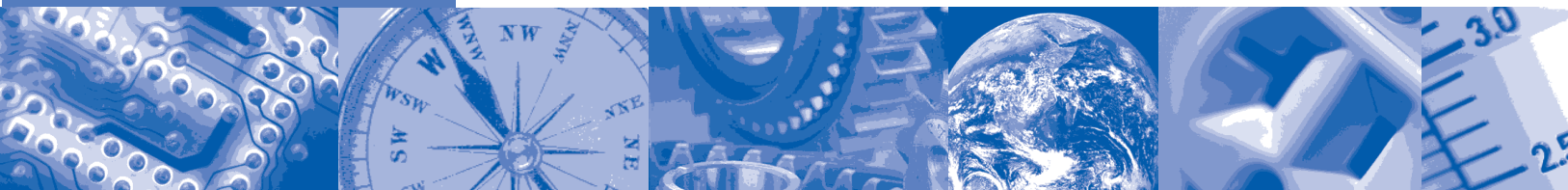


## ISA-TR84.00.02-2002 - Part 4



# **Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 4: Determining the SIL of a SIF via Markov Analysis**



ISA—The Instrumentation,  
Systems, and  
Automation Society

Approved 17 June 2002

ISA-TR84.00.02-2002 – Part 4

Safety Instrumented Functions (SIF) — Safety Integrity Levels (SIL) Evaluation Techniques Part 4:  
Determining the SIL of a SIF via Markov Analysis

ISBN: 1-55617-805-0

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 4.

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:

<b>NAME</b>	<b>COMPANY</b>
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	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. Icahan	ACES Inc
A. Iverson	Ivy Optiks
R. Jones	Dow Chemical Company
V. Maggioli	Feltronics Corporation
T. McAviney	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

Foreword .....	9
Introduction .....	11
1 Scope .....	17
2 References .....	17
3 Definitions .....	18
4 Introduction to Markov .....	18
5 Modeling and calculation procedures .....	19
5.1 Modeling and calculation procedures .....	19
6 Assumptions for Markov calculations for an SIF .....	20
7 Overview examples .....	21
8 Example 1 .....	22
9 Quantifying a Markov model .....	27
10 Results Example 1 .....	29
11 Example 2 .....	32
12 Results Example 2 .....	35
13 Example 3 .....	38
14 Base example calculation for an SIF using Markov models .....	39
15 Results base example .....	48
16 Index .....	50

This page intentionally left blank.



## Safety Instrumented Functions (SIF)

### — Safety Integrity Level (SIL) Evaluation Techniques

#### Part 4: Determining the SIL of a SIF via Markov 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 <sup>(1)</sup> requirements.

The purpose of ISA-TR84.00.02-2002 <sup>(2)</sup> 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 <sup>(6)</sup> of the process. This document demonstrates methodologies for the SIL and reliability evaluation of SIF.

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

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

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

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

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

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

Part 1: Introduction

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

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

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

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

## Introduction

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

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

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

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

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

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

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

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

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

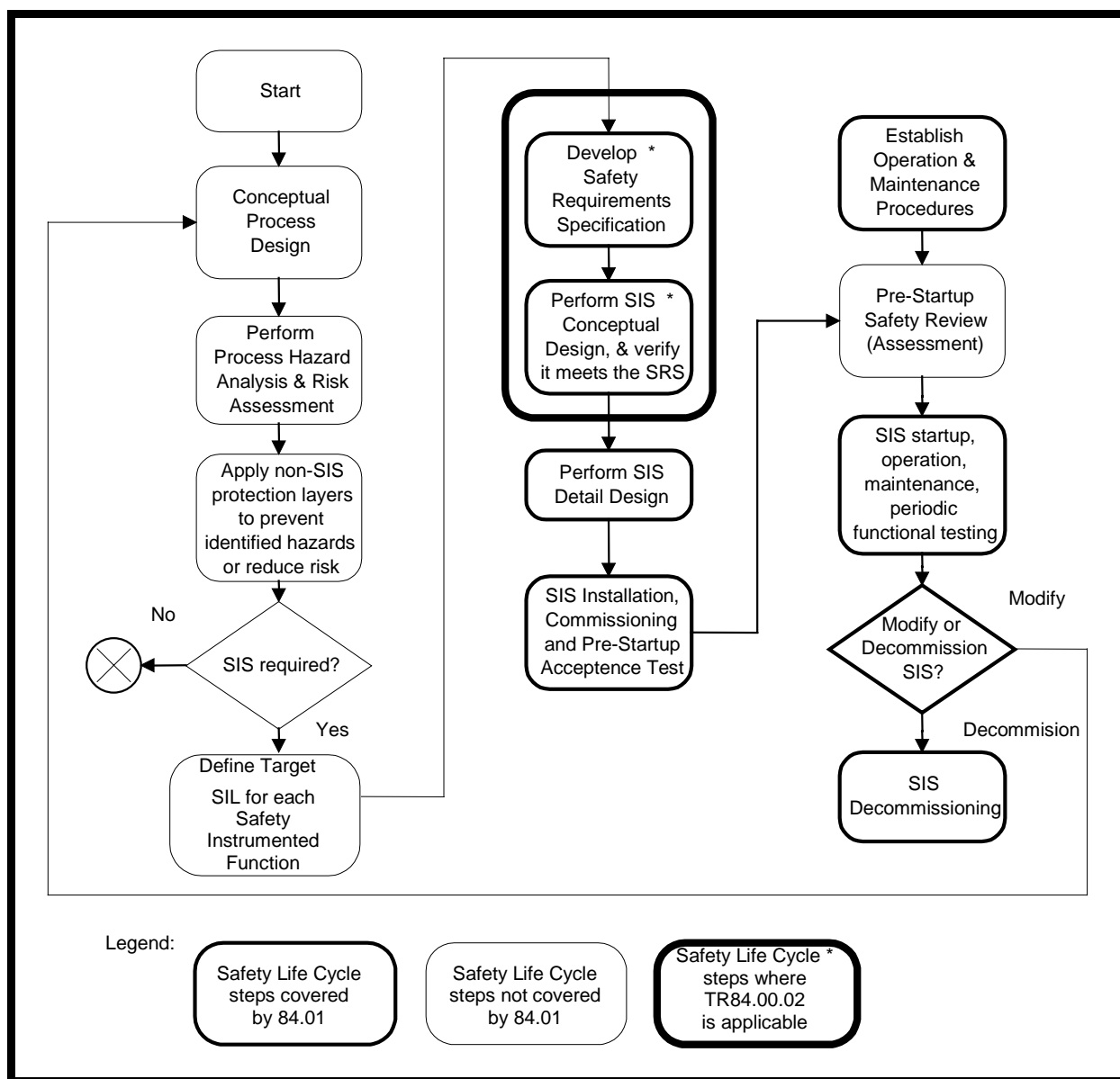
- element of a SIS that is common to more than one safety instrumented function; and
- redundant element with one or more safety instrumented function.

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

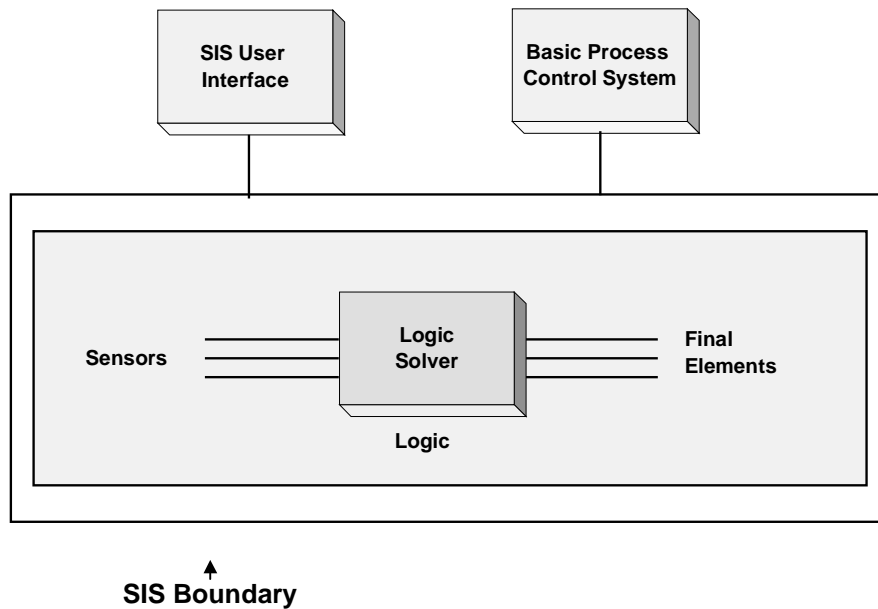
- to ensure that it meets the integrity level required for each safety instrumented function;
- to understand the interactions of all the safety instrumented functions; and
- to understand the impact of failure of each component.

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

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



**Figure I.1 — Safety life cycle model**



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

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

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

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

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

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

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

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

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

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

ISA-TR84.00.02-2002 - Part 1 provides

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

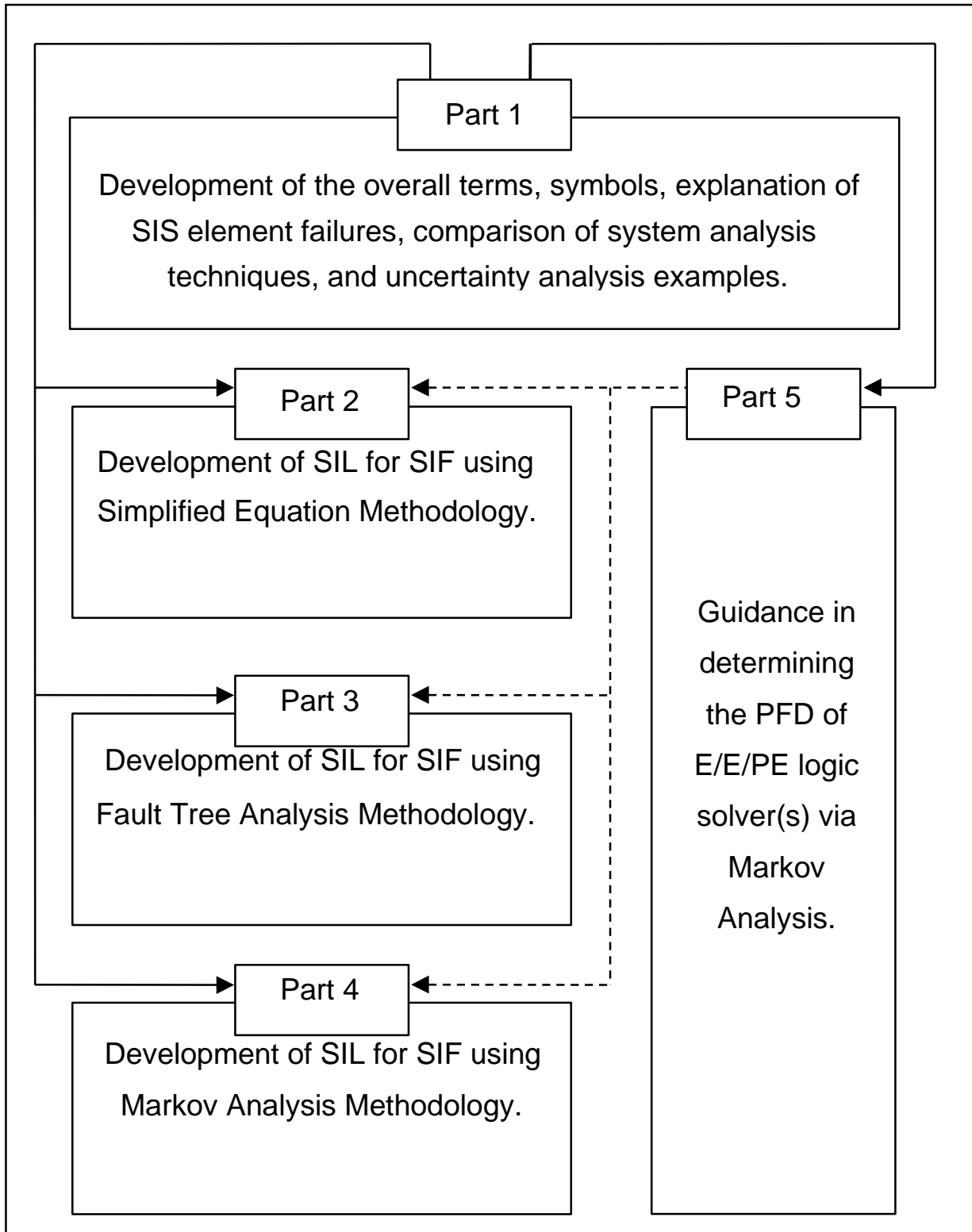
ISA-TR84.00.02-2002 - Part 2 provides simplified equations for calculating the SIL values for Demand Mode Safety Instrumented Functions (SIF) installed in accordance with ANSI/ISA-84.01-1996, "Applications of Safety Instrumented Systems for the Process Industries". Part 2 should not be interpreted as 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 4 is informative and does not contain any mandatory requirements. ISA-TR84.00.02-2002 - Part 4 is intended to be used only after a thorough understanding of ISA-TR84.00.02-2002 – Part 1. This technical report is intended to provide

- 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 4 provides one possible technique for calculating  $PFD_{avg}$  values for Safety Instrumented Systems (SIS) installed in accordance with ANSI/ISA-84.01-1996, "Application of Safety Instrumented Systems for the Process Industries."

1.3 Persons using ISA-TR84.00.02-2002 - Part 4 require knowledge of the Markov modeling technique. The reader who is interested in learning more about Markov modeling is referred to:

- Evaluating Control Systems Reliability<sup>(5)</sup>, Chapter 5;
- Reliability Evaluation of Engineering Systems<sup>(12)</sup>, Chapter 8 and 9;
- Introduction to Reliability Engineering<sup>(13)</sup>, Chapter 9;
- ISA-TR84.00.02-2002 - Part 5.

1.4 ISA-TR84.00.02-2002 - Part 4 introduces the reader to three examples, which explain the Markov theory and capabilities. These three examples make it possible to better understand the Base Example, which is also presented in ISA-TR84.00.02-2002 – Part 2 and ISA-TR84.00.02-2002 – Part 3.

## 2 References

1. ANSI/ISA-84.01-1996 "Application of Safety Instrumented Systems for the Process Industries," Instrumentation, Systems, and Automation Society," ISA, Research Triangle Park, NC, 27709, February 1996.
2. ISA-TR84.00.02-2002, "Safety Instrumented Functions (SIF) – Safety Integrity Level Evaluation Techniques, Part 1: Introduction; Part 2: Determining the SIL of a SIF via Simplified Equations; Part 3: Determining the SIL of a SIF via Fault Tree Analysis; Part 4: Determining the SIL of a SIF via Markov Analysis; Part 5: Determining the PFD of SIS Logic Solvers via Markov Analysis," Instrumentation, Systems and Automation Society, Technical Report, Research Triangle Park, NC, 27709, 2002.
3. "Reliability, Maintainability and Risk (Practical Methods for Engineers)," 4<sup>th</sup> Edition, D.J. Smith, Butterworth-Heinemann, 1993. ISBN 0-7506-0854-4.
4. "Guidelines for Safe Automation of Chemical Processes," Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY 10017, 1993.
5. "Evaluating Control Systems Reliability," W. M. Goble, Instrument Society of America, Research Triangle Park, NC, 27709, 1990.

6. Probabilistic Risk Assessment, Henley, Ernest J. and Kumamoto, Hiromitsu, IEEE Press, New York, New York, 1992.
7. CARE III, COSMIC, University of Georgia, 382 Broad East Street, Athens, GA 30602, USA.
8. CARMS, DAINA Corp., 4111 Central Ave. NE, Suite 212, Columbia Heights, MN 55421-2953, USA.
9. MARKOV1, Decision Systems Associates, 746 Crompton Rd., Redwood City, CA 94061, USA.
10. PC Availability, Management Sciences, 6022 Constitution Ave. NE, Albuquerque, NM 87110, USA.
11. MKV, Item Software Inc., 6545 Sunrise Blvd. Suite 201, Citrus Heights, California 95610-5105, USA.
12. "Reliability Evaluation of Engineering Systems," R. Billinton, R.N. Allan, Pitman Advanced Publishing Program, Marshfield, MA 02050, 1983.
13. "Introduction to Reliability Engineering," E.E. Lewis, John Wiley & Sons, New York, NY 10158, 1987.

### 3 Definitions

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

### 4 Introduction to Markov

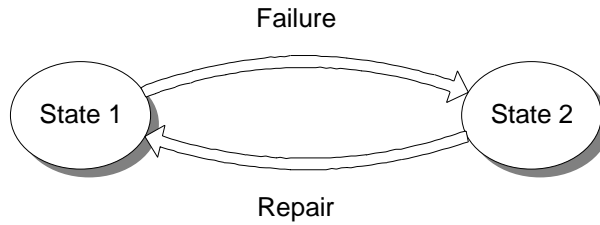
4.1 The Markov approach or Markov modeling technique originated from the Russian mathematician A.A. Markov (1856 - 1922). Markov was engaged in research on mathematically describing random processes. With the years, that work has been extensively developed and the Markov technique has received more attention and increased use.

The basic principle of Markov analysis is that a system can exist in different states. Each state is defined by an internal failure in the system. Usually these internal failures are combined to the level of what are called system states. These states are often driven by the availability of data, for example, data can be available on board level but can also be available on transistor level. Independent of the level of detail the system can be a:

- Fully operational system;
- Partially failed system (degraded), but still fulfilling its function; or
- Totally failed system.

4.2 A Markov model consists of Markov states and the transitions between these states, see Figure 4.1. The driving force to transition from one state to another is the failure or repair probability of components. There are two reasons why a transition from one state to another can occur:

- First, a component in an operating state can fail.
- Second, a component in a failed state can be repaired.



**Figure 4.1 — Simple Markov model**

## 5 Modeling and calculation procedures

Markov analysis offers certain advantages and disadvantages. The main advantage of Markov modeling is its modeling flexibility. Markov analysis can model all the aspects that are important for SIFs. In one Markov model, it is, for example, possible to model different failure modes of different components, different repair or test strategies (i.e., on-line, off-line, periodic), imperfect testing and repair, diagnostics capabilities, time dependent sequences of failures and common cause or systematic failures. Once the Markov model is constructed all the information is available to calculate the probability of a failure on demand or spurious trip.

The main disadvantage is its computational and modeling complexity. A number of computer programs are available on the market to perform the actual calculations, for example CARE III<sup>(7)</sup>, CARMS<sup>(8)</sup>, MARKOV1<sup>(9)</sup>, PC Availability<sup>(10)</sup>, MKV<sup>(11)</sup>. The construction of the Markov model is seen by users and practitioners of the technique as the largest disadvantage. Today's current practice is that these models are constructed by hand. ISA-TR84.00.02-2002 – Part 4, Clause 5 explains a straight forward FMEA type of approach to construct the Markov model. This method is easy in use although constructing the Markov model is more time consuming and tedious as the SIS grows in complexity.

### 5.1 Modeling and calculation procedures

1. Assign each safety function to its SIS as defined in the safety requirements specification<sup>(1)</sup>.
2. List the components that have a safety impact on each safety function. This will include logic solver(s), sensor(s) and final control element(s).
3. List the possible failure modes for each component.
4. Determine the degraded (intermediate) and failure system states by introducing in a systematic way the different failure modes of each component and its effect on the safety function. Determine how the SIS can be repaired from the degraded (intermediate) and failure system states and construct the Markov model (Clause 7).
5. Solve the Markov model to determine the probability of being in any state as a function of time.
6. Calculate the  $PFD_{avg}$  and the probability of a spurious trip of the SIS (Clause 8).
7. Determine if the  $PFD_{avg}$  of the SIS generated by the Markov Model Technique meets the SIL requirements of the safety requirements specification<sup>(1)</sup>.
8. If required, modify the configuration (hardware configuration, functional test interval, hardware selection, etc.) and repeat from step 3.

9. If the calculated probability of a spurious trip is unacceptable, modify the configuration (incorporate redundancy, use components with better reliability, etc.) and repeat from step 3.
10. When the SIS SIL and the probability of a spurious trip meet the specified requirements the calculation procedure is done.

## 6 Assumptions for Markov calculations for an SIF

The following assumptions were used in this Part for Markov analysis:

- 6.1 The SIF being evaluated will be designed, installed, and maintained in accordance with ANSI/ISA-84.01-1996.
- 6.2 Component failure and repair rates are assumed to be constant over the life of the SIF.
- 6.3 Redundant components have the same failure rates.
- 6.4 The sensor failure rate includes everything from the sensor to the input module of the Logic solver including the process effects (e.g., plugged impulse line to transmitter).
- 6.5 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.

For the examples shown in this Part, the logic solver failure rate was estimated by taking the  $PFD_{avg}$  for the logic solver, as supplied by the vendor, and converting it using Equation 6.1 into a rate. The derivation of this equation is shown in ISA-TR84.00.02-2002 – Part 3 Annex B.

$$(Eq. 6.1) \quad PFD_{avg} = \frac{\lambda TI}{2}$$

- 6.6 The final element failure rate includes everything from the output module to the final element including the process effects.
- 6.7 The Test Interval (TI) is assumed to be much shorter than the Mean Time To Failure (MTTF).
- 6.8 Testing and repair of components in the system are assumed to be perfect.
- 6.9 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.
- 6.10 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.

NOTE In real life it is, for example, possible that a component first fails dangerous and after some time fails safe.

- 6.11 It is assumed that when a dangerous detected failure occurs, the SIS will take the process to a safe state or plant personnel will take necessary action to ensure the process is safe (operator response is

assumed to be before a demand occurs, i.e., instantaneous, and PFD of operator response is assumed to be 0).

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

6.12 The fail-safe and fail-dangerous state are treated as absorbing states. This means that, once a component failure leads to either state, they will not be repaired. This assumption has been made to simplify the modeling effort. In real life, these states are not absorbing states. Specifically, the fail-safe state will be repaired relatively quickly because entering the fail-safe state will result in a spurious trip of the process. This assumption also brings about that it is not possible to fail again once entered into either states. For example, a failure of component causes a transition from the fail-dangerous state to the fail-safe state is not modeled.

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

6.14 For the first two examples the power supplies are not taken into account. The examples used in this part assume a de-energized to trip system, which means that power supply failures only contribute to the fail-safe state.

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

NOTE A detailed explanation of the Beta model is given in Annex A of ISA-TR84.00.02-2002 - Part 1.

## 7 Overview examples

Four examples are presented in this document. More detail on the architectures and the performed calculations can be found in the following clauses. The first three examples are specific examples for ISA-TR84.00.02-2002 – Part 4. Example 1 is a safety instrumented function (SIF) with two sets of sensors where each individual sensor can shut down the process. Example 2 is the analysis of the same SIF, taking into account diagnostic capabilities for the sensors and valves. Example 3 highlights additional features that show the modeling capabilities of the Markov technique. The fourth example is the base example that is also presented in ISA-TR84.00.02-2002 – Part 2 and ISA-TR84.00.02-2002 – Part 3. Table 7.1 gives an overview of the results of the performed calculations. Column 2 gives the  $PFD_{avg}$  after 1 year. Column 3 gives the  $MTTF^{spurious}$  after 1 year.

**Table 7.1 — Overview results examples**

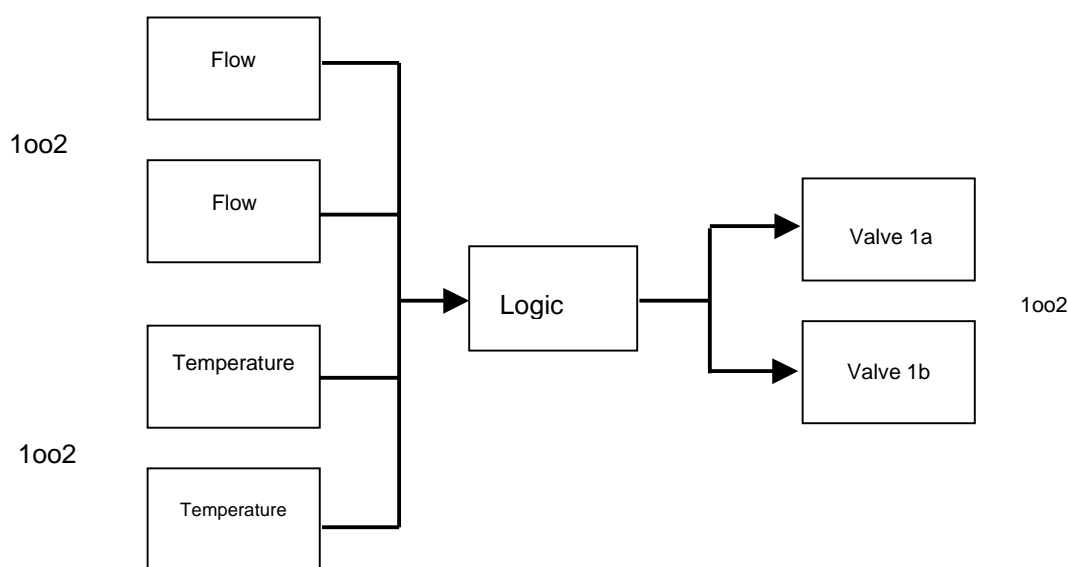
Example:	$PFD_{avg}$	$MTTF^{spurious}$ (years)
1	1.2 x E-2	3.3
2	5.3 x E-3	3.3
3	does not apply	does not apply
Base	8.3 x E-3	1.7

NOTE The four examples shown are NOT equivalent systems.

## 8 Example 1

The following example is used to explain the Markov approach (Clause 5, procedures 3 through 7).

Figure 8.1 presents a Safety Instrumented Function where each individual sensor can shut down the process. The system consists of two sets of sensors using 1oo2 shutdown logic connected to two valves piped in series. The first set consists of two identical flow sensors and the second set consists of two identical temperature sensors. Each sensor gives a signal to the logic solver. The signals from the sensors are used by the logic solver to close the valves in case of an unacceptable situation. The Hazard and Risk Analysis mandated a SIL 1. An analysis is performed to determine if the architecture shown in Figure 8.1 is adequate. Diagnostic capabilities for sensors and valves are not taken into account. This means that failure rates are only split into safe and dangerous rates. As a result, on-line repair is not taken into account.



**Figure 8.1 — Example 1 (demand mode process)**

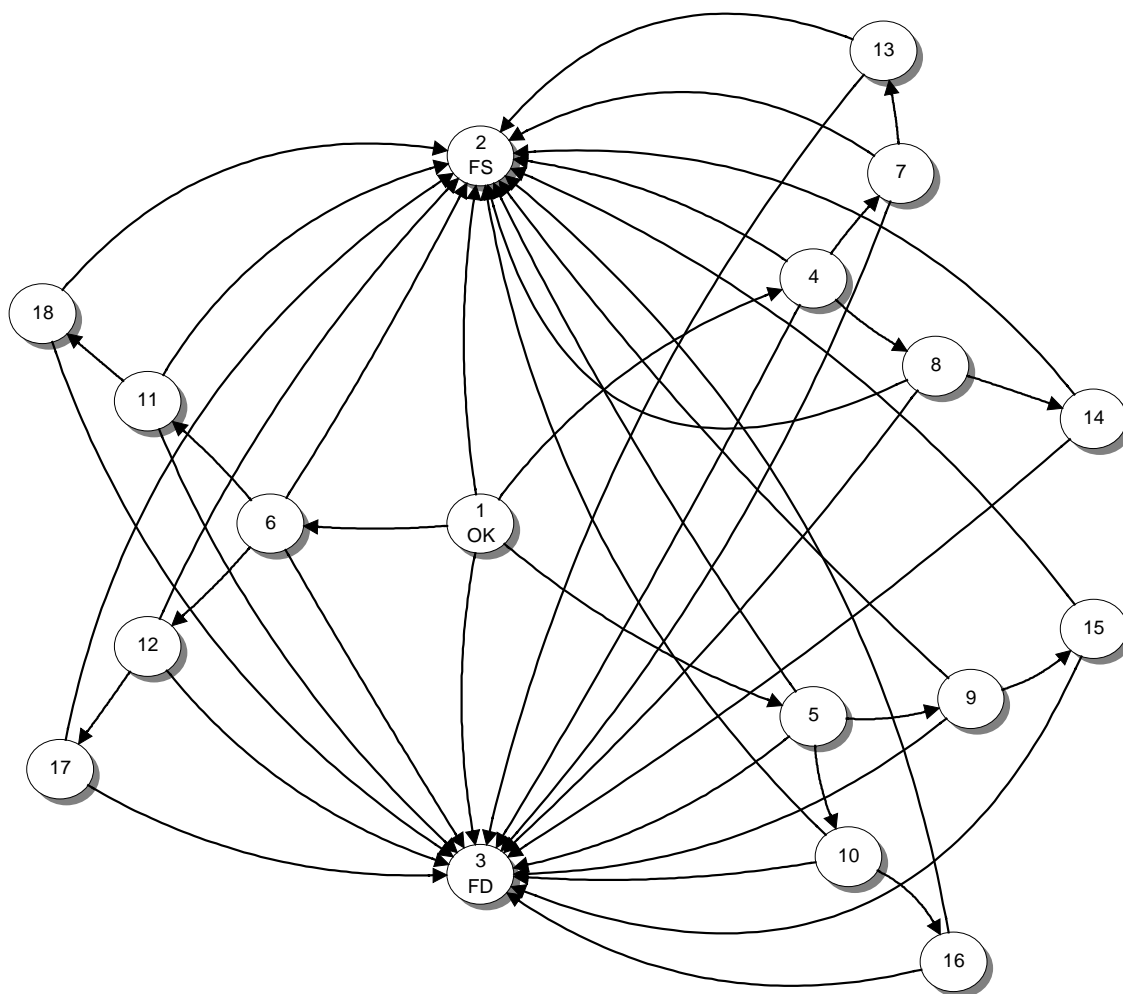
Table 8.1 shows a FMEA that lists the components, their failure modes and the effect on system level after a single failure. Only one failure at the time is introduced. It is assumed that components can fail due to a Safe (S), Dangerous (D), Safe Common Cause (SCC) or Dangerous Common Cause (DCC) failure. The effect of a failure on the SIF can result in a fail-safe (FS) (or spurious trip state), a fail-dangerous (FD) (or fail to function state) or in an intermediate state (IS).

Some component failures will lead to an intermediate state and, in that case, it is still possible for other components to fail. For example, the SIF will enter an intermediate state if the Flow Sensor 1 fails in a dangerous mode. Since this sensor has failed already it cannot fail in any other way. On the other hand, the remaining components can still fail in the failure modes as presented in Table 8.1. All the information to present the full Markov model is gathered, once there are no intermediate states left or there are no components left that can fail. Table 8.1 only presents the information after a single component failure.

**Table 8.1 — Resulting state after single failure - Example 1**

Starting from OK state		
Component	Failure Mode	Resulting System State after a single failure
Flow Sensor 1a (S1)	S	FS
	D	IS
	SCC	FS
	DCC	FD
Flow Sensor 1b (S1)	S	FS
	D	IS
	SCC	FS
	DCC	FD
Temperature Sensor 2a (S2)	S	FS
	D	IS
	SCC	FS
	DCC	FD
Temperature Sensor 2b (S2)	S	FS
	D	IS
	SCC	FS
	DCC	FD
Logic Solver (L)*	S	FS
	D	FD
Valve 1a (A)	S	FS
	D	IS
	SCC	FS
	DCC	FD
Valve 1b (A)	S	FS
	D	IS
	SCC	FS
	DCC	FD
S = Safe, D = Dangerous, SCC = Safe Common Cause, DCC = Dangerous Common Cause		
FS = Fail-safe, FD = Fail-dangerous, IS = Intermediate State		
*The data for the logic solver comes from the vendor (or the methodology used in Part 5). The data for the logic solver also includes elements like common cause, systematic failures, etc.		

Figure 8.2 presents, without going into detail, the full Markov model for this example.



**Figure 8.2 — Fully developed Markov model - Example 1**



Table 8.2 gives a complete overview of the different states and associated meaning. Please note that Table 8.2 does not show any transitions between the different states and does not provide information on the specific failure that resulted in the current state. Each state gives the SIF status.

**Table 8.2 — Description of the different states of the SIS - Example 1**

State		Description of the state
1, OK		No failures, SIS operates without any component failed.
2, FS		A component failure caused a spurious trip of the SIS.
3, FD		A component failure caused a fail to function on demand of the SIS.
4		One Flow Sensor failed dangerous (but not both), the SIS still performs its function.
	7	One Flow Sensor failed dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both), the SIS still performs its function.
	13	One Flow Sensor failed dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both) AND one Valve failed dangerous (but not both), the SIS still performs its function.
	8	One Flow Sensor failed dangerous (but not both) AND one Valve failed dangerous (but not both), the SIS still performs its function.
	14	One Flow Sensor failed dangerous (but not both) AND one Valve failed dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both), the SIS still performs its function.
5		One Temperature Sensor failed dangerous (but not both), the SIS still performs its function.
	9	One Temperature Sensor failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both), the SIS still performs its function.
	15	One Temperature Sensor failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both) AND one Valve failed dangerous (but not both), the SIS still performs its function.
	10	One Temperature Sensor failed dangerous (but not both) AND one Valve failed dangerous (but not both), the SIS still performs its function.
	16	One Temperature Sensor failed dangerous (but not both) AND one Valve failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both), the SIS still performs its function.
6		One Valve failed dangerous (but not both), the SIS still performs its function.
	11	One Valve failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both), the SIS still performs its function.
	18	One Valve failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both), the SIS still performs its function.
	12	One Valve failed dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both), the SIS still performs its function.
	17	One Valve failed dangerous (but not both) AND one Temperature Sensor failed dangerous (but not both) AND one Flow Sensor Failed Dangerous (but not both), the SIS still performs its function.

The transition from the operating state 1 to the fail-safe state 2 can be represented as follows:

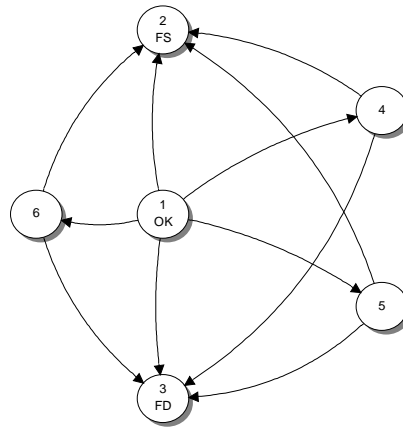
$$\lambda_{1,2} = 2\lambda_{s1}^s + 2\lambda_{s2}^s + \lambda_L^s + 2\lambda_A^s + \beta[\lambda_{s1}^s + \lambda_{s2}^s + \lambda_A^s]$$

where  $\lambda$  represents the failure rate and  $\beta$  represents the beta model for common cause failures. This expression means that any safe failure of one of the flow sensors, one of the temperature sensors, the logic or one of the valves will lead to the fail-safe state. A safe common cause failure of the flow sensors, the temperature sensor or the valves will also lead to the fail-safe state.

Similar transitions can be derived for the other states. State 3 is the fail-dangerous state and the states 4 through 18 represent intermediate states. The intermediate states 4, 5 and 6 are caused by a dangerous failure of any of the flow sensors, a dangerous failure of any of the temperature sensors or a dangerous failure of any of the valves, respectively. From the Markov model, it can be concluded that there are single failures that directly lead to the fail-safe or fail-dangerous states, but also combinations of failures (2, 3 or 4) that can lead to the fail-safe or fail-dangerous state. For example, a dangerous failure of one of the flow sensors will lead to state 4. If this failure is followed by dangerous failure of one of the temperature sensors, the system will transition to state 7. A dangerous failure of one the valves will lead to state 13. The system is still functioning because there is still a working flow sensor, a working temperature sensor and a working valve left. Any other failure from this state will lead to the fail-safe or to the fail-dangerous state.

Aspects like voting, redundancy or diversity bring about a full Markov model of a SIF usually consisting of many intermediate states. The quantitative results will mostly depend on the direct transitions to the fail-safe and fail-dangerous states. As a result, in most cases, it is not necessary to present a fully developed Markov model.

Each transition is an independent event. The transition from state 1 to state 2 is characterized by a probability. The transition from state 1 to state 2 via state 4 is characterized by the probability to transition from state 1 to state 4 AND the probability to transition from state 4 to state 2. In statistical terms, this means that these probabilities need to be multiplied. The probabilities used in the safety industry are so small that the contribution to a state by a transition of more than two steps can be neglected. Therefore, the following simplified Markov model is presented:



**Figure 8.3 — Simplified Markov model - Example 1**

The meaning of each state corresponds with the description in Table 8.2. A maximum sequence of two failures is presented. From the intermediate states 4, 5 and 6 only the transitions are shown that lead to

the fail-safe and fail-dangerous states directly. The possible intermediates states resulting from 4, 5 and 6 are neglected. The formulas belonging to this Markov model are presented next.

$$\lambda_{1,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S1}^S + \lambda_{S2}^S + \lambda_A^S]$$

$$\lambda_{1,3} = \lambda_L^D + \beta[\lambda_{S1}^D + \lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{1,4} = 2\lambda_{S1}^D$$

$$\lambda_{1,5} = 2\lambda_{S2}^D$$

$$\lambda_{1,6} = 2\lambda_A^D$$

$$\lambda_{4,2} = \lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S2}^S + \lambda_A^S]$$

$$\lambda_{4,3} = \lambda_{S1}^D + \lambda_L^D + \beta[\lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{5,2} = 2\lambda_{S1}^S + \lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S1}^S + \lambda_A^S]$$

$$\lambda_{5,3} = \lambda_{S2}^D + \lambda_L^D + \beta[\lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{6,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + \lambda_A^S + \beta[\lambda_{S1}^S + \lambda_{S1}^S]$$

$$\lambda_{6,3} = \lambda_L^D + \lambda_A^D + \beta[\lambda_{S1}^D + \lambda_{S2}^D]$$

## 9 Quantifying a Markov model

Once the Markov model has been developed it can be quantified. Two methods are available to quantify a Markov model. These methods are

- the Differential Equations Method; and
- the Matrix Multiplication Method.

9.1 The Differential Equations Method<sup>(3)</sup> is practical if the number of Markov states is limited ( $\leq 6$ ). For small systems this is an acceptable method. When the systems are larger, the Markov models become more complex and the Differential Equation Method is very time consuming and cumbersome. This technique is discussed in Annex A.4.1 of ISA-TR84.00.02-2002 – Part 5.

9.2 The Matrix Multiplication Method is a straightforward method and is relatively easy to translate into computer code. The method is based on a Stochastic Transition Matrix whose elements represent the probability of making a transition from one state to another in a certain time interval. If  $\Delta$  represents this transition matrix then the element  $\lambda_{1,2}$  of the matrix is defined as the Probability of making a transition to state 2 after a time interval  $t + \Delta t$ , given that the system was in state 1 at time  $t$ .

$$T = \begin{matrix} & \text{ToState} \rightarrow \\ \text{FromState} \downarrow & \begin{bmatrix} \lambda_{1,1} & \lambda_{1,2} \\ \lambda_{2,1} & \lambda_{2,2} \end{bmatrix} \end{matrix}.$$

The term  $\Delta t$  is introduced to transfer from failure rate to probabilities. This is done by multiplying the failure rate by  $\Delta t$ , because  $P(\text{Failure}) \cong \lambda \Delta t$  (for more details see ISA-TR84.00.02-2002 – Part 5).  $\Delta t$  must be chosen so small that the probability of having two or more failures in this time interval can be neglected. To simplify calculations  $\Delta t$  is often chosen to be 1 hour. For the Markov model in Figure 8.3 the transition matrix  $T$  looks like:

$$T = \begin{bmatrix} 1 - \sum_{i \neq 1}^6 \lambda_{1,i} \cdot \Delta t & \lambda_{1,2} \cdot \Delta t & \lambda_{1,3} \cdot \Delta t & \lambda_{1,4} \cdot \Delta t & \lambda_{1,5} \cdot \Delta t & \lambda_{1,6} \cdot \Delta t \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \lambda_{4,2} \cdot \Delta t & \lambda_{4,3} \cdot \Delta t & 1 - \sum_{i \neq 4}^6 \lambda_{4,i} \cdot \Delta t & 0 & 0 \\ 0 & \lambda_{5,2} \cdot \Delta t & \lambda_{5,3} \cdot \Delta t & 0 & 1 - \sum_{i \neq 5}^6 \lambda_{5,i} \cdot \Delta t & 0 \\ 0 & \lambda_{6,2} \cdot \Delta t & \lambda_{6,3} \cdot \Delta t & 0 & 0 & 1 - \sum_{i \neq 6}^6 \lambda_{6,i} \cdot \Delta t \end{bmatrix}.$$

Once the matrix has been defined the probability of making a transition from one state to another after  $q$  time intervals can be determined using the following formula

$$T(q) = T^q$$

which means multiplying the matrix  $q$  times with itself or taking the matrix to the  $q$ -th power. The variable  $q$  should be in-line with  $\Delta t$ . Therefore, if  $\Delta t$  equals 1 hour and the system should be evaluated for two years then  $q$  equals to

$$q = \frac{2 \cdot 365 \cdot 24}{1} = 17520,$$

assuming 24 hours a day and 365 days a year.  $T(q)$  is a new transition matrix after  $q$  time intervals. Eventually the system can be evaluated with the following expression

$$P(t) = P(0) \cdot T^q,$$

where the vector  $P(t)$  represents the probability of being in a state at time  $t$ ,  $P(0)$  represents the initial state vector and  $t = q\Delta t$ . The initial vector for the example used in this paragraph equals

$$P(0) = [1 \ 0 \ 0 \ 0 \ 0 \ 0].$$

This vector states that, at time zero, the probability of being in state one (OK state) is 1 and the probability of being in any other state is 0.  $P(t)$  represents the vector of being in any of the states at time  $t$ ,

$$P(t) = [P_1(t) \ P_2(t) \ P_3(t) \ P_4(t) \ P_5(t) \ P_6(t)].$$

The states 2 and 3 represent the Spurious Trip state and the Fail to Function state, respectively. The probability of a system to be in a spurious trip state at time  $t$  equals

$$P_{\text{Spurious Trip}}(t) = P_2(t)$$

and the probability of a system to fail to function on demand at time  $t$  equals

$$P_{\text{Fail to Function}}(t) = P_3(t)$$

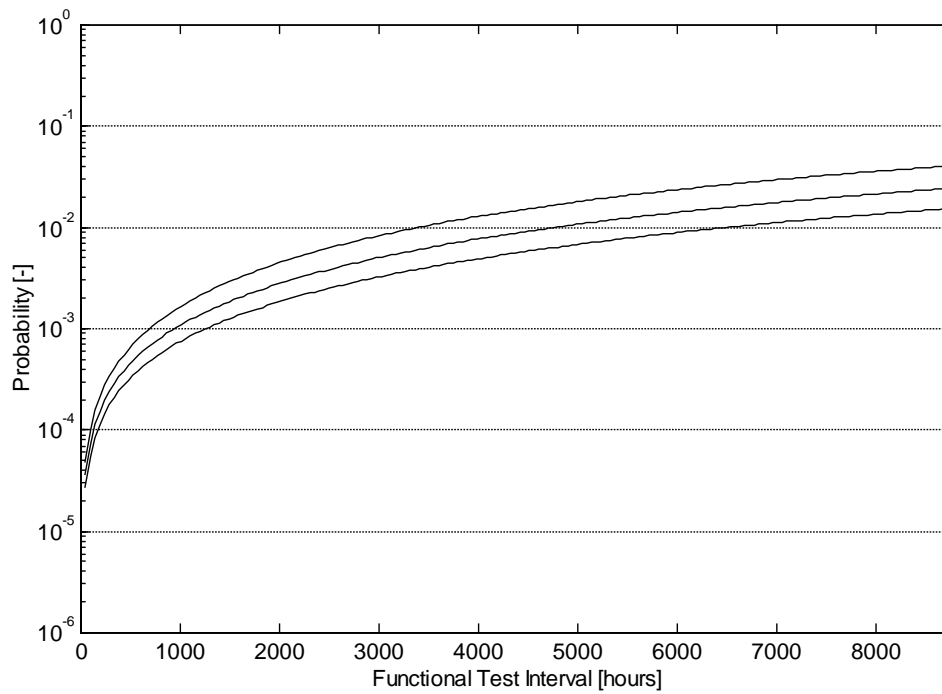
The  $PFD_{\text{avg}}$  can be calculated by using the following formula:

$$PFD_{\text{avg}}(t) = \frac{\int_0^t P_{\text{Fail to Function}}(t) dt}{t}.$$

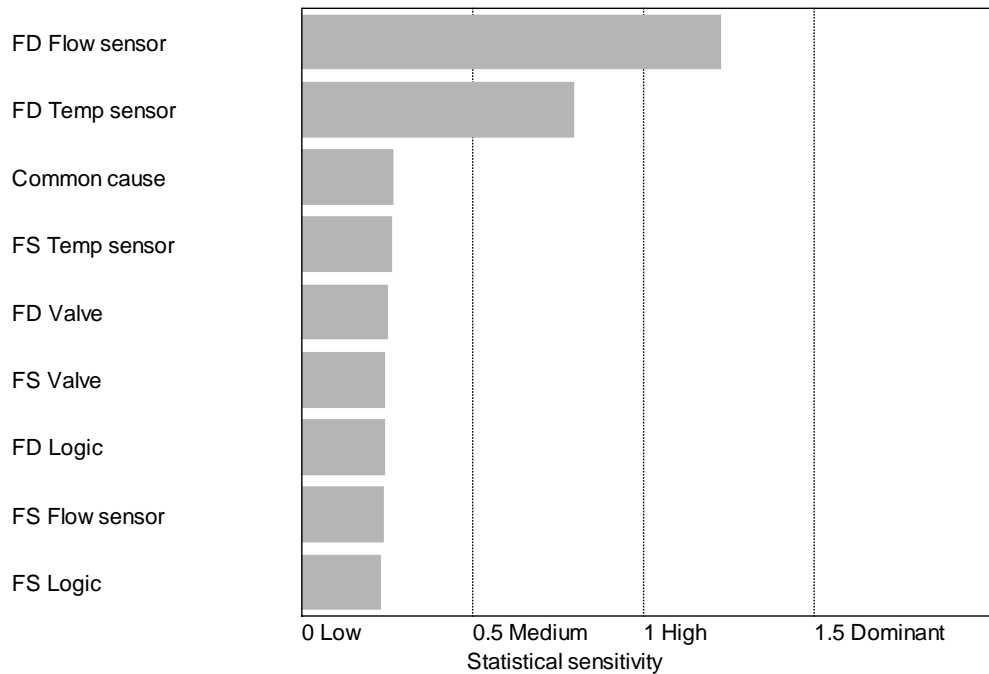
## 10 Results Example 1

To actually perform the calculations, the data from Table 4.1 in ISA-TR84.00.02-2002 – Part 1 has been used. For the logic solver, the assumption is made that it has a  $PFD_{\text{avg}}$  of 0.005. For more detail on how to evaluate the performance of the logic solver, see ISA-TR84.00.02-2002 – Part 5, which takes into account the important aspects of a logic solver like redundancy, voting, diagnostics capabilities, etc. In this example, the logic solver is modeled as one block. The probability of failure on demand and the probability of spurious trip are shown in Figure 10.1 and Figure 10.2, respectively. The theory behind the uncertainty and sensitivity plots is explained in ISA-TR84.00.02-2002 – Part 1, Clause 5.9.

Figure 10.1 shows the instantaneous PFD for the SIF as a function of the testing interval, TI. The  $PFD_{\text{avg}}$  can be calculated from Figure 10.1, by averaging the instantaneous values over 1 year. The  $PFD_{\text{avg}}$  is  $1.2 \times E-2$ , which means that this SIF has SIL 1 performance. The STR for example 1 can be calculated from Figure 10.2 and equals 0.303 per year. This is equivalent to a  $MTTF^{\text{spurious}}$  of 3.3 years.

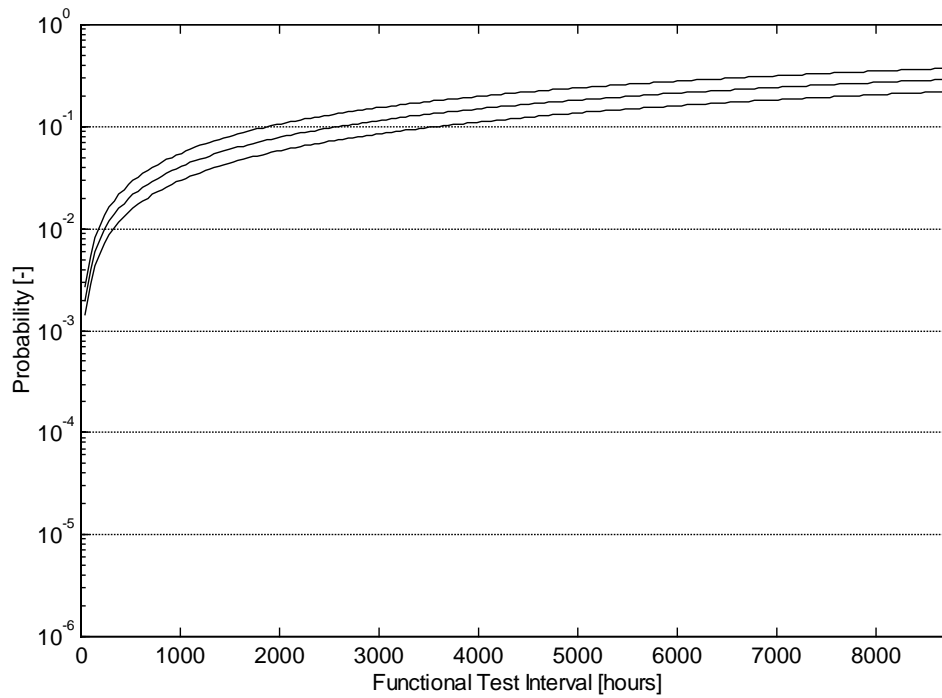


***PFD, Example 1, No Diagnostics***

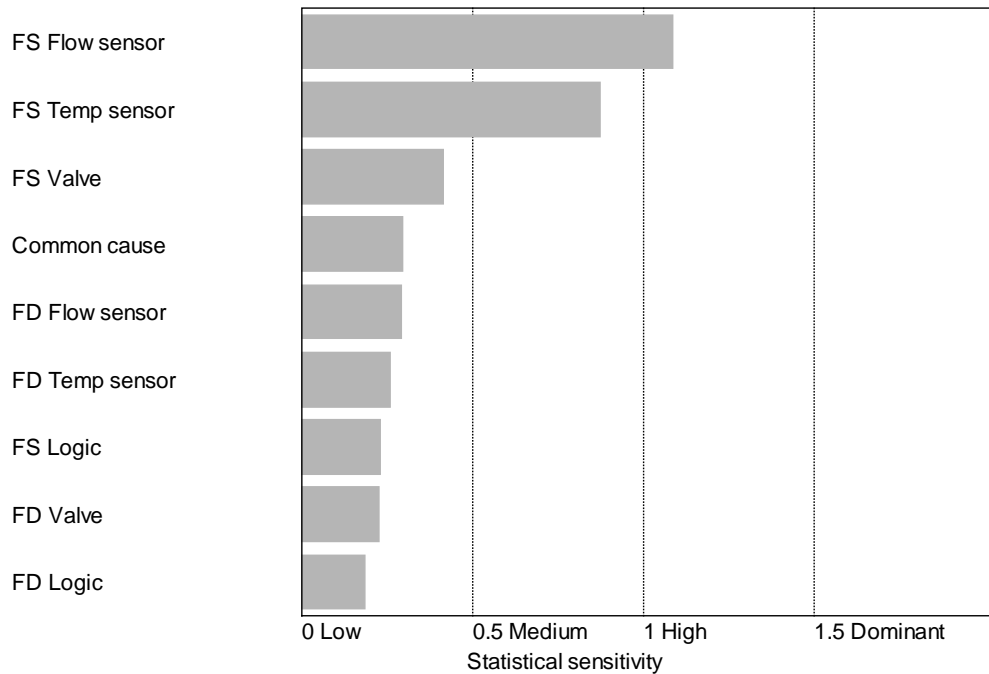


***Statistical Sensitivity Parameters for the PFD, Example 1, No Diagnostics***

**Figure 10.1 — PFD and sensitivity plot - Example 1**



***PFS, Example 1, No Diagnostics***



***Statistical Sensitivity Parameters of the PFS, Example 1, No Diagnostics***

**Figure 10.2 — Probability of spurious trip and sensitivity plot - Example 1**

## 11 Example 2

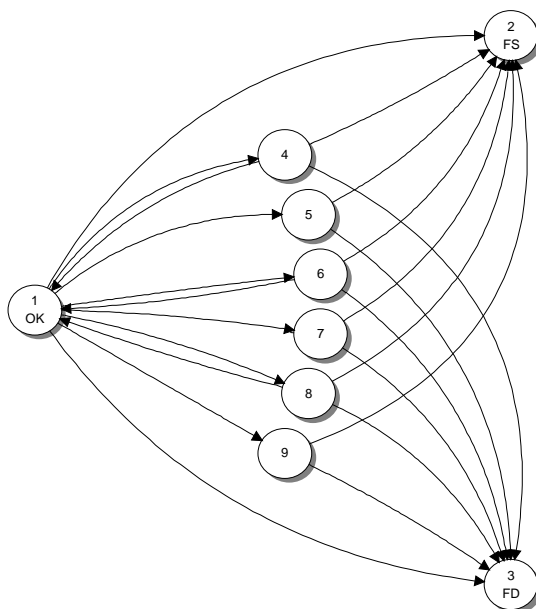
Example 2 is the same SIF as in Example 1. In this case, sensors and valve diagnostic capability is taken into account. This is intended to illustrate what impact the addition of diagnostic coverage to the architecture in Example 1 has on the attainable SIL. The use of the diagnostics coverage factor divides each of the safe and dangerous failures rates into a detected part and an undetected part. This means that a sensor or valve can now fail in four different ways, i.e., safe detected (SD), safe undetected (SU), dangerous detected (DD) and dangerous undetected (DU). Using these failure modes for the example in Figure 8.1, Table 11.1 can be created for the resulting states after a single failure. Failures that lead to an intermediate state and are detected can be repaired on-line.

**Table 11.1 — Resulting state after single failure with diagnostic capabilities - Examples 2**

Starting from Ok state			
Component	Failure Mode	Resulting State after single failure	Repair action
Flow Sensor 1a (S1)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	
Flow Sensor 1b (S1)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	
Temperature Sensor 2a (S2)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	
Temperature Sensor 2b (S2)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	



Logic Solver (L)*	S	FS	
	D	FD	
Valve 1a (A)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	
Valve 1b (A)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
	SCC	FS	
	DCC	FD	
S = Safe, SD = Safe Detected, SU = Safe Undetected, SCC = Safe Common Cause, D = Dangerous, DD = Dangerous Detected, DU = Dangerous Undetected, DCC = Dangerous Common Cause			
FS = Fail-safe, FD = Fail-dangerous, IS = Intermediate State			
* The data for the logic solver comes from the vendor (or the methodology used in Part 5).			



**Figure 11.1 — Simplified Markov model with diagnostics - Example 2**

Figure 11.1 shows the associated simplified Markov model taking into account sequences of only two failures that will lead to the fail-safe and fail-dangerous state.

Table 11.2 gives an overview of the states of Figure 11.1. Please note that Table 11.2 does not show any transitions between the different states and does not provide information on the specific failure that resulted in the current state. Each state gives the SIF status.

**Table 11.2 — Description of the different states of the SIS - Example 2**

State	Description of the state
1, OK	No failures, SIS operates without any component failed.
2, FS	A component failure caused a spurious trip of the SIS.
3, FD	A component failure caused a fail to function on demand of the SIS.
4	One Flow Sensor failed dangerous detected (but not both), the SIS still performs its function.
5	One Flow Sensor failed dangerous undetected (but not both), the SIS still performs its function.
6	One Temperature Sensor failed dangerous detected (but not both), the SIS still performs its function.
7	One Temperature Sensor failed dangerous undetected (but not both), the SIS still performs its function.
8	One Valve failed dangerous detected (but not both), the SIS still performs its function.
9	One Valve failed dangerous undetected (but not both), the SIS still performs its function.

The formulas belonging to this Markov model are presented next:

$$\lambda_{1,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S2}^S + \lambda_{S2}^S + \lambda_A^S]$$

$$\lambda_{1,3} = \lambda_L^D + \beta[\lambda_{S1}^D + \lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{1,4} = 2\lambda_{S1}^{DD} \quad \lambda_{4,1} = \mu_{OT}$$

$$\lambda_{1,5} = 2\lambda_{S1}^{DU}$$

$$\lambda_{1,6} = 2\lambda_{S2}^{DD} \quad \lambda_{6,1} = \mu_{OT}$$

$$\lambda_{1,7} = 2\lambda_{S2}^{DU}$$

$$\lambda_{1,8} = 2\lambda_A^{DD} \quad \lambda_{8,1} = \mu_{OT}$$

$$\lambda_{1,9} = 2\lambda_A^{DU}$$

$$\lambda_{4,2} = \lambda_{S1}^S + \lambda_{S1}^{DD} + 2\lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S2}^S + \lambda_A^S]$$

$$\lambda_{4,3} = \lambda_{S1}^{DU} + \lambda_L^D + \beta[\lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{5,2} = \lambda_{S1}^S + \lambda_{S1}^{DD} + 2\lambda_{S2}^S + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S2}^S + \lambda_A^S]$$

$$\lambda_{5,3} = \lambda_{S1}^{DU} + \lambda_L^D + \beta[\lambda_{S2}^D + \lambda_A^D]$$

$$\lambda_{6,2} = 2\lambda_{S1}^S + \lambda_{S2}^S + \lambda_{S2}^{DD} + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S1}^S + \lambda_A^S]$$

$$\lambda_{6,3} = \lambda_{S1}^{DU} + \lambda_L^D + \beta[\lambda_{S1}^D + \lambda_A^D]$$

$$\lambda_{7,2} = 2\lambda_{S1}^S + \lambda_{S2}^S + \lambda_{S2}^{DD} + \lambda_L^S + 2\lambda_A^S + \beta[\lambda_{S1}^S + \lambda_A^S]$$

$$\lambda_{7,3} = \lambda_{S2}^{DU} + \lambda_L^D + \beta[\lambda_{S1}^D + \lambda_A^D]$$

$$\lambda_{8,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + \lambda_A^S + \lambda_A^{DD} + \beta[\lambda_{S1}^S + \lambda_{S2}^S]$$

$$\lambda_{8,3} = \lambda_L^D + \lambda_A^{DU} + \beta[\lambda_{S1}^D + \lambda_{S2}^D]$$

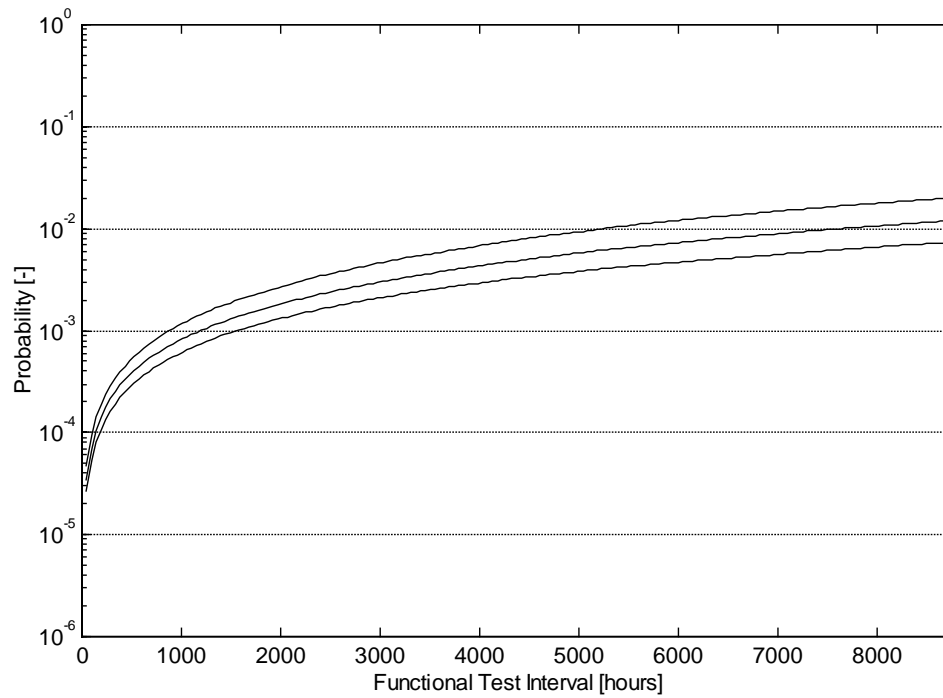
$$\lambda_{9,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + \lambda_L^S + \lambda_A^S + \lambda_A^{DD} + \beta[\lambda_{S1}^S + \lambda_{S1}^S]$$

$$\lambda_{9,3} = \lambda_L^D + \lambda_A^{DU} + \beta[\lambda_{S1}^D + \lambda_{S2}^D]$$

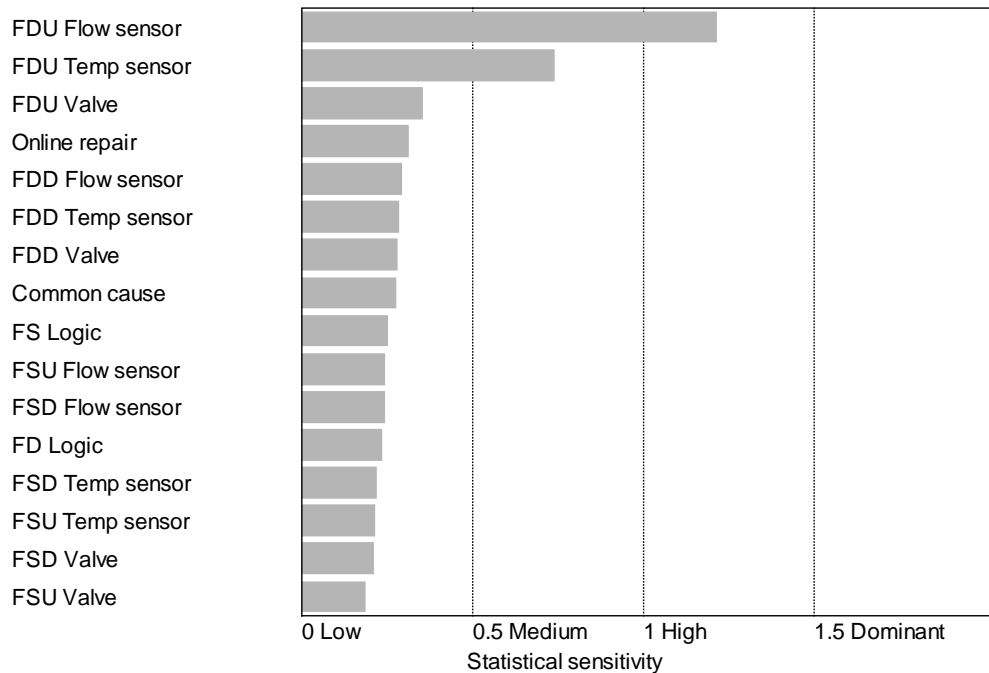
## 12 Results Example 2

To actually perform the calculations, the data from Table 4.1 in TR84.00.02-2002 - Part 1 has been used. For the logic solver, the assumption is made that it has a  $PFD_{avg}$  of 0.005. For more detail on how to evaluate the performance of the logic solver, see ISA-TR84.00.02-2002 – Part 5, which takes into account the important aspects of a logic solver like redundancy, voting, diagnostics capabilities, etc. In this example the logic solver is modeled as one block. The probability of failure on demand and the probability of spurious trip are shown respectively in Figure 12.1 and Figure 12.2. The theory behind the uncertainty and sensitivity plots is explained in ISA-TR84.00.02-2002 – Part 1, Clause 5.9.

Figure 12.1 shows the instantaneous PFD for the SIF as a function of the testing interval, TI. The  $PFD_{avg}$  can be calculated from Figure 12.1, by averaging the instantaneous values over 1 year. The  $PFD_{avg}$  is  $5.3 \times E-3$ , which means that this SIF has SIL 2 performance. The STR for example 2 can be calculated from Figure 12.2 and equals 0.303 per year. This is equivalent to a  $MTTF^{spurious}$  of 3.3 years.

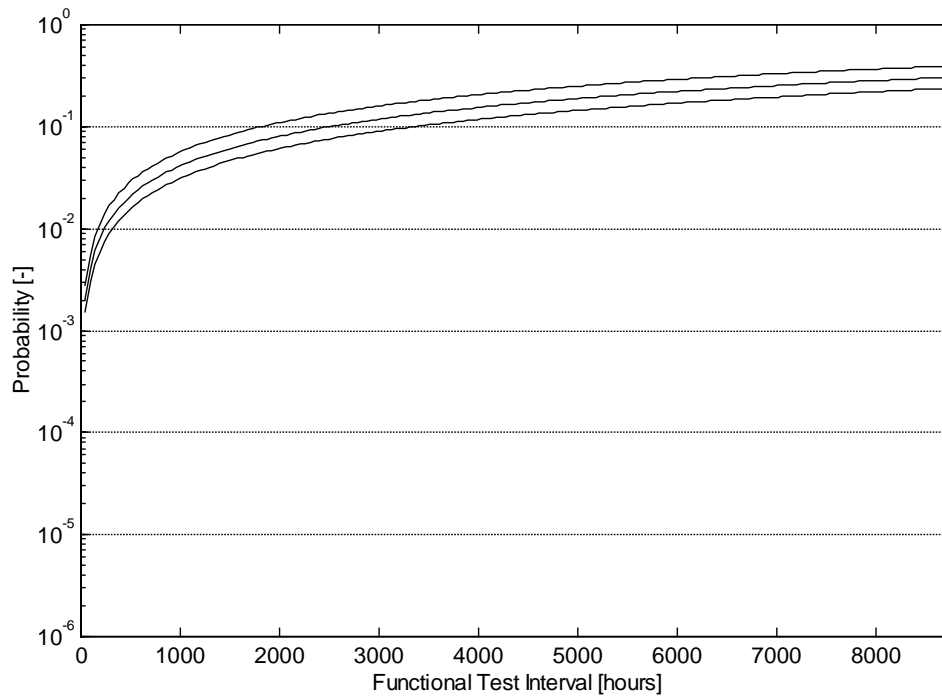


***PFD, Example 2, With Diagnostics***

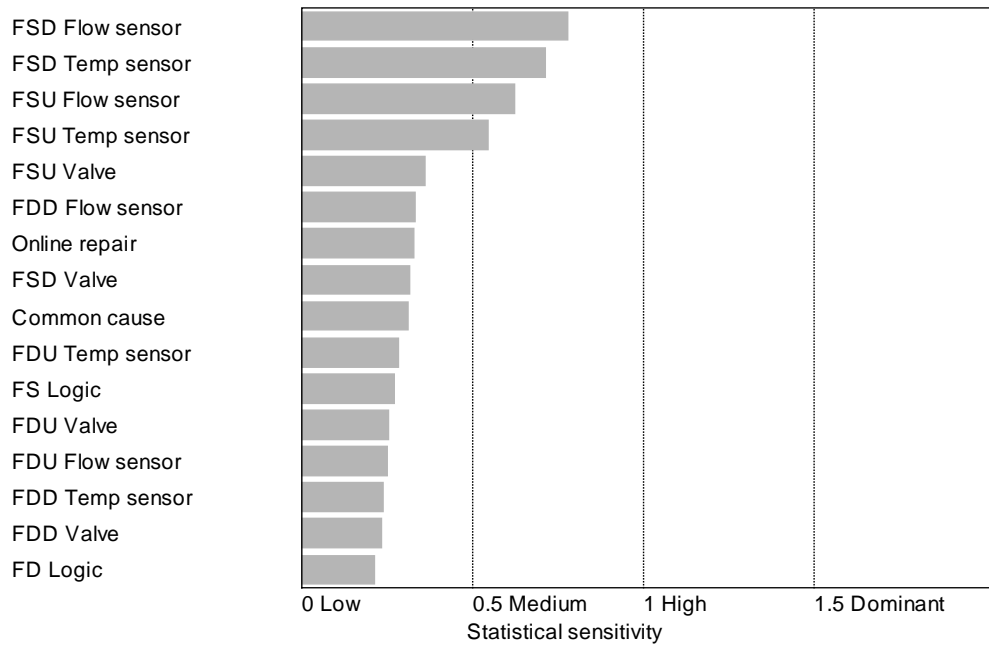


***Statistical Sensitivity PFD, Example 2, With Diagnostics***

**Figure 12.1 — Probability of fail on demand and sensitivity plot with diagnostics - Example 2**



**PFS Example 2 With Diagnostics**



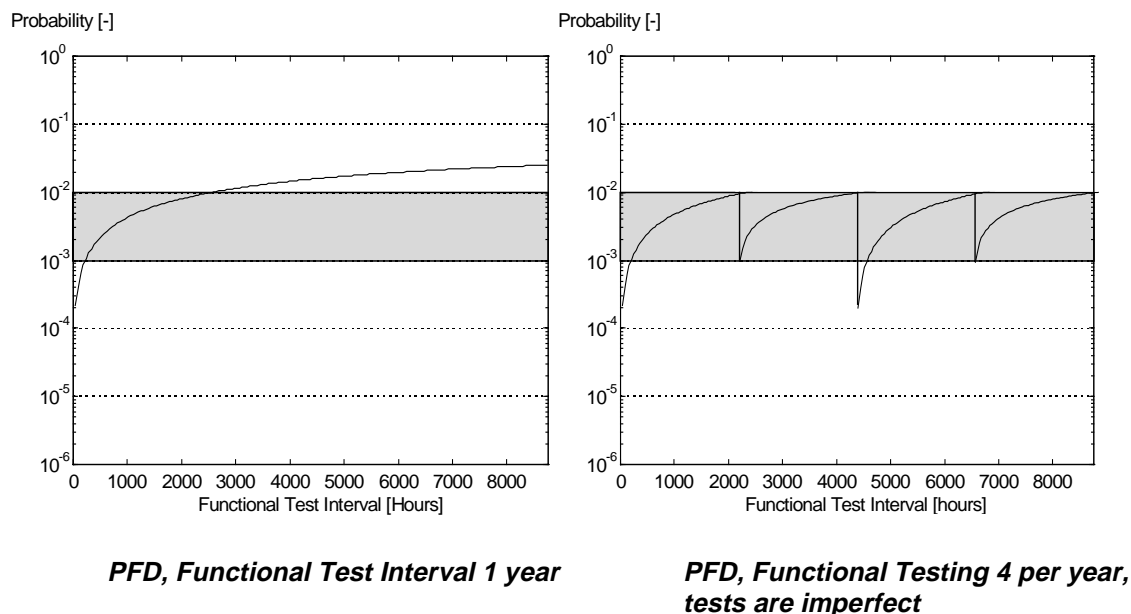
**Statistical Sensitivity PFS, Example 2, With Diagnostics**

**Figure 12.2 — PFS and sensitivity plot with diagnostics - Example 2**

### 13 Example 3

Example 1 and 2 clearly show that more detailed modeling of the SIF application can make a large difference in the results. Example 1, which did not include diagnostics capabilities of the sensors and valves, resulted in a lower SIL level than Example 2, which included the diagnostic capability of the redundant components. The Markov approach can account for the diagnostic coverage without introducing additional complexity concerning the model or the analysis of the model.

The following example includes two modeling features that can easily be included in a Markov model. The modeling features highlighted are periodic testing and imperfect testing. It is assumed that an existing SIF application has a PFD as presented in the left graph of Figure 13.1. The required SIL of the SIF application is SIL 2. With the current functional test interval of one (1) year, it is clear that most of the time the PFD does not reach a SIL 2. It is decided that the SIF application will be subject to four Functional Tests, one every three months. These tests are very simple and will not find every failure in the SIF application, which means that they are imperfect. The results of the quarterly functional imperfect testing are shown in the right graph of Figure 13.1. By testing the SIS on an increased basis, it can be seen that it is possible to keep the SIS application in the SIL 2 range. The second functional test, carried out after 6 months, is a better test than the two tests carried out after 3 and 9 months and results in a larger drop in PFD. From this example, it can be seen that it is possible to model different functional tests where each test can have a different coverage.



**Figure 13.1 — PFD before and after periodic and imperfect testing**

For a SIF application, it is possible to include important design, installation, and testing aspects and model it in one Markov model. For example, one Markov model can include all the information necessary to calculate the PFD and PFS of the SIS application, including different failure modes for different components, diverse components, sequences of failures in time, systematic failures and common cause failures, different repair strategies for different components, functional testing, imperfect testing (repair) and all of this as a function of time.

## 14 Base example calculation for an SIF using Markov models

The following example, see Figure 14.1, is the base example that can also be found in ISA-TR84.00.02-2002 – Part 2 and ISA-TR84.00.02-2002 – Part 3. In this example, a tank is equipped with four safeguards to reduce the risk associated with the involved hazards. The SIF used to protect the process is presented in Figure 14.2.

This SIF is evaluated to demonstrate the procedure for calculating a SIF  $PFD_{avg}$  and  $MTTF^{spurious}$ . **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 the SIS components:

1. All inputs and outputs in the example are assumed to be part of the same SIF. Therefore a single  $PFD_{avg}$  and a single  $MTTF^{spurious}$  are calculated for the entire SIF.
2. In a process hazards analysis, it was determined that the SIF should have a SIL 2.
3. The SIF is designed as de-energize to trip and will go to a safe state on loss of power. The  $MTTF^{spurious}$  of the power supply is assumed to be 20 years.
4. Redundant AC power supplies (2) are provided external to the system.
5. All redundant devices are assumed to have the same failure rate.
6. The logic solver is a PES with output redundancy to prevent unsafe failure of an output and has an external watchdog circuit. The  $PFD_L$  and  $MTTF^{spurious}$  for the logic solver are assumed values. The  $PFD_{avg}$  is 0.005 and the  $MTTF^{spurious}$  is 10 years.

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

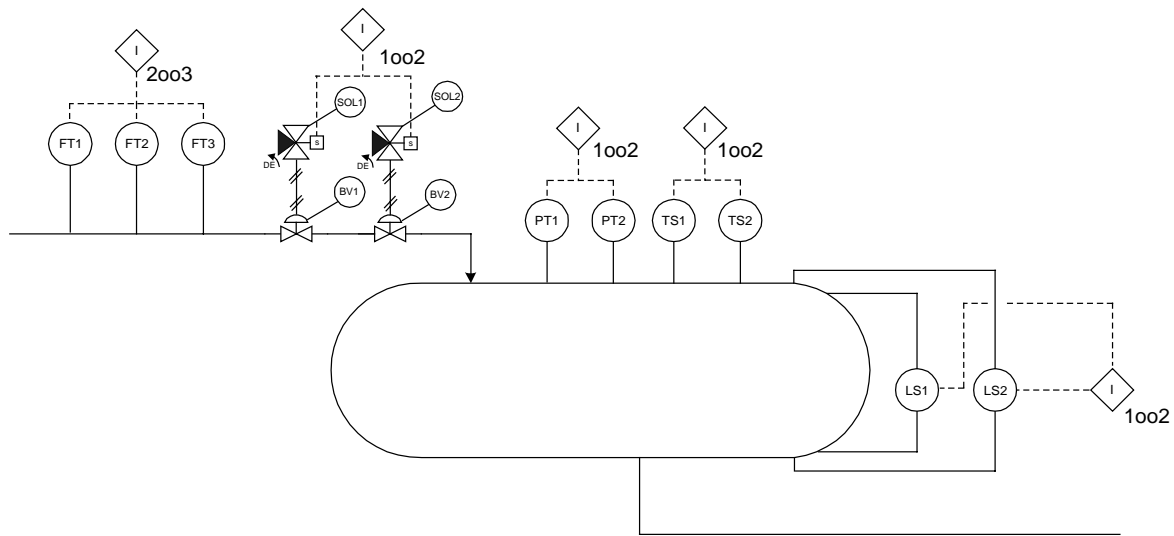
7. It is generally assumed that when a dangerous detected failure occurs, the SIF will take the process to a safe state or plant personnel will take necessary action to ensure the process is safe (operator response is assumed to be before a demand occurs and  $PFD$  of operator response is assumed to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

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

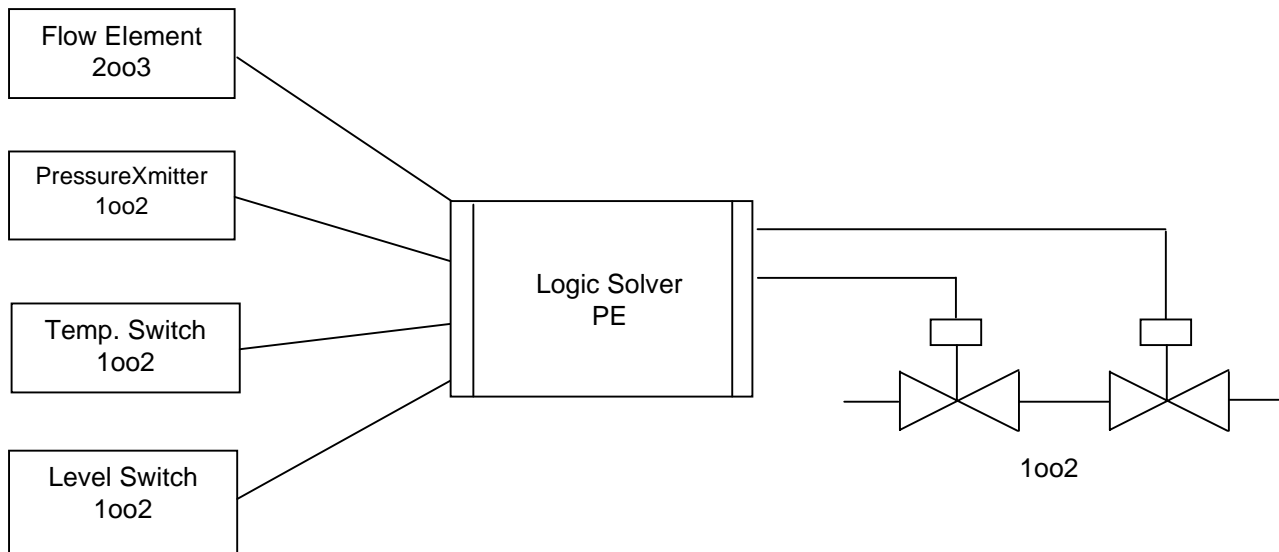
8. A one (1) year functional test interval is assumed for the SIF components. Testing is assumed to be perfect.
9. The mean time to repair is assumed to be 8 hours, and the repair is assumed to be perfect.
10. The effects of common cause and systematic errors are assumed to be negligible in the calculations.
11. 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.
13. The data used to perform the calculations is taken from Clause 6 in ISA-TR84.00.02-2002 – Part 2.

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





**Figure 14.1 — SIS process diagram - Base example**



**Figure 14.2 — SIS configuration - Base example**

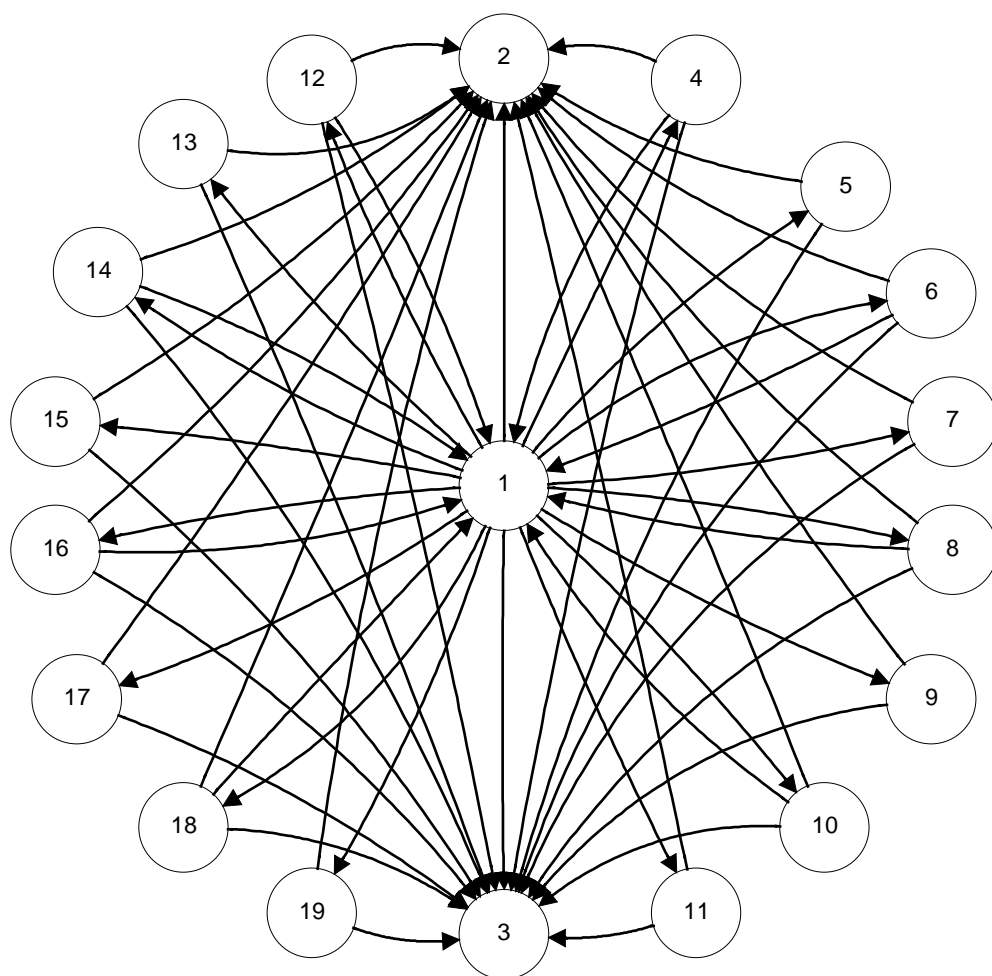
Table 14.1 shows the resulting state after a single failure.

**Table 14.1 — Resulting state after single failure - Base example**

<b>Starting from OK state</b>			
<b>Component</b>	<b>Failure Mode</b>	<b>Resulting State after single failure</b>	<b>Repair action</b>
Flow Sensor 1a (S1)	SD	IS	on-line
	SU	IS	
	DD	IS	online
	DU	IS	
Flow Sensor 1b (S1)	SD	IS	on-line
	SU	IS	
	DD	IS	online
	DU	IS	
Flow Sensor 1c (S1)	SD	IS	on-line
	SU	IS	
	DD	IS	online
	DU	IS	
Pressure Sensor 2a (S2)	SD	FS	
	SU	FS	
	DD	IS	on-line
	DU	IS	
Pressure Sensor 2b (S2)	SD	FS	
	SU	FS	
	DD	IS	on-line
	DU	IS	
Temperature Sensor 3a (S3)	SD	FS	
	SU	FS	
	DD	IS	on-line
	DU	IS	
Temperature Sensor 3b (S3)	SD	FS	
	SU	FS	
	DD	IS	on-line
	DU	IS	
Level Sensor 4a (S4)	SD	FS	
	SU	FS	
	DD	IS	on-line
	DU	IS	

Level Sensor 4b (S4)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
Logic Solver (L)*	S	FS	
	D	FD	
Solenoid Valve 1a (A1)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
Solenoid Valve 1b (A1)	SD	FS	on-line
	SU	FS	
	DD	ID	
	DU	ID	
Valve 1a (A2)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
Valve 1b (A2)	SD	FS	on-line
	SU	FS	
	DD	IS	
	DU	IS	
Power supply 1a (PS)	SD	IS	on-line
	SU	IS	
Power supply 1b (PS)	SD	IS	on-line
	SU	IS	
S = Safe, D = Dangerous, SD = Safe Detected, SU = Safe Undetected, DD = Dangerous Detected DU = Dangerous Undetected, FS = Fail-safe, FD = Fail-dangerous, IS = Intermediate State			
* The data for the logic solver comes from the vendor (or the methodology used in Part 5).			

Figure 14.3 shows the associated Markov model taking into account only sequences of two failures that will lead to the fail-safe and fail-dangerous state.



### Figure 14.3 — Simplified Markov model - Base example

Table 14.2 gives an overview of the states of Figure 14.3. Please note that Table 14.2 does not say anything about the transitions between the different states. Each state gives the current status of the SIS. How the SIS got into this state is not described in this table.

**Table 14.2 — Description of the different states of the SIS - Base example**

State	Description of the states
1, OK	No failures, SIS operates without any component failed.
2, FS	A component failure caused a spurious trip of the SIS.
3, FD	A component failure caused a fail to function on demand of the SIS.
4	One Flow sensor failed safe detected (but not all three of them), the SIS still performs its function.
5	One Flow sensor failed safe undetected (but not all three of them), the SIS still performs its function.
6	One Flow sensor failed dangerous detected (but not all three of them), the SIS still performs its function.
7	One Flow sensor failed dangerous undetected (but not all three of them), the SIS still performs its function.
8	One Pressure sensor failed dangerous detected (but not both), the SIS still performs its function.
9	One Pressure sensor failed dangerous undetected (but not both), the SIS still performs its function.
10	One Temperature sensor failed dangerous detected (but not both), the SIS still performs its function.
11	One Temperature sensor failed dangerous undetected (but not both), the SIS still performs its function.
12	One Level sensor failed dangerous detected (but not both), the SIS still performs its function.
13	One Level sensor failed dangerous undetected (but not both), the SIS still performs its function.
14	One Solenoid Valve failed dangerous detected (but not both), the SIS still performs its function.
15	One Solenoid Valve failed dangerous undetected (but not both), the SIS still performs its function.
16	One Valve sensor failed dangerous detected (but not both), the SIS still performs its function.
17	One Valve sensor failed dangerous undetected (but not both), the SIS still performs its function.
18	One Power supply failed safe detected (but not both), the SIS still performs its function.
19	One Power supply failed safe undetected (but not both), the SIS still performs its function.

The formulas belonging to this Markov model are presented next:

$$\lambda_{1,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{1,3} = \lambda_L^D$$

$$\lambda_{1,4} = 3\lambda_{S1}^{SD} \quad \lambda_{4,1} = \mu_{OT}$$

$$\lambda_{4,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{4,3} = \lambda_L^D$$

$$\lambda_{1,5} = 3\lambda_{S1}^{SU}$$

$$\lambda_{5,2} = 2\lambda_{S1}^S + 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{5,3} = \lambda_L^D$$

$$\lambda_{1,6} = 3\lambda_{S1}^{DD} \quad \lambda_{6,1} = \mu_{OT}$$

$$\lambda_{6,2} = 2\lambda_{S1}^{DD} + 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{6,3} = \lambda_L^D$$

$$\lambda_{1,7} = 3\lambda_{S1}^{DU}$$

$$\lambda_{7,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{7,3} = 2\lambda_{S1}^{DU} + 2\lambda_{S1}^{DD} + \lambda_L^D$$

$$\lambda_{1,8} = 2\lambda_{S2}^{DD} \quad \lambda_{8,1} = \mu_{OT}$$

$$\lambda_{8,2} = \lambda_{S2}^S + \lambda_{S2}^{DD} + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{8,3} = \lambda_{S2}^{DU} + \lambda_L^D$$

$$\lambda_{1,9} = 2\lambda_{S2}^{DU}$$

$$\lambda_{9,2} = \lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{9,3} = \lambda_{S2}^{DD} + \lambda_{S2}^{DU} + \lambda_L^D$$

$$\lambda_{1,10} = 2\lambda_{S3}^{DD} \quad \lambda_{10,1} = \mu_{OT}$$

$$\lambda_{10,2} = 2\lambda_{S2}^S + \lambda_{S3}^S + \lambda_{S3}^{DD} + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{10,3} = \lambda_{S3}^{DU} + \lambda_L^D$$

$$\lambda_{1,11} = 2\lambda_{S3}^{DU}$$

$$\lambda_{11,2} = 2\lambda_{S2}^S + \lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{11,3} = \lambda_{S3}^{DD} + \lambda_{S3}^{DU} + \lambda_L^D$$

$$\lambda_{1,12} = 2\lambda_{S4}^{DD} \quad \lambda_{12,1} = \mu_{OT}$$

$$\lambda_{12,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + \lambda_{S4}^S + \lambda_{S4}^{DD} + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{12,3} = \lambda_{S4}^{DU} + \lambda_L^D$$

$$\lambda_{1,13} = 2\lambda_{S4}^{DU}$$

$$\lambda_{13,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + \lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{13,3} = \lambda_{S4}^{DD} + \lambda_{S4}^{DU} + \lambda_L^D$$

$$\lambda_{1,14} = 2\lambda_{A1}^{DD} \quad \lambda_{14,1} = \mu_{OT}$$

$$\lambda_{14,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + \lambda_{A1}^S + \lambda_{A1}^{DD} + 2\lambda_{A2}^S + \lambda_{A2}^{DD}$$

$$\lambda_{14,3} = \lambda_{A1}^{DU} + \lambda_{A2}^{DU} + \lambda_L^D$$

$$\lambda_{1,15} = 2\lambda_{A1}^{DU}$$

$$\lambda_{15,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + \lambda_{A1}^S + 2\lambda_{A2}^S$$

$$\lambda_{15,3} = \lambda_{A1}^{DD} + \lambda_{A1}^{DU} + \lambda_{A2}^{DD} + \lambda_{A2}^{DU} + \lambda_L^D$$

$$\lambda_{1,16} = 2\lambda_{A2}^{DD} \quad \lambda_{16,1} = \mu_{OT}$$

$$\lambda_{16,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + \lambda_{A1}^{DD} + \lambda_{A2}^S + \lambda_{A2}^{DD}$$

$$\lambda_{16,3} = \lambda_{A1}^{DU} + \lambda_{A2}^{DU} + \lambda_L^D$$

$$\lambda_{1,17} = 2\lambda_{A2}^{DU}$$

$$\lambda_{17,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + \lambda_{A2}^S$$

$$\lambda_{17,3} = \lambda_{A1}^{DD} + \lambda_{A1}^{DU} + \lambda_{A2}^{DD} + \lambda_{A2}^{DU} + \lambda_L^D$$

$$\lambda_{1,18} = 2\lambda_{PS}^{SD} \quad \lambda_{18,1} = \mu_{OT}$$

$$\lambda_{18,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S + \lambda_{PS}^S$$

$$\lambda_{18,3} = \lambda_L^D$$

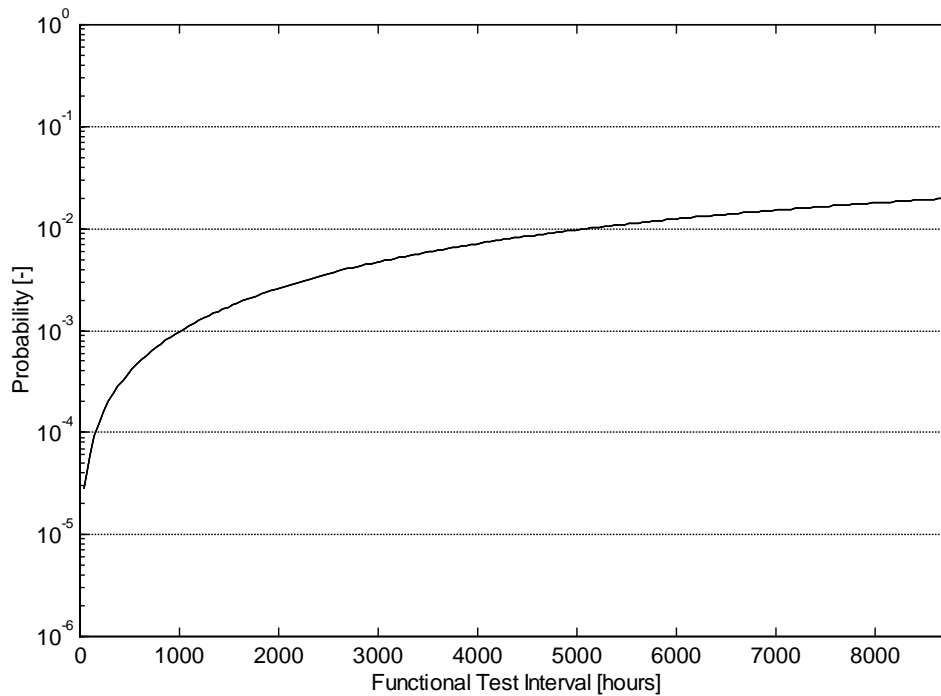
$$\lambda_{1,19} = 2\lambda_{PS}^{SU}$$

$$\lambda_{19,2} = 2\lambda_{S2}^S + 2\lambda_{S3}^S + 2\lambda_{S4}^S + \lambda_L^S + 2\lambda_{A1}^S + 2\lambda_{A2}^S + \lambda_{PS}^S$$

$$\lambda_{19,3} = \lambda_L^D$$

## 15 Results base example

Using the data from ISA-TR84.00.02-2002 – Part 1 and the assumptions from ISA-TR84.00.02-2002 – Part 2, the results shown in Figure 15.1 and Figure 15.2 are obtained. The logic solver is assumed to have a  $PFD_{avg}$  of 0.005 and  $MTTF^{spurious}$  of 10 years.



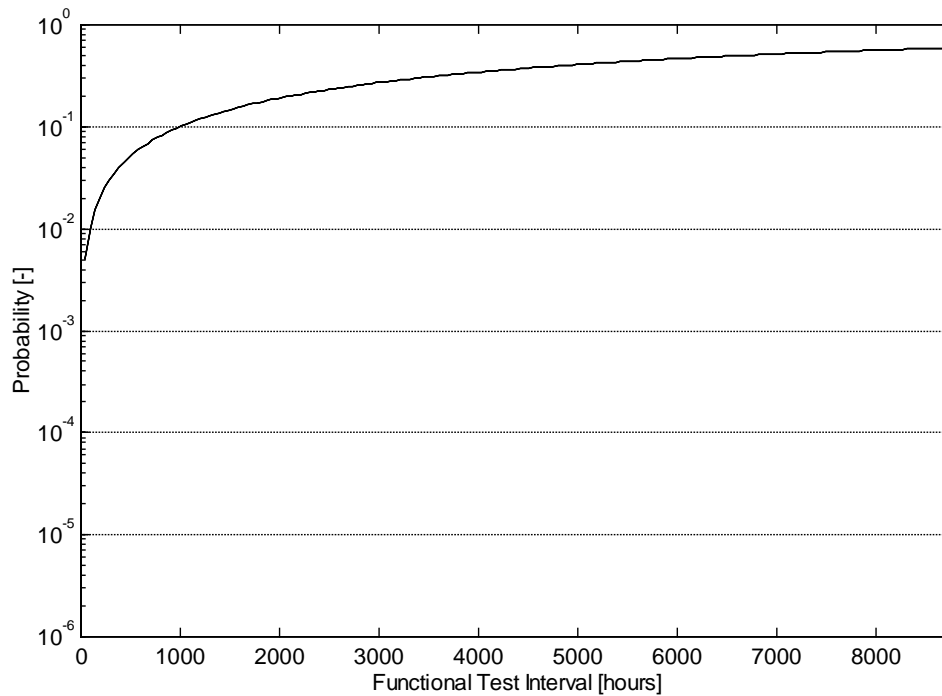
**PFD, Base Example**

**Figure 15.1 — Probability of failure on demand - Base example**

Figure 15.1 shows the instantaneous PFD for the SIF as a function of the testing interval, TI. The  $PFD_{avg}$  for the Base Example can be calculated from Figure 15.1, by averaging the instantaneous values over 1 year. The  $PFD_{avg}$  equals  $8.3 \times 10^{-3}$ , which means that this SIF meets a SIL 2 performance. Next, the calculated  $PFD_{avg}$  should be compared to the target SIL specified in the Safety Requirements



Specification (See ANSI/ISA-84.01-1996, Clause 5 and Clause 6.2.2) for each SIF. Since the target SIL is SIL 2, the SIF does meet the specification.



*PFS, Base Example*

**Figure 15.2 — Probability of spurious trip - Base example**

The STR for the base case example can be calculated from Figure 15.2 and equals 0.59 per year. This is equivalent to a  $MTTF^{spurious}$  of 1.7 years.

## 16 Index

accuracy	13
<b>architecture(s)</b>	9, 10, 21, 22, 32
assessment	9
availability	11, 13, 18
boundary(ies)	12
calculation(s)	14, 19, 20, 21, 28, 29, 35, 39
code(s)	27
common cause	11, 14, 15, 19, 21, 26, 38, 39
common cause failure(s)	14, 15, 21, 26, 38
complex	13, 27
computational	19
<b>configuration(s)</b>	9, 11, 14, 15, 19, 20
cost	14
coverage	9, 15, 17, 32, 38
coverage factor	32
covert	17
covert fault(s)	17
current	19, 25, 34, 38, 45
dangerous detected failure(s)	20, 39
de-energize(d) to trip	21, 39
de-energized	21
definitions	14
demand	9, 11, 13, 19, 21, 25, 29, 34, 35, 39, 45
demand mode	11, 13
designer	9, 14
diagnostic coverage	9, 15, 17, 32

diagnostic(s)	9, 15, 17, 19, 21, 29, 32, 35, 38, 40
diagram	13
diverse	38
diversity	9, 13, 26
document(s)	9, 11, 12, 13, 14, 21, 39
documents	11, 12, 13, 14
errors	39
fail-safe	21, 26, 27, 33, 43
Failure Mode and Effect Analysis (FMEA)	19, 22
failure mode(s)	17, 19, 20, 22, 32
failure rate data	14
failure rate(s)	14, 17, 20, 22, 26, 28, 39
false	14
fault tree(s)	13
field device(s)	9
final control element(s) [See field device(s)]	19, 20
<b>final element(s) [See field device(s)]</b>	11, 14, 20
flow	22, 26
frequency	9, 13
function	11, 13, 15
function(s)	9, 10, 11, 13, 15, 18, 19, 21, 22, 25, 29, 34, 38, 39, 45, 49
functional test interval	19, 38, 39
functional test(s)	19, 38, 39
functional testing	38
hardware	9, 13, 14, 19
hardware configuration	19
hazard(s)	9, 39
hazardous	14

hazardous event(s)	14
identical	22, 32
IEC	14
industry	9, 11, 26
input module(s)	20
inspection(s)	9, 13
inspections	13
<b>installation</b>	11
internal	18
life cycle	11
<b>logic solver(s)</b>	11, 14, 15, 19, 20, 22, 29, 33, 35, 39, 43, 48
maintenance	9, 10, 11, 13, 15
<b>Markov analysis</b>	9, 10, 14
Markov modeling	17, 18, 19
measure(s)	11, 13
mode(s)	11, 13, 17, 19, 20, 22, 32, 38
modeling	14, 15, 17, 18, 19, 20, 21, 38
modification(s)	13
MTTFspurious	10, 39, 48
nuisance trip	9, 14
objective(s)	14
off-line	19
on-line	19, 22, 32, 33, 42, 43
operator response	20, 39
operator(s)	15, 20, 39
output(s) [See input/output devices and input/output modules]	20, 39
panel(s)	9
parameter(s)	9, 14, 15

period(s)	13, 14
PFDavg	10, 17, 19, 21, 29, 35, 39, 48
plant	20, 21, 39
power	21, 28, 39
power supply(ies)	21, 39
process industry(ies)	9, 11
program(s)	19
Programmable Electronic System(s) (PES)	9, 10, 14, 39
purpose(s)	9, 40
quality	9, 13
quantified	27
quantitative	14, 26
redundancy	9, 13, 17, 20, 26, 29, 35, 39
redundant	11, 39
reference(s)	11
reliability	9, 10, 13, 20
repair(s)	15, 18, 19, 20, 22, 38, 39
response(s)	21, 39
risk assessment	9
risk reduction	11
risk(s)	9, 11, 39
safe	14, 20, 21, 22, 26, 27, 32, 33, 39, 43, 45
safe state(s)	20, 21, 26, 39
safety availability	11, 13
safety function(s)	9, 11, 13, 19, 21, 39, 49
<b>Safety Instrumented System(s) (SIS)</b>	9, 10, 11, 12, 13, 14, 17, 19, 20, 21, 22, 25, 26, 34, 38, 39, 40, 41, 45
safety integrity	11, 13, 14

<b>Safety Integrity Level (SIL)</b>	9, 10, 11, 17
<b>Safety Integrity Level (SIL) Evaluation Techniques</b>	9, 10, 17
<b>sensor(s) [See field device(s)]</b>	11, 14, 19, 20, 21, 22, 26, 32, 38, 45
sequence(s) of failure(s)	19, 38
sequencer(s) of failure(s)	19, 38
shutdown	14, 22
SIL 1	11, 22, 29
SIL 2	35, 38, 39, 48
simple	38
SIS application(s)	38
SIS architecture	9, 10
SIS components	10, 39
software	9, 13, 15
spurious trip(s)	14, 19, 20, 21, 22, 25, 29, 34, 35, 45
supplier(s)	9
system analysis techniques	14
systematic error(s)	39
systematic failure(s)	13, 14, 15, 19, 38
team	9
temperature	22, 26
terminology	18
Test Interval (TI)	17, 19, 20, 38, 39
test(s)	17, 19, 20, 38, 39
testing	9, 13, 19, 38, 39
time(s)	13, 14, 15, 19, 20, 21, 22, 27, 28, 29, 38
TR84.00.02	9, 10, 11, 14, 16, 17, 18, 20, 21, 27, 28, 29, 35, 39, 48
transistor(s)	18
trip(s)	9, 14, 19, 20, 21, 22, 25, 29, 34, 35, 39, 45

validation	17
valve(s)	20, 21, 22, 26, 32, 38
variable(s)	28
vendor(s)	20, 33, 39, 43
voting	26, 29, 35
watchdog	39
watchdog circuit	39

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: 1-55617-805-0