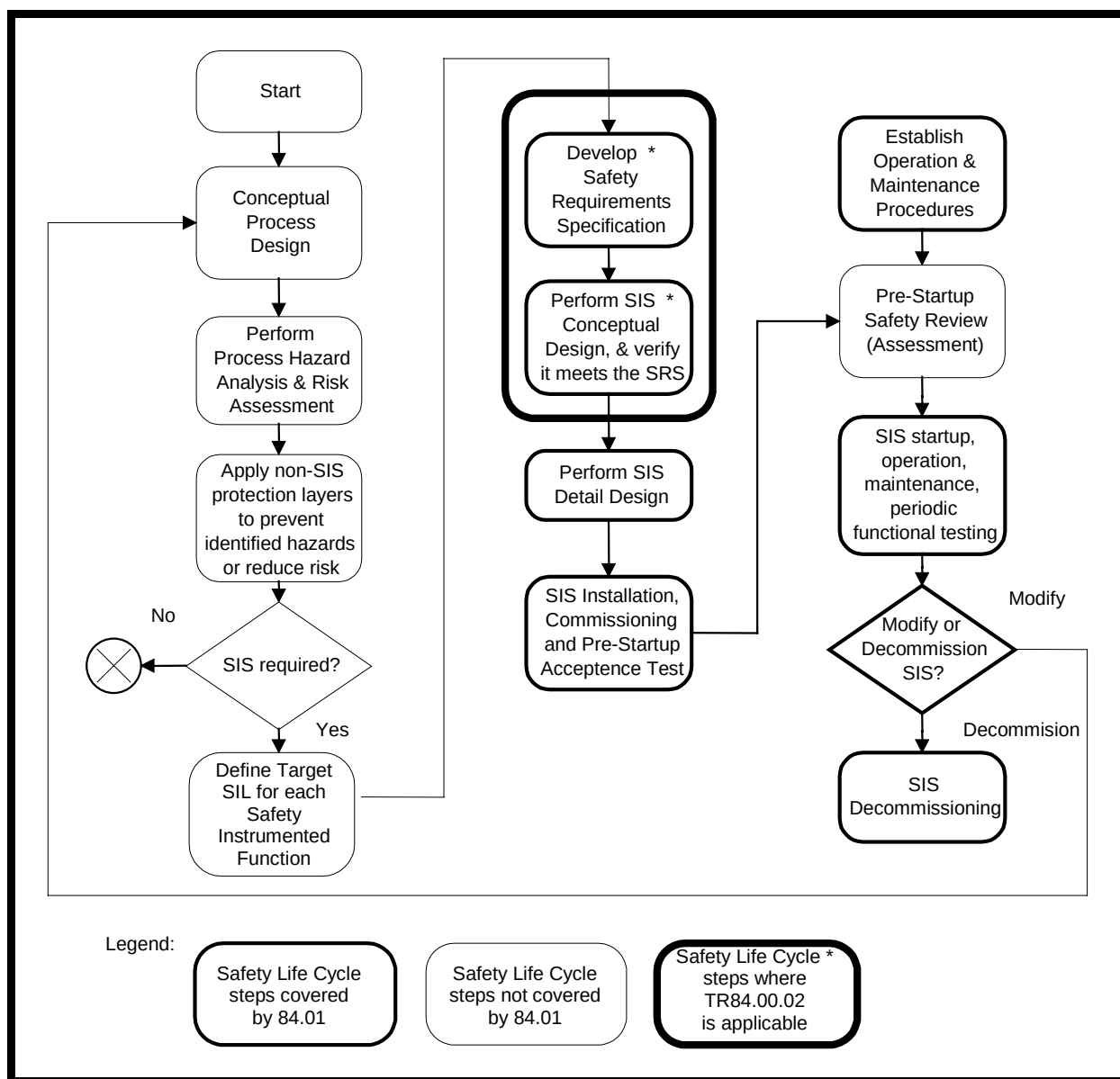


Figure I.1 — Safety life cycle model

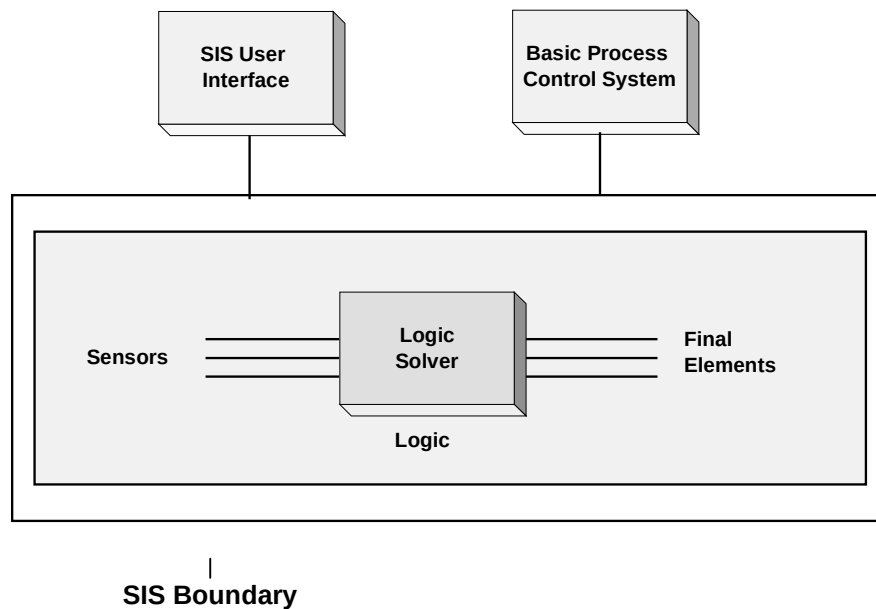


Figure I.2 — Definition of Safety Instrumented Systems (SIS)

The SIS Safety Requirements address 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 are used to evaluate the PFD of each safety 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, which allow a user to determine if a SIS meets the required safety integrity levels.

Safety integrity is defined as “The probability of a Safety Instrumented System 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 and systematic safety integrity by specifying target failure measures for each SIL. For SIS operating in the demand mode the target failure measure is **PFD_{avg}** (average probability of failure to perform its design function on demand). **PFD_{avg}** is also commonly referred to as the average probability of failure on demand. Systematic integrity is difficult to quantify due to the diversity of causes of failures; systematic failures may be introduced during the specification, design, implementation, operational and modification phases 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 SIS. 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 SIS, since process start up and shutdown are frequently periods where chances of a hazardous event are high. Hence in many cases, the reduction of spurious trips will increase the safety of the process. The acceptable safe failure rate is typically expressed as the mean time to a spurious trip ($MTTF^{spurious}$).

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

The objective of this technical report is to provide users with techniques for the evaluation of the hardware and systematic safety integrity of SIS (PFD_{avg}) and the determination of $MTTF^{spurious}$. The three methods in this technical report allow modeling of both systematic failures so that a quantitative analysis can be performed.

ISA-TR84.00.02-2002 shows how to model complete SIF, which include 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 SIS designer to select the proper system configuration to achieve the required safety integrity level.

ISA-TR84.00.02-2002 - Part 1 provides

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

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

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

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

engineer(s) performing design for a SIS with an overall technique for assessing the capability of the designed SIF.

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

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

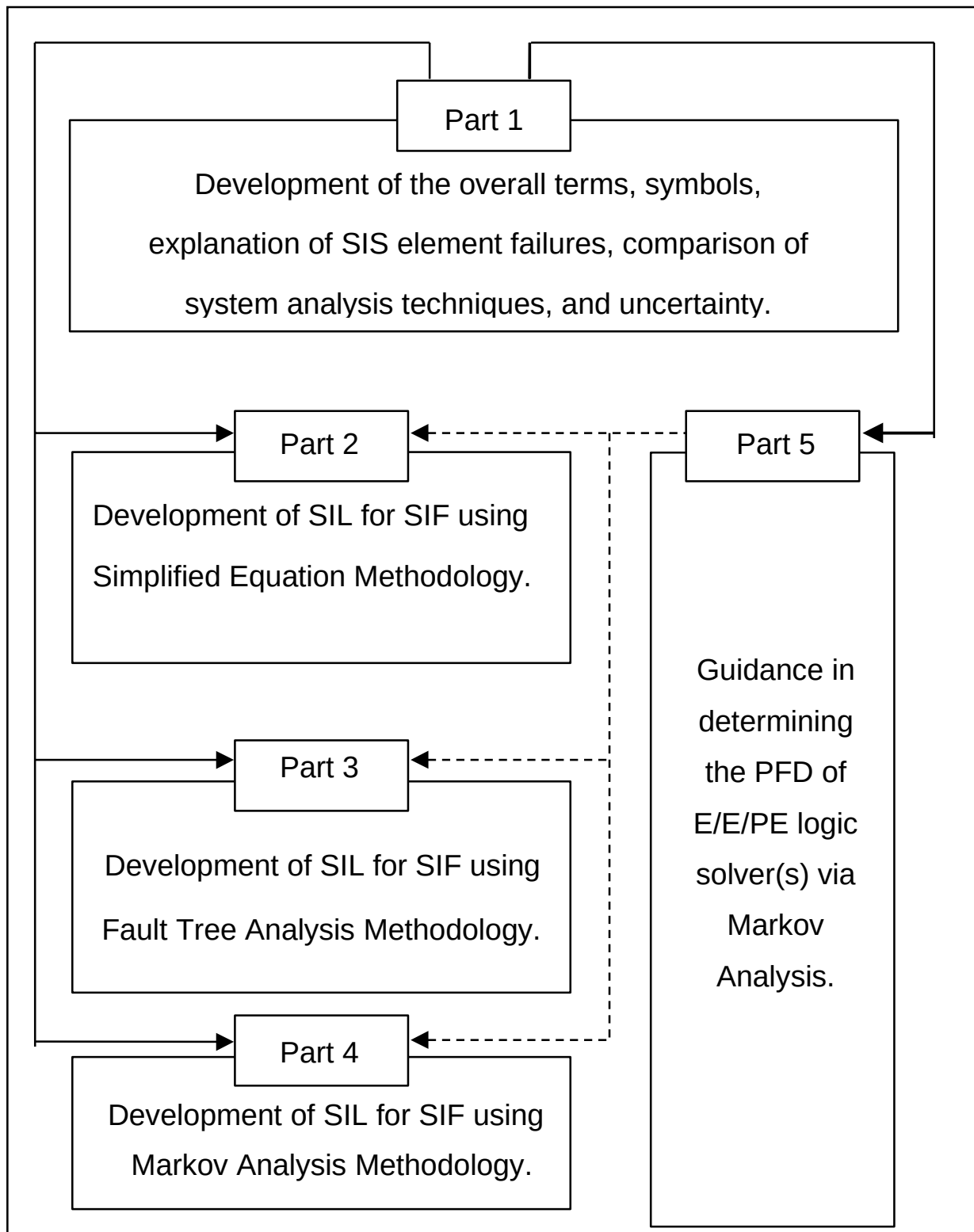


Figure I.3 — ISA-TR84.00.02-2002 overall framework

1 Scope

1.1 ISA-TR84.00.02-2002 - Part 5 is informative and does not contain any mandatory requirements. ISA-TR84.00.02-2002 - Part 5 is intended to be used only with a thorough understanding of ISA-TR84.00.02-2002 - Part 1 which defines the overall scope.

1.2 ISA-TR84.00.02-2002 - Part 5 provides:

a) guidance in PFD analysis of logic solvers;

NOTE The term "logic solver" will be used throughout Part 5 to indicate the SIS logic solver. The logic solver technology may be any E/E/PES.

b) a method to determine the PFD of logic solvers;

c) failure rates and failure modes of logic solvers;

d) the impact of diagnostics, diagnostic coverage, covert faults, test intervals, common cause, systematic failures, redundancy of logic solvers on the PFD of the logic solver; and

e) a method for the verification of PFD of logic solvers.

1.3 The procedures and examples outlined in ISA-TR84.00.02-2002 - Part 5 provide the engineer with Markov modeling steps to be followed in determining a mathematical value for the PFD for typical configurations of SIS logic solvers designed according to ANSI/ISA-84.01-1996.

1.4 Persons using ISA-TR84.00.02-2002 - Part 5 require a basic knowledge of Markov Analysis.

1.5 See ISA-TR84.00.02-2002 - Part 1 (Introduction), Part 2 (Simplified Equations), Part 3 (Fault Tree Analysis), and Part 4 (Markov Analysis) if it is necessary to mathematically evaluate the SIL of the safety instrumented function (SIF).

NOTE The method illustrated herein (i. e. Markov analysis) may also be used to determine the PFD of other SIF components such as sensors and final elements. The logic solver was selected to illustrate how Markov Analysis is applied to a complex SIF component.

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, 1990.
6. "Probabilistic Risk Assessment," Henley, Ernest J. and Kumamoto, Kiromitsu, IEEE Press, New York, New York, 1992.
7. "Reliability by Design," A.C. Brombacher, John Wiley & Sons, New York, NY 10158, 1992.
8. "Software Reliability Handbook," P. Rook, Elsevier Science Press, New York, NY 10010, 1990.
9. "Introduction to Reliability Engineering," E.E. Lewis, John Wiley & Sons, New York, NY 10158, 1987.
10. "Reliability Evaluation of Engineering Systems," R. Billinton, R.N. Allan, Pitman Advanced Publishing Program, Marshfield, MA 02050, 1983.

3 Definitions

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

4 Logic solver modeling using Markov analysis

ISA-TR84.00.02-2002 – Part 5 focuses on the logic solver associated with the safety instrumented function (SIF).

The objective is to develop the reliability models for three logic solver architectures using Markov analysis. The quantification of the models will produce the desired logic solver performance parameters:

- a) The probability to fail on demand (PFD), and
- b) The probability to fail spurious (PFS).

The Markov technique has been explained in ISA-TR84.00.02-2002 - Part 4 (Determining the SIL of a SIF using Markov Analysis). The reader who is interested in learning more about Markov modeling is referred to

- a) Evaluating Control Systems Reliability⁽⁵⁾, Chapter 5;
- b) Reliability Evaluation of Engineering Systems⁽¹⁰⁾, Chapters 8 and 9;
- c) Introduction to Reliability Engineering⁽⁹⁾, Chapter 9; and
- d) ISA-TR84.00.02-2002 – Part 4.

4.1 Probability of Failure on Demand (PFD)

See ISA-TR84.00.02-2002 - Part 1, Clause 4 for information on the probability of failure on demand (PFD).

4.2 Markov modeling methodology

Markov models^(7,9,10) are created by identifying all the possible states that the logic solver may enter while transitioning from fully operational, through partially failed (degraded) states, to the failed state. To accomplish this task, the different logic solver states are identified during the failure modes and effects analysis (FMEA) and the corresponding transition probabilities (i.e., probabilities of components that must fail in order to transition from one state to another state) are shown as arcs on the Markov model.

Markov model construction starts with the state of the logic solver where all of the components are functioning properly (successful state). To develop the other states, the following general procedure is followed:

For any state

- a) list all of the logic solver components, and
- b) list the ways the logic solver components may leave that state. There are two ways that a component can leave a state.
 - 1) First, a component in an operating state can fail.
 - 2) Second, a component in a failed state can be repaired.

In the former case, the probability of a component failure is the driving mechanism to force a transition out of the state. For exponential failure and repair probability distributions and using the rare event approximation (ISA-TR84.00.02-2002 – Part 5, Annex A, Clause A.4, Equation 4) the probability of failure is defined as λt , where λ is the failure rate of the component and t is the time. For the latter case, the repair probability is given as μt , where μ is the repair rate. Due to convention, these probabilities in the Markov models are shown as simply failure rates and/or repair rates and are commonly referred to as transition rates. The transition probabilities are always considered in the formulation and analysis of the models.

Annex A illustrates how a Markov model is created for the logic solver shown in Figure 4.1 which is a Dual PE logic solver having Dual Input and Dual Output modules, with One-out-of-Two (1oo2) shutdown logic.

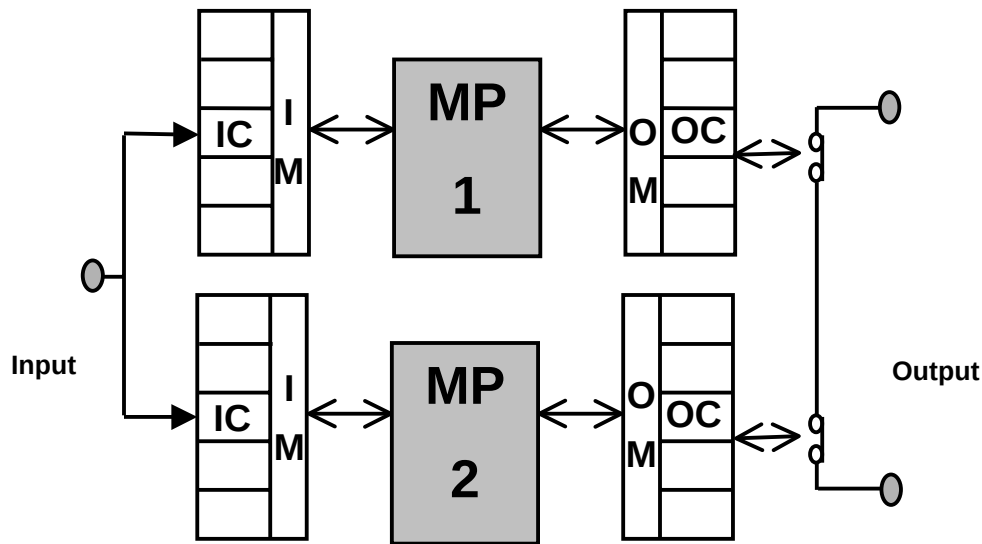


Figure 4.1 — Hypothetical - dual PE logic solver with dual I/O, one-out-of-two (1oo2) shutdown logic

Before a Markov Model can be developed an FMEA is typically performed to determine the hardware failure rates. The failure rate must be broken down into safe and dangerous fractions, so the complete performance of the logic solver can be evaluated. In fact, the safe and dangerous failure rates should also be broken down into the detected and undetected failures, as determined by the logic solver on-line diagnostics. Hence the FMEA should result in the determination of the component failure categories shown in Table 4.1. The FMEA method is described in ISA-TR84.00.02-2002 - Part 1, Annex D.

Table 4.1 — Component failure categories

Component	Failure Categories					
IP	SCC	DCC	SD	SU	DD	DU
OP	SCC	DCC	SD	SU	DD	DU
MP	SCC	DCC	SD	SU	DD	DU
IC	SCC	DCC	SD	SU	DD	DU
OC	SCC	DCC	SD	SU	DD	DU

Legend: Component

IP – Common part of input module
 OP – Common part of output module
 MP – Main Processor
 IC – Input Channel
 OC – Output Channel

Failure Categories

SCC – Safe common cause failure
 DCC – Dangerous common cause failure
 SD – Safe detected hardware failure
 SU – Safe undetected hardware failure
 DD – Dangerous detected hardware failure
 DU – Dangerous undetected hardware failure

4.3 Assumptions and limitations

All of the assumptions made while developing the models are listed below. The impact on the models if these assumptions are changed is also discussed.

1. The calculations are based on de-energize-to-trip SIFs.
2. Failure rates and on-line repair rates are assumed to be constant.
3. The mission time for the logic solver is assumed to be the time between function tests of the logic solver. This assumption eliminates the repair of any undetected failures because they would only be detected during the functional test interval.
4. The hazard and risk analysis shall define the acceptable response in the event of loss of power.
5. One type of input module and one type of output module are used in all Markov models. It is assumed that there are *n* input modules and *m* output modules in each leg of every architecture. Additional module types can be easily included by modifying the models to account for the additional safe and dangerous failure transitions.
6. It is assumed that plant personnel will initiate action to take the process to a safe state when a dangerous failure is detected in the logic solver (operator response is assumed to be before a demand occurs, i.e., instantaneous, and PFD of operator response is assumed to be 0).

NOTE If the action depends on the 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.

7. The models assume that the inspection and repair functions that are performed are perfect and bring the logic solver to a "as good as new state."
8. Channels in multi-channel architectures are treated as completely independent.
9. The data used for the example calculations can be found in Annex B.

4.4 Basic Markov model description

The basic Markov model used for the logic solver architectures is given in Figure 4.2.

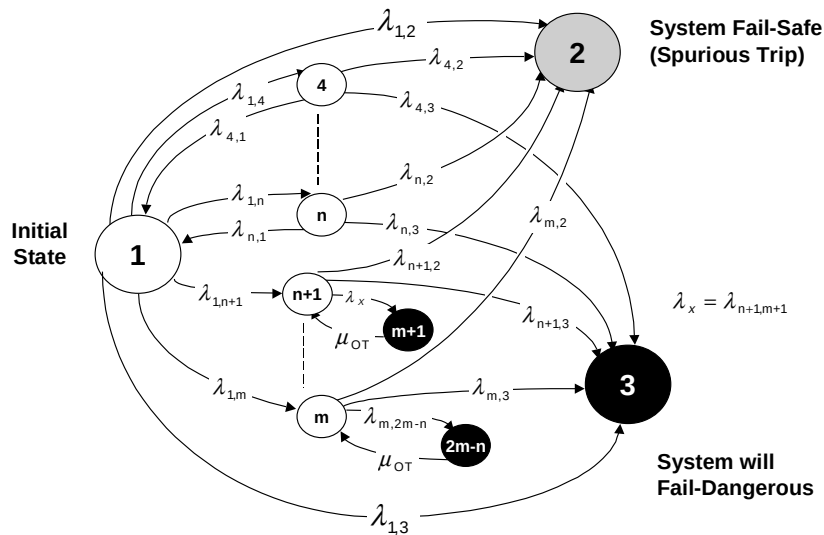


Figure 4.2 — Basic Markov model

The basic Markov model has the following final and intermediate (transition) states:

- | | |
|-------------|--|
| 1: | The initial state. No failures are present in the logic solver. |
| 2: | The fail-safe state. The logic solver is in the shutdown safe state. |
| 3: | The fail-dangerous state. The logic solver will not respond to a process demand. |
| 4...n: | The intermediate states where one or more (safe detected, safe undetected or dangerous detected) failures are present without being in the fail-safe state. |
| n+1...m: | The intermediate safe states where one or more dangerous undetected failures are present without being in the fail-dangerous state. |
| m+1...2m-n: | The intermediate fail-dangerous states where a combination of dangerous undetected and a safe or dangerous detected fault is present that can be repaired bringing the logic solver back to state n+1÷m. If a demand comes in this situation the logic solver will not be able to perform the safety function. |

The transitions in this model are:

- | | |
|----------------|---|
| λ_{12} | Immediate transition from the initial-state to the fail-safe state. Caused by safe failures in single components (e.g., single inputs) and by safe common cause failures. |
|----------------|---|

$\lambda_{1,3}$	Immediate transition from the initial-state to the fail-dangerous state. Caused by dangerous failures in single components (e.g., single outputs) and by dangerous common cause failures.
$\lambda_{1,4} \dots \lambda_{1,n}$	Transition from the initial-state to an intermediate safe state. Caused by safe failures in redundant components (e.g., dual input modules). These failures can be safe detected, safe undetected and dangerous detected.
$\lambda_{1,n+1} \dots \lambda_{1,m}$	Transition from the initial-state to an intermediate safe state. Caused by dangerous undetected failures in redundant components (e.g., dual input modules).
$\lambda_{n+1,m+1} \dots \lambda_{m,2m-n}$	Transition from the intermediate safe state to an intermediate dangerous state. Caused by dangerous detected fault in a related redundant component (e.g., 1 output channel dangerous undetected combined with an output channel dangerous detected).
$\lambda_{4,2} \dots \lambda_{n,2}$	Transition from an intermediate safe state to the fail-safe state. Caused by a second safe fault in a redundant related component (e.g., dual input modules). These failures can be safe detected, safe undetected, dangerous detected and all failures that result in a transition from state 1 to state 2.
$\lambda_{4,3} \dots \lambda_{n,3}$	Transition from an intermediate safe state to the fail-dangerous state. Caused by the same failures that result in a transition from state 1 to state 3.
$\lambda_{n+1,2} \dots \lambda_{m,2}$	Transition from an intermediate safe state to the fail-safe state. Caused by all failures that result in a transition from state 1 to state 2.
$\lambda_{n+1,3} \dots \lambda_{m,3}$	Transition from an intermediate safe state to the fail-dangerous state. Caused by a second dangerous undetected fault in a redundant related component (e.g., 2 input modules) and all failures that result in a transition from state 1 to state 3.

Numerous other transitions are possible (e.g. from state m+1 to states 2 and 3, from state 4 to state m+1, etc.) but these are not drawn for clarity and as their contribution is negligible.

The matrix development methodology discussed in Annex A does not include the state transitions $\lambda_{4,2} \dots \lambda_{n,2}$, $\lambda_{n+1,2} \dots \lambda_{m,2}$, $\lambda_{4,3} \dots \lambda_{n,3}$, $\lambda_{n+1,3} \dots \lambda_{m,3}$ in the resulting Markov models as these transitions prevent the use of a closed form solution.

5 Procedures for quantification of logic solver performance

This clause will outline steps that will allow a vendor and user to agree on the information necessary to quantify and to document SIF component performance. The components include sensors, logic solvers, and final elements. This text illustrates procedures for logic solvers.

5.1 Assumptions and limitations

This clause will outline communications and agreements necessary to ensure proper modeling.

5.1.1 Assumptions and limitations inherent to the logic solver

The vendor should state:

- What data (e.g., functional test interval) is used for failure rates of cards or components, and what is the source (historical records and population size, or calculated and how) of the data.
- What data is used for diagnostic coverage of cards or components, and what is the source of the data.
- Common cause assumptions and the basis for the assumption.

5.1.2 Assumptions and limitations associated with the end user and the specific application

Since the logic solver PFD_{avg} is affected by the off-line functional test interval, the user should provide the intended test interval to the vendor for use in the calculations. This information may be generic to user company standards and practices, or may be dictated by the specific requirements of the application being modeled.

The following information needs to be available for all calculations:

- Power system failure rates
NOTE Some parts of the power supply may be outside the vendor's scope of supply. The interface must be defined.
- Redundancy of each component, communication channel, or card included in the calculation
- Time interval for off-line testing
- Time interval for off-line repair
- Time interval for on-line repair (this will require up-front analysis by the user and supplier for practicality and safety)

For PFD_{avg} calculation:

- Definition of each safety instrumented function and associated SIL
- Number of inputs and outputs for each SIF and redundancy of each.
(NOTE Inputs and outputs with no SIL requirement such as indicator lights or alarms can generally be omitted from the calculation.)
- Generally, the safety function case with the highest SIL requirement will be the case that determines whether the logic solver meets the performance requirements. When multiple safety function cases have the same SIL, select the case with the largest number of I/O, number of I/O channels, etc. to determine whether the logic solver meets the performance requirements.

For $MTTF^{spurious}$ calculations:

- Desired I/O groupings for spurious trip calculations
- Number of inputs and outputs for each group and redundancy of each.

(NOTE Number of I/O associated with spurious trip may be different than number associated with PFD_{avg} . I/O not associated with spurious trips should be omitted.)

5.1.3 Assumptions and limitations inherent in the quantification technique

The vendor should state:

- The type and source of the program used to perform calculations
- Any limitations and assumptions that may be inherent in the specific program used for the calculation
- Mission time that is assumed for the calculation

Some examples of limitations that might be inherent in modeling programs (see Clause 4.3 also):

- Failure rates are assumed to be constant.
- Inspection and repair is assumed to be perfect.

The vendor and user should reach a mutual understanding of how these limitations and assumptions relate to the users application, and whether the model is adequate for the intended use.

5.2 Calculations and reports

5.2.1 The vendor should incorporate all data and assumptions specific to the application in a model and perform the calculations.

5.2.2 Reports

Information for each calculation should include the following:

- The vendor and specific equipment being modeled
- The end user and the specific application(s) being modeled
- All assumptions and limitations (input data)
- Calculation methods (or specific models, programs, options)
- Who performed the calculations
- Date the calculations were performed
- PFD_{avg} and $MTTF^{spurious}$ for each case calculated, and any data specific to that case
- Any additional information specifically agreed to by the parties

6 Logic solver Markov models calculation results

The objective of this clause is to define the logic solver architectures that are selected as examples for the application of Markov modeling technique, define their associated Markov models and give the calculation results.

6.1 Description and results of the reliability calculation for three E/E/PE logic solver configurations including input data tables

6.1.1 Configuration names

Config 1 Single PE logic solver with single I/O, One-out-of-One (1oo1) shutdown logic

Config 2 Dual PE logic solver with dual I/O, One-out-of-Two (1oo2) shutdown logic

Config 3 Single E/E logic unit with dual Inputs and Outputs and 1oo2 voting logic implemented by either:

- relay, or
- solid state, or
- fail-safe solid state logic solvers

6.1.2 Overview of the three calculated configurations

The calculation results per configuration includes

- hardware failures;
- common cause failures; and
- systematic failures and diagnostic coverage factors.

Configurations are without sensors and final elements.

For each of the configurations the results consist of two graphs:

A: Probability of Fail-Dangerous (PFD) is related to the safety integrity level (SIL) as defined by ANSI/ISA-84.01-1996, IEC 61508, and IEC 61511. The PFD is typically plotted as function of the functional test interval and its relationship to other calculation variables can be more thoroughly understood by performing uncertainty analysis. The probability of fail-dangerous is derived from the **fail-dangerous state**.

B: Probability of Fail-Safe (PFS) is also typically plotted as a function of the functional test interval. The Probability of **fail-safe** is derived from the logic solver **fail-safe state (spurious trip)**.

The included uncertainty analysis shows three curves in each graph and indicates the 10th - the 50th - and the 90th percentile graph. The theory behind the uncertainty analysis is explained in Clause 5.9 of ISA-TR84.00.02-2002 – Part 1.

NOTE The 90th percentile graph indicates the line where 90% of the logic solvers have a lower Probability or 90% are better in terms of Safety Integrity or Spurious failures.

For Configuration 2 there are two types of additional graphs

C: Sensitivity graphs for the PFD and PFS.

D: Correlation graphs for the PFD and PFS.

NOTE The theory behind the sensitivity and correlation analysis is explained in Clause 5.9 of ISA-TR84.00.02-2002 – Part 1.

Configuration No. 3 is calculated for Relays, Solid State logic and Inherently fail-safe solid state logic.

6.1.3 Abbreviations used in the fail-dangerous sensitivity graphs

1oo1 (single) = One-out-of-One

1oo2 (serial) = One-out-of-Two

And gate = Dual Input voter

Coverage factory test = Coverage factor for the factory acceptance test (see tables)

DDfrac = Diagnostic coverage factor for dangerous failures

E = Electric logic solver

E = Electronic logic solver

Inp = Input

Outp = Output

PE = Programmable Electronic

PFD (Safety Integrity Level) = Fail-dangerous = Probability of failure on demand

PFS (Spurious Trip) = Fail-safe = Probability of fail-safe

Pow. sup = Power supply

Proc = Processor

S frac = Failure mode ratio safe – Unsafe failures

SD frac = Diagnostic coverage factors safe failures

Start Prob = Systematic failures

6.1.4 Input data tables used for the comparison calculations of the different E/E/PE logic solver configurations

The data used for the calculations are shown in the tables of Annex B.

6.2 Configuration drawings, Markov diagrams and calculation results

This clause describes the architecture models, Markov models and gives the graphic results for Probability of Failure on Demand (PFD) and the Probability to Fail-Safe (PFS).

6.2.1 Single PE with single I/O, one-out-of-one (1oo1) shutdown logic

Figure 6.1 shows the block diagram for the first architecture. It should be noted that the logic solver has only one main processor. For clarity one input and one output module are shown in Figure 6.1.

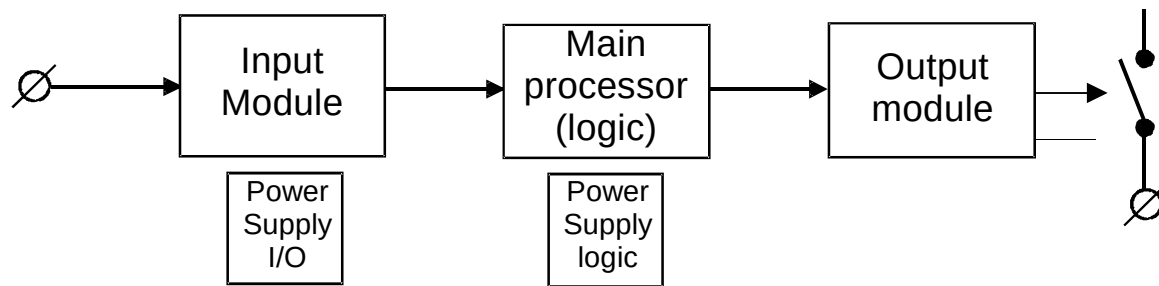


Figure 6.1 — Single PE logic solver with single I/O, one-out-of-one (1oo1) shutdown logic

The Markov model given in Figure 6.2 assumes there are n input modules and m output modules.

As mentioned previously, the safe and dangerous failure rates for each module in the logic solver are computed and then the dangerous detected and dangerous undetected failure rates are computed using the diagnostic coverage factors for dangerous failures (C_{IM}^D , C_{IC}^D , C_{MP}^D , C_{OM}^D , and C_{oc}^D).

The total safe and fail-dangerous failure rates for this simplex logic solver are the sum of the failure rates leading from state 1 to state 2 and from state 1 to state 3 respectively. As there is no redundancy in this architecture there are no intermediate states.

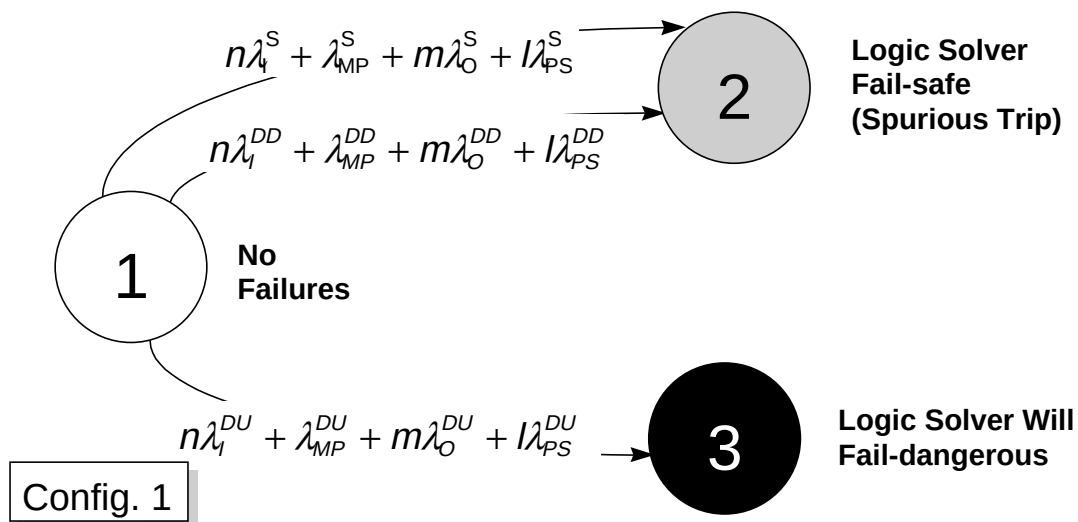


Figure 6.2 — Markov model Configuration 1: Single PE logic solver with single I/O, one-out-of-one (1oo1) shutdown logic

The graph provided in Figure 6.3 allows determination of probability of **fail-dangerous** of a single logic solver (1oo1) with a single input and output.

NOTE The 90th percentile graph indicates the line where 90% of the logic are better in terms of PFD.

The graph provided in Figure 6.4 allows determination of probability of fail-safe of a single logic solver (1oo1) with a single input and output.

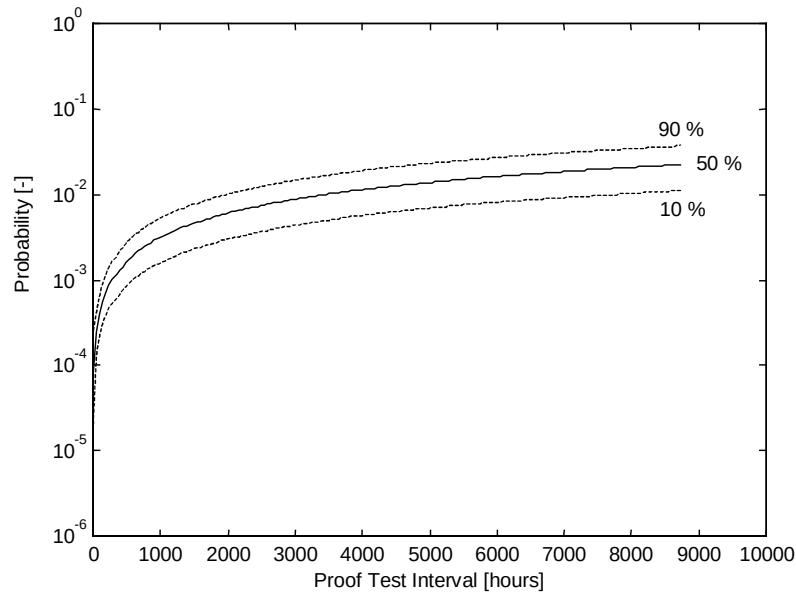


Figure 6.3 — PFD Configuration 1 – Probability fail-dangerous of a single PE logic solver with single input and output – 1oo1 configuration

Legend:

- 90th percentile
- 50th percentile
- ... 10th percentile

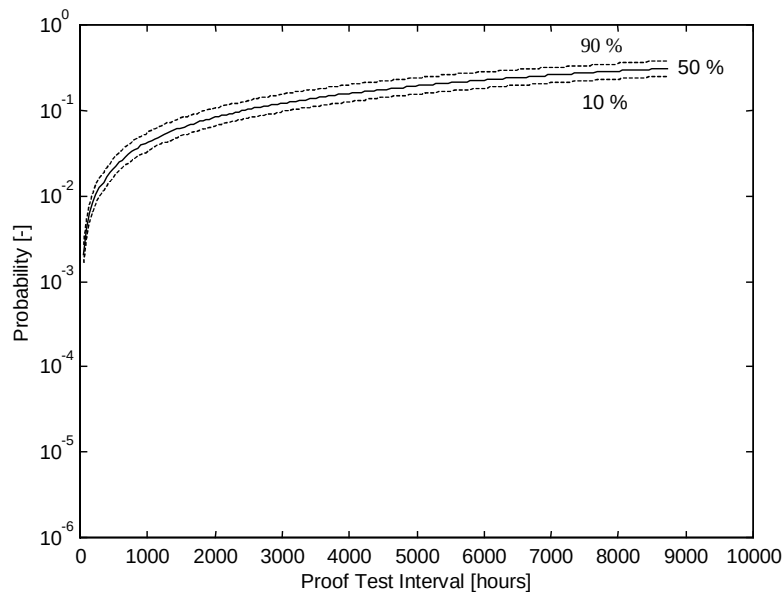


Figure 6.4 — PFS Configuration 1 – Probability of fail-safe of a single PE logic solver with single input and output – 1oo1 configuration

Legend:

- 90th percentile
- 50th percentile
- ... 10th percentile

6.2.2 Dual PE with dual I/O, one-out-of-two (1oo2) shutdown logic

A block diagram of this logic solver architecture is shown in Figure 6.5. This architecture consists of two completely independent legs. Each leg consists of a main processor with its associated I/O modules and power supplies. There is no communication between the two legs. The PE has two separate inputs, one input on each of the two legs or channels of the logic solver. Each output circuit consists of an output from each leg wired in series. Hence, each leg can independently open the output circuit and put the logic solver in the safe state.

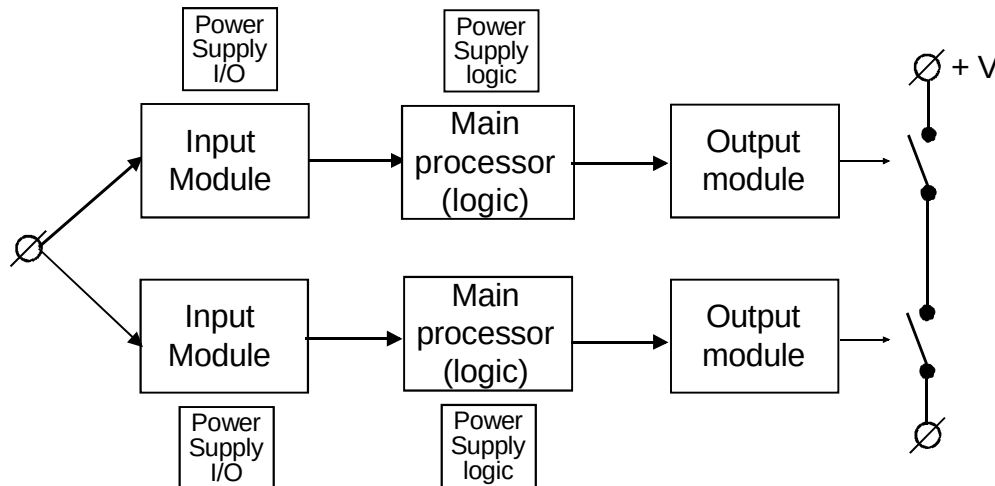


Figure 6.5 — Configuration 2 – Dual PE logic solver with dual I/O, one-out-of-two (1oo2) shutdown logic

The Markov model for this architecture is shown in Figure 6.6. The top arc in the Markov model represents a safe failure of any element in either leg of the PE. Any safe failure in either leg or channel will cause a spurious trip, because of the 1oo2 shutdown logic that allows either channel to shutdown the installation being protected. The bottom arc in the Markov model is for the common cause dangerous hardware failures.

Because of the dual redundancy and the 1oo2 logic, two failures of elements, one in each leg of the logic solver must occur before a fail-dangerous condition occurs. State 3 represents the state where the logic solver is in the fail-dangerous state and will not be repaired on-line since the failures are undetected. The PFD for the logic solver is computed by determining the probability of the logic solver being in state 3.

No inter-processor communication in this dual logic solver architecture is assumed. Since there is no inter-processor communication, each leg of the logic solver independently reads its inputs and determines what the outputs should be by execution of the shutdown logic IP (i.e., unable to respond to a demand). Note that a dangerous undetected failure of an input processor on one leg can result in a number of outputs on the leg stuck in the dangerous state. This is referenced in state 3 of Figure 6.6. So, the process will be in a fail-dangerous state if one of the corresponding outputs on the other leg fails in a dangerous state.

The states 4 to 9 are the safe intermediate states where a safe or detected failure has occurred that may be repaired before a subsequent failure brings the logic solver in the fail-safe or fail-dangerous state.

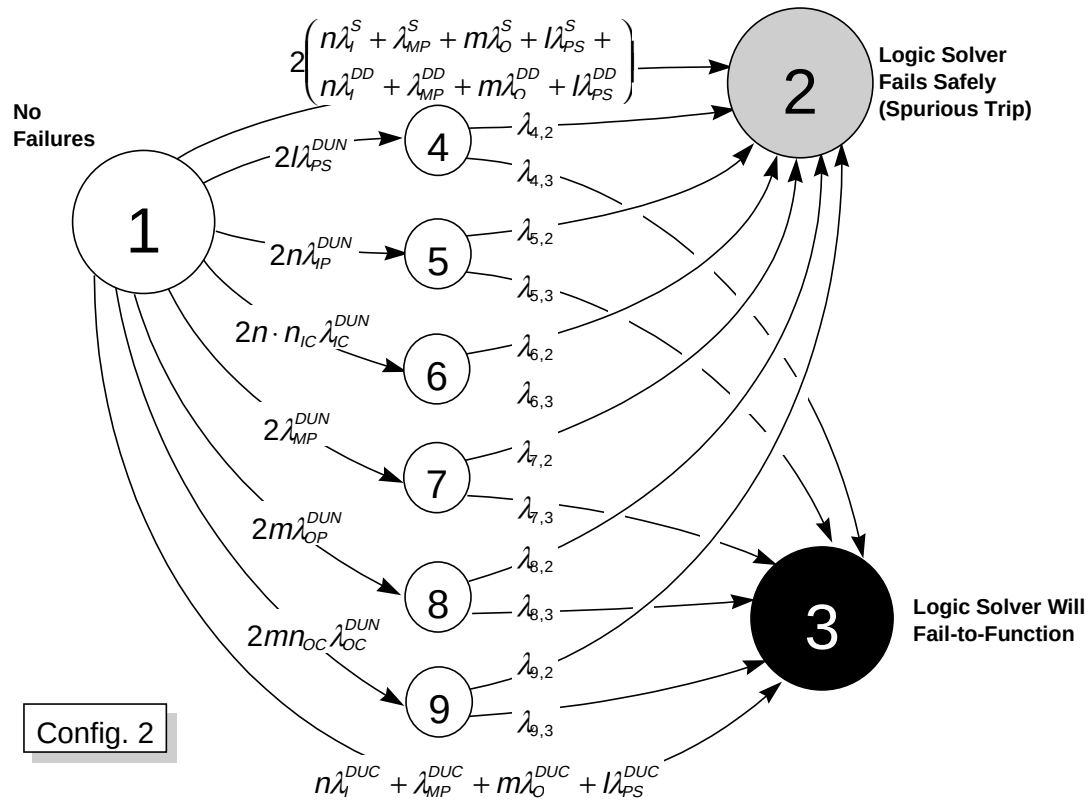


Figure 6.6 — Markov model for dual PE logic solver with dual I/O, one-out-of-two (1oo2) shutdown logic