

TECHNICAL REPORT

ISA-TR84.00.02-2015

**Safety Integrity Level (SIL)
Verification of Safety
Instrumented Functions**

Approved 8 September 2015

ISA-TR84.00.02-2015, Safety Integrity Level (SIL) Verification of Safety Instrumented Functions

ISBN: 978-1-941546-70-3

Copyright © 2015 by ISA. 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-TR84.00.02-2015.

This document has been prepared as part of the service of ISA 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, NC27709; 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 DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NON-DISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

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

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

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 voting members of ISA Committee ISA84:

NAME	AFFILIATION
W. Johnson, Jr., Chair	Consultant
V. Maggioli, Sr., Co-Managing Director	Feltronics Corp.
D. Zetterberg, Co-Managing Director	Chevron Energy Technology Co.
R. Adamski	RA Safety Consulting LLC
T. Ando	Yokogawa China Co. Ltd.
R. Avali	Westinghouse Electric Corp.
M. Balsubramanian	ExxonMobil Research & Engineering
L. Beckman	Safeplex Systems Inc.
D. Bennett	Phillips 66
J. Campbell	Consultant
I. Chen	Aramco
R. Chittilapilly	Oil & Natural Gas Corp.
R. Dunn	DuPont Engineering
P. Early	Langdon Coffman Services
C. Fialkowski	Siemens Industry Inc.
K. Gandhi	Kellogg Brown & Root
I. Gibson	Consultant
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida
P. Gruhn	Rockwell Automation
J. Harris	UOP A Honeywell Company
F. Hendi	Schneider Electric
J. Jamison	Encana Corp.
R. Johnson	Engineering Solutions
P. Kannan	Woodgroup CCC
L. Laskowski	Emerson
D. Lyons	Valero Energy Corp.
E. Marszal	Kenexis
N. McLeod	Arkema
M. Mollicone	SYM Consultoria
N. Muthiah	Wood Group Mustang Inc
J. Neeley	CH2M HILL
B. Shashank Pataskar	Bayer
G. Ramachandran	Systems Research International Inc.
R. Roberts	Suncor Energy Inc
M. Scott	ae Solutions
C. Sossman	CLS Tech-Reg Consultants
R. Strube	Universal Instruments Corporation
A. Summers	SIS-TECH Solutions LP.

L. Suttinger
K. Szafron
T. Walczak
M. Weber
A. Woltman
P. Wright

Savannah River Nuclear Solutions LLC
BP
Conversions Inc.
System Safety Inc.
Shell Projects and Technology-Engineering
BHP Engineering & Construction Inc.

This published standard was approved for publication by the ISA Standards and Practices Board on 8 September 2015.

NAME**AFFILIATION**

N. Sands, Vice President
D. Bartusiak
P. Brett
E. Cosman
D. Dunn
J. Federlein
B. Fitzpatrick
J. Gilsinn
J. Hauet
J. Jamison
K. P. Lindner
V. Maggioli
T. McAvinew
V. Mezzano
C. Monchinski
H. Sasajima
T. Schnaare
J. Tatera
K. Unger
I. Verhappen
W. Weidman
J. Weiss
M. Wilkins
D. Zetterberg

DuPont
ExxonMobil Research & Engineering
Honeywell Inc.
OIT Concepts, LLC
Phillips 66
Federlein & Assoc. Inc.
Wood Group Mustang
Kenexis Consulting
KB Intelligence
Encana Corp.
Endress + Hauser Process Solutions AG
Feltronics Corp.
Instrumentation and Control Engineering, LLC
Fluor Corporation
Automated Control Concepts Inc.
Azbil Corp.
Rosemount Inc.
Tatera & Associates Inc.
Stone Technologies Inc.
Orbis Engineering Field Services
Consultant
Applied Control Solutions LLC
Yokogawa IA Global Marketing (USMK)
Chevron Energy Technology Co.

This page intentionally left blank.

Contents

1	Introduction	13
2	Scope	15
3	Background	16
4	Cautions	18
5	Nature of failures.....	20
5.1	Device failure	20
5.2	Failure causes and mechanisms	23
5.3	Failure classification	29
5.4	Failure rates	32
6	Average probability of failure on demand	40
6.1	Effect of out-of-service periods.....	42
6.2	Effect of partial testing	44
6.3	Effect of voting	45
6.4	Effect of test intervals and diagnostics	46
6.5	Effect of common cause	47
7	Spurious trip rate.....	48
8	SIF calculation overview	50
9	Special topics.....	54
9.1	Systematic failure and the management system.....	54
9.2	Methods to analyze the performance of equipment with revealed failures	55
9.3	Single sided confidence limit	56
9.4	Software packages	57
	Annex A—Abbreviations, acronyms and symbols.....	59
	Annex B—Definitions	61
	Annex C—Probability of failure.....	69
	Annex D—Fault Tree Analysis.....	79

Annex E–Markov Analysis	85
Annex F–Calculation examples	99
Annex G–Field device failure modes and their detection	127
Annex H–References	133

Foreword

ISA-84.00.01-2004 Part 1 gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. These requirements are presented in the 2004 standard using the safety lifecycle shown in ISA-84.00.01-2004 Part 1 Figure 8 and described in Part 1 Table 2.

The ISA84 committee has developed a series of complimentary technical reports to provide guidance, as well as practical examples of implementation, on various topics and applications. Three of these technical reports, TR84.00.02, TR84.00.03 and TR84.00.04, provide informative guidance related to specific phases of the SIS lifecycle. Figure 1 and Table 2 have been adapted for this foreword as shown in TR84.00.02 Figure 1 and Table 1, respectively. A brief overview of each technical report is given below including the report's relationship to the lifecycle requirements and the intended scope of each report's guidance.

TR84.00.02—Safety Integrity Level (SIL) Verification of Safety Instrumented Functions—Lifecycle phase 4 (Figure 1/Table 1) requires verification that the intended or installed SIS meets its specified safety integrity level (SIL). To support the calculation of the average probability of failure on demand as required by ISA 84.00.01-1 Clause 11.9, ISA-TR84.00.02 provides guidance on the following: a) assessing random and systematic failures, failure modes and failure rates; b) understanding the impact of diagnostics and mechanical integrity (MI) activities on the SIL and reliability; c) identifying sources of common cause, common mode and systematic failures; and d) using quantitative methodologies to verify the SIL and spurious trip rate. The approaches outlined in this document are performance-based; consequently, the reader is cautioned to understand that the examples provided do not represent prescriptive architectural configurations or MI requirements for any given SIL. Once a SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured MI program as described in TR84.00.03.

TR84.00.03—Mechanical Integrity of Safety Instrumented Systems (SIS)—Lifecycle phases 5 and 6 (Figure 1/Table 1) involve the installation and testing of the SIS, the validation that the SIS meets the safety requirements specification, and the assurance that functional safety is maintained during long term operation and maintenance. An important aspect of achieving and maintaining the SIS integrity and its specified SIL is the implementation of an MI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective MI program that demonstrates through traceable and auditable documentation that the SIS and its equipment are maintained in the "as good as new" condition. The technical report addresses the identification of personnel roles and responsibilities when establishing an MI plan, important considerations in establishing an effective MI program, and detailed examples to illustrate user work processes used to support various activities of the MI program. Data and information collected as part of the MI program can be used to validate the SIL Verification calculations as discussed in TR84.00.02 and the selection and continued use of devices as discussed in TR84.00.04 Annex L.

TR84.00.04—Guidelines for the Implementation of ISA 84.00.01—Lifecycle phases 2, 4, 9 and 10 (Figure 1/Table 1) address the management of functional safety, allocation of safety functions to protection layers, SIS design and engineering, and SIS verification. This technical report is divided into two parts. Part 1 provides an overview of the SIS lifecycle with references to annexes containing more detailed guidance on various subjects. Part 2 provides an end-user example of "how to" implement ISA-84.00.01. This report covers many aspects of the safety lifecycle including such topics as: "grandfathering" existing SISs (Clause 3 and Annex A); operator initiated functions (Annex B), separation of the BPCS and SIS (Annex F), field device and logic solver selection (Annex L), manual shutdown considerations (Annex P), and design/installation considerations (Annex N). TR84.00.02 expands Annex G, which only provides a brief introduction to the topic of failure calculations. TR84.00.04 does not address the MI program, which is discussed in TR84.00.03.

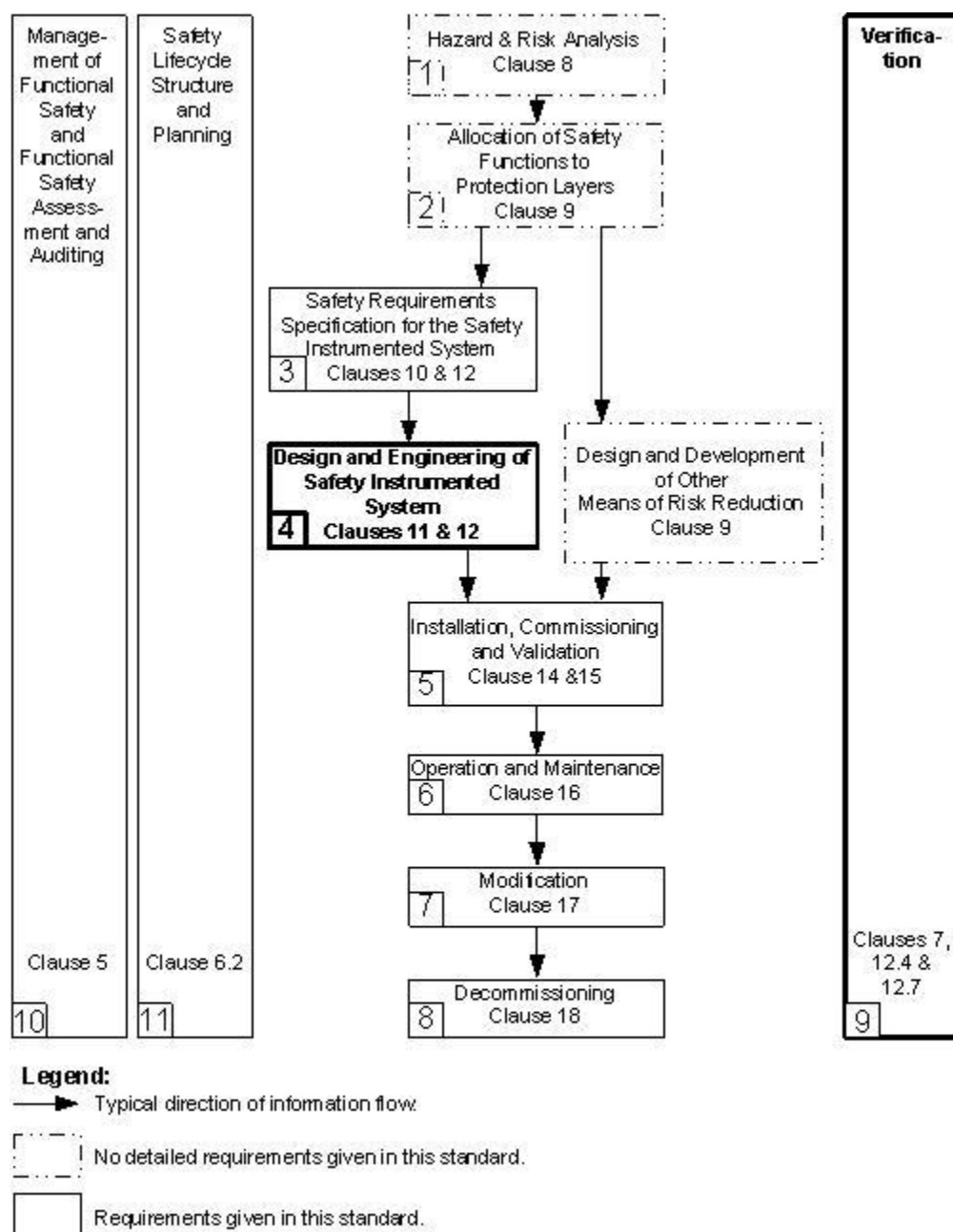


Figure 1 – SIS Safety Lifecycle Phases (modified ISA 84.00.01-1 Figure 8)

Table 1–SIS safety life-cycle overview (modified ISA 84.00.01-1 Table 2)

Safety lifecycle phase or activity		Objectives	ISA-84.00.01 Requirements Clause	ISA84 Technical Report Reference
Figure 1 box number	Title			
1	Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction.	8	None
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level.	9	ISA-TR84.00.04 Annexes B, F, and J
3	SIS safety requirements specification (SRS)	To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety.	10	No specific guidance, but many annexes assist in development of the SRS. Alternative: No specific guidance on documenting the SRS. An example is shown in ISA-TR84.00.04 Part 2. All three technical reports provide fundamental considerations for SRS development.
4	SIS design & engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity.	11 & 12.4	ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q ISA-TR84.00.02
5	SIS installation commissioning & validation	To integrate and test the SIS. To validate that the SIS meets, in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity.	12.3, 14, 15	ISA-TR84.00.03
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	ISA-TR84.00.03

Safety lifecycle phase or activity		Objectives	ISA-84.00.01 Requirements Clause	ISA84 Technical Report Reference
Figure 1 box number	Title			
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained.	17	Apply appropriate safety lifecycle phase during management of change activity
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remain appropriate.	18	Apply appropriate safety lifecycle phase during project execution
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.	7, 12.7	ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02
10	SIS functional safety assessment	To investigate and arrive at a judgment on the functional safety achieved by the SIS.	5	ISA-TR84.00.04 Clause 3 and Annexes A, C, D, E, and S

1 Introduction

ISA-84.00.01-2004 Part 1 describes a safety lifecycle model (Figure 1.1) for the implementation of safety instrumented systems (SIS) for the process industry. The standard defines four levels of safety integrity (Safety Integrity Levels, SIL) that may be used to benchmark the capability that a safety instrumented function (SIF) within the SIS to operate under all stated conditions within the time required.

ISA-TR84.00.02-2015 provides methodologies, formulas, and examples for verifying that each SIF achieves its specified SIL. The approaches outlined in this document are performance-based. Consequently, examples provided in this document do not represent prescriptive architectural configurations or mechanical integrity requirements for any given SIL.

THE METHODOLOGIES ARE DEMONSTRATED THROUGH EXAMPLES (SIS ARCHITECTURES) THAT REPRESENT POSSIBLE SYSTEM CONFIGURATIONS AND SHOULD NOT BE INTERPRETED AS RECOMMENDATIONS FOR SIS.

THE READER/USER IS THEREFORE CAUTIONED TO CLEARLY UNDERSTAND THE ASSUMPTIONS ASSOCIATED WITH THE METHODOLOGIES AND EXAMPLES IN THIS DOCUMENT BEFORE DERIVING ANY CONCLUSIONS REGARDING THE PERFORMANCE VERIFICATION OF ANY SPECIFIC SIF.

The users of ISA-TR84.00.02 include:

Developers of SIS components wishing to ensure that users can correctly implement and verify equipment performance

SIS designers who want a better understanding of how device selection, redundancy, diagnostic coverage, test interval, common cause failure, etc. affect the SIS performance

Personnel who need an introduction to the reliability techniques used to analyze and verify each SIF

Personnel involved in verification, functional safety assessment and auditing, who must ensure that the SIL is being provided in the changing facility environment.

The quantitative verification of SIL takes place before the SIS detailed design phase of the life cycle (see Figure 1.1, Safety Lifecycle Model).

SIL verification is intended to confirm the following:

- All devices of the SIS are fit for use in the operating environment and are user approved at the required SIL for their intended application.
- The architecture of the SIS meets the hardware fault tolerance for each SIF according to IEC-61511-1 Clause 11.4.
- Each SIF achieves its target failure measure (e.g., average frequency of dangerous failure or average probability of failure on demand) according to IEC 61511-1 Clause 11.9.
- The potential for common cause failure, common mode failure and systematic errors to affect multiple safety controls, alarms and interlocks (ANSI/ISA-84.91.01) that provide risk reduction for the same hazardous event has been taken into account in the hazards and risk analysis in accordance with IEC 61511-1 Clauses 8 and 9.

SIS device selection is addressed in ISA-TR84.00.04 Annex L, with ISA-TR84.00.03 providing guidance on the mechanical integrity program and data collection/analysis necessary to support user approval of safety devices. Minimum hardware fault tolerance is covered within ISA-TR84.00.04 Annex K. ISA-TR84.00.02 focuses on providing guidance on determining the target

failure measures. Consideration of common cause failure, common mode failure and systematic error within a SIS is discussed in this revision, however, guidance on determining this across multiple instrumented safeguards is being held for the next revision of ISA-TR84.00.02.

Each device of the SIS should be evaluated to:

- determine the impact of its failure on the SIF operation;
- understand its contribution to systematic, common cause, and common mode failures within and between SIFs; and
- ensure that it meets the performance necessary to achieve the required SIL of any SIF it services.

The safety requirements specification (SRS) addresses the design features (hardware, software, redundancy, etc.) and the operating plan (inspection/maintenance policy, frequency and method of testing, etc.) of the SIS. Verification demonstrates quantitatively that each SIF is capable of meeting the required SIL in the operating environment. How well this calculation reflects reality is dependent on whether the data reflects the in-service performance of the equipment. Refer to ISA-TR84.00.03 for guidance on the mechanical integrity program and how to collect data during validation, inspection, testing, and process demands. Refer to ISA-TR84.00.04 for guidance on the user approval process, which uses mechanical integrity records to verify that equipment is fit for service and provides the required performance in-service.

The objective of this technical report is to provide users with techniques for the evaluation of the average probability of failure on demand (PFD_{avg}) and mean time to failure spurious ($MTTF^{SP}$). ISA-TR84.00.02-2015 shows examples of how to model complete SIF, which includes the sensors, the logic solver and final elements.

2 Scope

ISA-TR84.00.02-2015 is informative and does not contain any mandatory clauses. ISA-TR84.00.02 is intended for use by those with a thorough understanding of ISA-84.00.01-2004 Part 1. This document assumes that a SIS is required. It does not provide guidance on the hazard and risk assessment used to identify the need for a SIS. The user is referred to ISA-84.00.01-2004 Part 3, and CCPS's *Hazard Evaluation Procedures and Layers of Protection Analysis: Simplified Risk Assessment* for guidance on assigning the SIL.

Prior to proceeding with use of ISA-TR84.00.02-2015, the hazards and risk assessment and the allocation of safety functions to protection layers should be completed and the following information provided:

At least one SIF is required

The functional requirements of the SIF

The integrity requirements of the SIF

ISA-TR84.00.02-2015 provides guidance on different issues that impact SIL verification:

Assessing random and systematic failures, classifying failure modes, and estimating the failure rates for individual devices of an SIF;

Assessing the impact of diagnostic and mechanical integrity choices on the performance of the SIF and its devices;

Assessing and estimating the potential for common cause and common mode failures; and

Verifying that the SIF achieves a specified SIL and spurious trip rate.

ISA-TR84.00.02 provides guidance on techniques for evaluating the following:

Average probability of failure on demand for low demand mode

Spurious trip rate

There are four topics that are being held until the next revision of ISA-TR84.00.02. Until then, the reader should refer to ISO 12489 for appropriate methodologies.

- Modeling of continuous and high demand mode systems
- Understanding proof test effectiveness and how this is addressed by design and mechanical integrity practices
- Understanding how to model common cause and systematic contribution to the failure of subsystems and systems and to the occurrence of the hazardous event
- Expanding the discussion of common cause and systematic error to address these issues across the entire lifecycle

3 Background

During a hazard and risk assessment, initiating causes for hazardous events are identified where deviation from intended operation results in abnormal process condition(s). Safety functions are identified that achieve or maintain a safe state of the process when defined safe operating limits are exceeded. Each safety function is allocated to an independent protection layer and allocated the risk reduction necessary to reduce the process risk below the owner/operator risk tolerance criteria. When the safety function is allocated to the SIS, the allocated risk reduction determines its SIL according to Table 4 in ISA 84.00.01-2004. Clause 11.9 requires that the target failure measure assigned to the SIF be verified quantitatively.

The SIL is related to a range of the average probability of failure on demand (PFD_{avg}) for low demand mode. SIS device performance can be determined using historical data from maintenance records. A relatively large data pool is necessary to have a statistically significant population; so many users initially estimate the PFD_{avg} using predictive analysis and comparison to previously approved equipment. As more data is collected, the data certainty improves.

This technical report provides users with a discussion of quantitative analysis techniques that can be used to verify whether a SIF meets the required SIL. Quantitative analysis breaks down complex systems to determine the effect of the failure of each device on the overall system. While this technical report will focus on the estimation of random hardware failure, the standard requires that the SIF meet the safety integrity requirements. This includes consideration of the SIF susceptibility to systematic failures.

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 is based upon random hardware failures and can normally be estimated to a reasonable level of accuracy. ISA-84.00.01-2004 addresses the hardware safety integrity by specifying target failure measures for each SIL.

Systematic integrity is difficult to quantify due to the diversity of causes of failures; systematic failures may be introduced during the specification, design, implementation, operation, and modification phases and may affect hardware as well as software. ISA-84.00.01-2004 addresses systematic safety integrity by requiring the implementation of a functional safety management system that seeks to identify and minimize the potential for systematic failures to a sufficiently low level.

The target SIL serves as the performance benchmark for the design and management practices used throughout the SIF life. The SIL establishes three criteria: 1) equipment should be user approved for the operating environment and claimed failure rate – Refer to ISA-TR84.00.04 Annex L; 2) the subsystems should have the necessary fault tolerance against dangerous failure – Refer to ISA-TR84.00.04 Annex K; and 3) the PFD_{avg} for a low demand mode SIF.

The target SIL also establishes a minimum level of management system rigor necessary to reduce the potential for systematic failures to a sufficiently low level. Systematic failures are caused, or indirectly induced, by human error or unforeseeable complex process conditions. Systematic failures are not random events and must be addressed by the management system, using quality management processes to minimize systemic failures. Systematic failures are not easily included in the verification calculation.

Random failures are easily modeled using probabilistic math, allowing the performance to be estimated. Random failures occur when stress causes a fault to develop in a component of a device. The performance calculation determines whether the planned SIF design can theoretically achieve the desired integrity and reliability, by considering factors such as:

Mean time to failure (MTTF),

Failure modes,
Distribution of failure modes,
Effect of failure mode on SIF operation,
Voting architecture,
Diagnostic coverage (DC),
Diagnostic interval (DI)
Test coverage (TC),
Inspection and preventive maintenance interval,
Testing interval (TI),
Mean time to repair (MTTR), and
Common cause failure.

Once the SIF performance is benchmarked, it is possible to identify optimal solutions that meet the process unit's operability, maintainability, and reliability requirements. Any personnel assigned responsibility for verifying the risk reduction should understand how installed equipment fails and the strategies used to address its failures. There are many books available on the subject of reliability engineering, so this technical report provides only a brief overview of the mathematics for calculation of the average frequency of failure, PFD_{avg} , and spurious trip rate.

An acceptable spurious trip rate is also normally specified for an SIF. A target spurious trip rate is typically expressed as the mean time to failure spurious (**MTTF^{SP}**). A spurious trip is also commonly referred to as a false trip, nuisance trip, or unnecessary trip - key is that the spurious action of the SIF or any of its devices was not in response to a process demand. The spurious trip rate should be considered during the evaluation of an SIF, since unnecessary shutdowns lead to economic loss and unnecessary process start-ups, which are frequently periods where the likelihood of abnormal operation and field occupation is higher than normal. Hence, in many cases, a reduction of spurious trips enhances the overall safety of the process. Further, spurious trips have a direct impact on production and product quality. Often, an increase in the target MTTF^{SP} can be justified based on the cost and impact of a spurious trip.

4 Cautions

Safe operation is achieved by designing and implementing SISs that take into account a wide variety of site-specific criteria. Verification involves a predictive calculation that is only as good as the quality of the failure rate data and the assumptions behind the system model. The calculation should be viewed as a tool for benchmarking and comparing different options. The calculations should never be perceived as an accurate measure of SIF performance or event risk. The data provided in this technical report is for illustration and should be replaced with prior use data that reflects the operating environment.

The calculations only address a portion of the safety lifecycle requirements. Some of the requirements are prescriptive or semi-quantitative in nature or are related to limitations elsewhere in the protection strategy, which might impact SIL allocation to the SIF. These requirements include items such as:

- Ensuring the initiating source frequency is within the limit noted in the standard
- Ensuring the risk reduction allocated to any individual non-SIL safety control, alarm, or interlock within a scenario does not exceed 10
- Ensuring the total risk reduction allocated to all non-SIL safety controls, alarms, or interlocks within that hazard scenario does not exceed 100
- Ensuring that any sensors or final elements used in the safeguard design are “fit for use” (e.g., can read the process accurately at the hazardous condition, are fast enough, strong enough and sufficiently effective to perform the protection or mitigation function against that hazard successfully)
- Ensuring that any sensors or final elements used in designs for SIL1 to 3 are user approved for safety (see ISA-TR84.00.04 Annex L)
- Ensuring that the protection strategy does not exceed the capability of any logic solver(s) involved in the instrumented safeguard function(s)
- Ensuring that any sensor, logic solver, or final element subsystem involved in executing a SIF meets the minimum hardware fault tolerance requirement per the related SIL

Since the quantitative SIL verification (i.e., PFD or PFH) analysis is separate from and in addition to the prescriptive requirements above, it is strongly recommended that any SIS design or verification process begin with ensuring the prescriptive requirements are satisfied before continuing to the PFD/PFH analysis. The cautions and guidance related to the other requirements are not within the scope of this document.

SIS are designed, constructed, installed and maintained to minimize the risk of significant consequence events, especially those involving highly hazardous chemicals. SIS equipment must not be run to failure, but maintained in the “as good as new” condition (see ISA-TR84.00.03). This requires an on-going mechanical integrity program, which assures the equipment’s long-term integrity.

The functional safety management system must seek to identify and correct systematic failures, which reduce the SIF’s actual performance. User experience is that most failures of a SIF to operate under demand are related to systematic failure not random hardware failure. A significant assumption in the calculation is that inspection, preventive maintenance, and proof testing are performed at a rate sufficient to sustain the assumed failure rate. Maintenance activities are discussed further in ISA-TR84.00.03. The quality of these activities affects similar devices and thus serves as a large source of common cause failures across presumably independent instrumentation and control systems. The calculation does not implicitly or explicitly account for

how changes in the design, operating, and maintenance practices affect the achievable failure rate of any device or device(s).

The calculation may indicate that a change in testing from once per year to once in 10 years is acceptable. However, the change in testing will result in less opportunity to detect incipient and degraded failures, allowing more complete failures to occur. Less frequent movement of mechanical components and linkages may result in a higher potential for the device to freeze in position or lock-up. Less frequent review of the current installation allows undocumented changes to accumulate, including field installation, configuration, and equipment changes.

As the test interval is extended, it becomes more likely that the test will find a failed device, rather than a degraded one. Breakdown maintenance is not acceptable for the SIS. Consequently, when dangerous failures are found, an investigation should determine the root cause and should identify means to reduce recurrence, as necessary, including an increase in the inspection, preventive maintenance, and/or proof test frequency and rigor.

Process industry experience demonstrates that sensors and final elements are major contributors to loss of SIS integrity and that the operating environment plays a major role in sensor and final element failure. When evaluating the performance of sensors and final elements, issues such as component technology, environmental specifications, installation, and maintenance should be considered.

PE logic solvers pose significant risk of common cause failure between multiple SIFs. The larger the number of I/O implemented in a single PE logic solver, the more SIF are affected by its failure and the larger the number of pieces of equipment put at risk when it fails. In contrast, a single sensor, relay, or final element rarely affects more than a single piece of equipment.

5 Nature of failures

Potential failures within an SIS can be predicted probabilistically through analysis of the SIS equipment in the system. Competent execution of the probability calculation requires a fundamental understanding of failure analysis, associated terms, and mathematics. The analysis of SIS equipment begins with identifying its failure modes, which are the symptoms, conditions, or effects by which its failure is observed. Failure modes that either cause a hazard or prevent equipment from performing their safety function are the primary focus of the SIL verification required by ISA-84.00.01. The following presents a discussion of various terms used to describe failure and to classify its impact.

5.1 Device failure

Device failure is often divided into three categories: complete failure, degraded condition, and incipient condition. A complete failure is the termination of the equipment's ability to operate as required in the SRS, whereas a degraded condition causes a partial loss of function. Incipient includes conditions that will likely result in a loss of one or more functions if not corrected in a reasonable time frame. These categories can be further classified as safe or dangerous depending on the effect that they have relative to the ability of the equipment to execute its safety function.

A failure results due to a variety of circumstances that manifests itself during design, manufacture, installation, commissioning, operation, or maintenance. Failures can be instantaneous or gradual, partial or complete, and intermittent or transient. The wide variety of failures invariably creates differing interpretations among engineers as to what happened, why it happened, and how it should be categorized. This clause provides a consistent set of definitions for failure terminology.

5.1.1 Complete failures

A complete failure results in the termination of the ability of a device to completely perform its specified safety function. From a mechanical integrity viewpoint, the SIS device has suffered a complete failure when it does not satisfy the pass/fail criteria of the proof test. Examples of complete failures include:

Block valve does not completely open or close on demand

Transmitter output fails high or low removing it from consideration in safety or control logic or the signal does not change with the process variable

Logic solver I/O board does not accept input signals or generate output signals

5.1.2 Degraded conditions

Degraded conditions are those that decrease a device's reliability and/or prevent the device from fully meeting its design specifications. The important distinction here is that the device performance is still sufficient to meet the SRS. If a degraded condition is allowed to remain, it may become a complete failure. Degraded conditions can be detected during inspection, proof testing, and preventive maintenance or by automated diagnostics. Diagnostics can significantly improve the ability to detect degraded conditions and to allow maintenance to be performed prior to complete failure. Examples of degraded conditions excerpted from the CCPS PERD instrument loop taxonomy include:

Control Output High

Control Output Low

Control Output Slow to Respond

Control Output Too Fast

Control Output Erratic

Auto Controller in Manual Mode
 Process Variable Indication High
 Process Variable Indication Low
 Process Variable Indication Erratic
 Control Output Indication High
 Control Output Indication Low
 Control Output Indication Erratic
 Alarm Function Delayed
 Interlock Function Early
 Interlock Function Delayed
 Interlock Voting Channel Fail to Function
 Interlock Voting Channel Spuriously Functions

5.1.3 Incipient conditions

Incipient conditions do not prevent a device from performing its safety function. If corrective action is not taken, the incipient condition is likely to progress into a degraded condition or complete failure. Incipient conditions can often be found during inspections. Examples of incipient conditions are:

loose electrical or mechanical connections
 corroded termination
 damaged electrical insulation
 partially plugged solenoid valve vent (shutdown valve doesn't exceed allowable response time)
 missing bolt from sensor flange (no leakage yet)
 buildup of water/oil in a junction box
 buildup of fluid in air/gas lines
 partially plugged impulse line (does not exceed SIF response time)
 partially plugged or corroded dip tube (does not exceed required calibration accuracy)
 outdoor panel cover gasket cut or missing
 missing filter or screen on an air line

Examples of remote actuated valve incipient conditions per CCPS PERD taxonomy:

Body Cracked
 Body Eroded
 Body Corroded
 Body Material Wrong
 Guide Fouled
 Guide Galled
 Guide Corroded
 Guide Worn
 Stem Fouled
 Stem Galled

Stem Corroded
Stem Bent
Stem Worn
Seat Fouled
Seat Cut
Seat Eroded
Seat Corroded
Seat Excessive Wear
Seat (soft) Embedded Debris
Seat (soft) Overheat Evidence
Seat Loading Mechanism Dysfunctional
Spring Cracked
Spring Corroded
Spring Fatigued
Spring Rubbing
Improperly Installed
Excessive Vibration

5.1.4 Failure modes

The user needs adequate information to design a safety instrumented system so that its probability of failing to function meets the requirement. This probability is a function of proof test intervals that account for dangerous undetected failures and repair times for dangerous detected failures. The user also needs data to determine the frequency of spurious trips related to safe equipment failures to predict plant reliability. This requires understanding the failure modes of the equipment and how these failure modes affect the ability of the equipment to function.

All devices eventually fail when a fault occurs somewhere within the device's components and propagates into a degraded condition or complete failure, resulting in the device's inability to operate as specified. The observed loss of function is the device's failure mode, e.g., the signal does not change with the process variable or the PLC output does not de-energize. User approval (see ISA-TR84.00.04 Annex L) of a manufacturer's device for safety applications relies heavily on gaining sufficient understanding of the device's failures in the operating environment.

Failure mode and effects analysis (FMEA) is a qualitative analysis method used to identify failure modes and assess their impact on the device operation, so the design basis can take these modes into account. The effects may include:

Complete failure (e.g., failure-to-operate),
Spurious operation (e.g., premature function),
Degraded condition (e.g., out-of-tolerance), and
Incipient condition (e.g., damaged electrical insulation).

Degraded conditions and complete failures cause the device to not operate as specified. These failures can occur suddenly or gradually over time. An incipient condition does not currently affect the device operation. However, if corrective action is not taken, the incipient condition could lead to degraded condition or complete failure. For example, the screen is missing from the vent port of a solenoid-operated valve. There is no obstruction currently in the vent port, but if the screen

were not replaced, debris could accumulate in the port, resulting in a degraded condition or complete failure.

Pass-fail criteria are established for each device to determine when a failure is classified as a complete failure, degraded condition, or incipient condition. If a device fails to operate as specified in the design basis for safety, the failure is considered dangerous. The risk reduction capability of a safety function is related to its dangerous failure rate. If the device has spuriously operated in a manner that does not create a hazard or does not result in the loss of its ability to perform its protective function, the failure is considered safe.

Annex F includes examples of failure modes and effects for the following:

Remote Actuated Valve

3-Way Solenoid Valve

Transmitter

Electromechanical relay

PES

5.2 Failure causes and mechanisms

The previous discussion of failure provides an initial foundation for the understanding of failure causes and failure mechanisms. These terms are used to facilitate a more fundamental and consistent interpretation of how (causes) and why (mechanisms) something failed. This understanding has great practical application when defining the “as found” and “as left” condition in inspection, maintenance, and proof test reports.

Failures can be traced to root causes, which may be systematic or random. Systematic failures result from root causes associated with a functional safety management system failure. They are often deterministic rather than time dependent. For a failure to be systematic, it should be possible to replicate the failure by producing the same set of conditions. Reducing systematic failure occurrence requires active identification of these failures and adaptation of site work processes. Random failures result from various degradation mechanisms and can occur at any time according to a probability distribution, which can be estimated through analysis of the system hardware components and design. These degradation mechanisms are impacted by the operating environment, which places physical, chemical, or electrical stresses on the equipment. Random failure does not follow any pattern, but instead occurs randomly during the device’s life.

From a modeling perspective, a significant difference between random and systematic failures is that the equipment failure rate arising from random hardware failures can be predicted with reasonable accuracy, but many systematic failures cannot be easily predicted and must be estimated based on historical experience.

Even though time dependency appears to be the easiest way to distinguish between systematic and random failures, this distinction is not always true. Many random failures are time dependent, but not all are. Most systematic failures are not a function of usage, cycles or time, but some are. Systematic failure can affect the random failure rate of equipment, and random failure can trigger human intervention that introduces systematic failures. The following examples illustrate the complex interaction between random and systematic failure and provide guidance on the failure modeling.

Equipment failures that occur during expected useful life. These failures are modeled probabilistically as a function of time. Consider these four cases:

Failure is related to the device and the estimated failure rate can be predicted by an analysis of the components within the device

Failure is accelerated by exposure to the operating environment and the estimated failure rate must consider prior use history

Failure occurs because the equipment is incorrectly specified for the operating environment (e.g., the wrong material installed in a corrosive environment)

Failure occurs due to quality assurance error in the supply chain (e.g., change in gasket material of construction results in accelerated failure)

Equipment failures that occur outside the expected useful life. Consider two cases:

The failure is random, but the failure rate is increasing as a function of time and not constant as assumed in typical SIL verification calculations. Consideration should be given to other reliability modeling techniques, such as Weibull analysis, to ensure that these failures are properly accounted for it in the calculations.

The failure occurs once the equipment experiences the loss of a known capacity or cyclic capability. For instance, a battery must provide a certain charge. An electrolytic analysis cell has a fixed amount of electrolyte and a relatively known consumption rate. The cell failure cannot be described analytically as random. This failure should be modeled deterministically using a short duration normal or log-normal distribution around a mean value.

Human error can appear to be systematic or random. These errors are generally estimated by the probability that the SIF is not commissioned or returned to service in the “as good as new” or “fully operational” condition. Consider these two cases:

An incorrect procedure will result in repeated systematic failures.

A well-trained technician using a correct procedure will still make mistakes that will randomly occur.

Software failures can also appear to be random or systematic. Software errors are generally considered systematic failures, because once the program bug is introduced, it remains until the right set of conditions occurs and the error occurs. The error itself appears at some random point in time but the root cause is considered systematic since the failure is present from the time the bug is introduced. ISA-84.00.01-1 Clause 12 emphasizes the importance of software specifications, modularity, verification, validation, and management of change to minimize such errors (see ISA-TR84.00.04 Part 1 Annex O). These failures are generally estimated deterministically as a probability that the software has a bug. Consider these two cases:

Software bugs are considered systematic failures. However, the failure may appear randomly when the right set of conditions occur.

Software bugs may be randomly introduced due to poor management of change, but the bug is considered a systematic failure.

Failures are managed within the ISA-84.00.01 work process using different strategies depending on whether they are random or systematic. Consequently, the following clauses briefly discuss random, systematic, and common cause failures, so the strategies for their management can be better understood.

5.2.1 Random failure

SIS equipment is often manufactured with electrical, electronic, programmable electronic and mechanical components. Each device wears out or breaks down after a different length of time, depending on how well it was originally manufactured, how much it has been used, the variation in the operating conditions, etc. Since various components are lumped together to make a device, the failures of the device appear to be random even though the failure distributions of the individual components may not be random. The user approval process should ensure that a device's random failures and failure modes are well understood prior to approval.

Random hardware failures occur at unpredictable times and result from one or more of the possible failure mechanisms that are applicable to the equipment. Random failures are the result of hardware degradation mechanisms, which can be accelerated by stress factors due to the operating environment. Many types of events cause stress, such as:

Normal or abnormal process conditions,

Presence of an adverse micro environment (e.g., corrosion produced by chemical impurities or metallurgy),

Presence of solids or other materials which randomly deposit in SIF devices,

Corrosion, erosion, fatigue due to mechanical or thermal cycling, and other environmental stresses,

Exposure to electrical surges,

Exposure to electrostatic discharge,

Operating for long periods at the extreme of the device's environmental specification,

Excessive device wear and tear,

Electronic devices operating in environments at temperature extremes or environments with significant temperature cycling,

Other external influences (e.g., weather, process upsets, electromagnetic interference, etc.).

These failure mechanisms may be inherent in the design of the equipment such as thermal or mechanical cyclic fatigue, or may be due to external influences such as mechanical shock or corrosion due to ambient and/or process conditions. Random failure generally manifests itself as a physical failure where a stressor (or combination of stressors) has exceeded the capability of the installed equipment by impacting one or more of its parts. There are many degradation mechanisms inherent in the equipment. These occur at different rates in different components in the equipment. In some cases the specific degradation mechanism is predictable, while for others it is not. For example, general corrosion is thought to be uniform, while the potential for stress corrosion cracking is much less so. When considering the complexity of an equipment system with varying part failure rates that are not completely predictable, it is easy to understand that failures occur at unpredictable (i.e., random) times over their useful lives.

Random failures can be identified by internal device diagnostics, external diagnostics, inspection, and proof tests. The equipment inspection and proof test interval is generally chosen based on maintenance history, manufacturer's recommendations, good engineering practice, insurance requirements, regulatory requirements, and what is necessary to achieve the required performance.

One very effective barrier against random device failures is to implement redundancy. Fault tolerance is provided using multiple devices in voting configurations that are appropriate for the SIL. If one device breaks down, another device is available to provide the safety action. Thus, redundant, fault tolerant subsystems reduce the probability that a single failure will cause the SIF to fail to operate correctly. Redundant subsystems also provide the opportunity for external diagnostics including the ability for comparison diagnostics, where a diagnostic algorithm is executed at a specified interval to detect device failures.

5.2.2 Systematic failures

Systematic failures are a major contributor to SIF failure and limit the performance that can be achieved by the SIF. Systematic failures are best addressed with a quality-focused management system, which emphasizes continuous improvement through performance monitoring. A rigorous system is necessary to decrease systematic failures and enhance safe and reliable operation. Each verification, assessment, audit, and validation is aimed at reducing the probability of systematic failure to a sufficiently low level. As errors or failures are detected, their occurrence should be investigated, so that lessons can be learned and communicated to affected personnel.

Unfortunately, since systematic failures are often related to human error, it is difficult to predict when and how frequently they can occur. Thus, the failures are deterministic only to an extent, as humans by their very nature are not fully predictable. Whereas improved training, practice and procedures can reduce the impact of human error, it cannot be eliminated in a fully deterministic manner. Systematic failure potential is highly related to the plant safety culture and the rigor of the management system processes used to minimize error occurrence and to detect and correct those errors that do occur. The most effective defense against systematic failure is full integration of the ISA-84.00.01-2004 lifecycle and functional safety management concepts into the project management process.

Systematic failure is related in a deterministic way to a root cause, which can only be minimized or eliminated by changes in the design basis, installation practices, software systems, or operating basis. Systematic failures can be due to a single failure event or to a combination of errors, such as poor design and operation/maintenance practices.

Systematic failures, which have resulted in process safety incidents, are:

- Risk assessment errors,
- Design errors,
- Specification errors,
- Unexpected operating environment impact,
- Installation and commissioning errors,
- Operator errors,
- Maintenance errors, and
- Change management errors.

Systematic failures include many types of errors, such as:

- Manufacturing defects, e.g., software and hardware errors due to its manufacture,
- Specification mistakes, e.g., incorrect design basis or incorrect software specification,
- Implementation errors, e.g., improper installation, incorrect programming, interface problems, or not following the safety manual, and
- Operation and maintenance, e.g., poor inspection, incomplete testing or improper bypassing.

As the SIF equipment and design becomes more complex, the potential for systematic failures increases. Each device has many known opportunities for systematic failure. With any new technology, there is the potential for many unknown (or as yet unidentified) failures. When issues associated with interconnectivity, communication, and support (utility) systems are added to the analysis, there are generally a large number of potential systematic failures. The following are examples where systematic failures can become more significant:

- Unusual, novel or complex design
- Complex diagnostic or maintenance features
- Poor maintenance competency
- Poor operating discipline
- Significant change in management practices, such as downsizing, impacting operating and maintenance practices

Redundancy may be ineffective against systematic failures, especially if the errors are related to the design, operation, or maintenance. Under the same conditions, all redundant devices can fail due to a common systematic failure. A partially effective barrier against systematic failures is to use device diversity, i.e., redundancy is provided using a different device, system, technology,

programmer, etc. If one device fails, the other continues to work if the cause of failure does not result in the failure of both devices. Use caution to avoid deterioration of SIF performance from the use of diverse devices with poor performance characteristics.

Systematic failures related to manufacturing defects can be reduced through the use of diverse redundancy. Diversity typically involves the use of different technologies or different manufacturers. While manufacturer errors can be addressed by diversity, this increases the SIF complexity. Incorrect specification, implementation, operation, and maintenance constitute root causes that are not solved by this type of diversity and can actually increase if unnecessary complexity is introduced into the SIS design. The level of and type of diversity utilized should be balanced against the level of complexity. The simplest design often yields the lowest likelihood of human error during design, operation, and maintenance.

The perceived improvements gained by diversity are based on the assumption that different devices exhibit different failures and failure modes. In other words, it is less probable for all of them to fail simultaneously, if they are different. However, diversity only reduces the potential for common mode failures. Many common cause failures may not be addressed by diversity.

The following is an actual case description of the impact of systematic failures, i.e., human error, operating discipline, etc., on the operation of an offshore production platform.

Offshore platforms have many different safety related systems. Several years after one system was started up, the low pressure flare system needed modification. (There were actually two flare systems; low and high pressure.) The modification required removing a piece of pipe to the flare in order to install a heater. The project was reviewed very carefully, considering other incidents the company had gone through. The pipe was removed while the plant was running, so the flare system was now operating at atmospheric pressure. The flare system was purged and deemed safe.

Personnel were instructed that if anything went wrong they were to hit a manual call point, which was an input into the fire and gas system. This was considered a "Class 1 ESD" – shutdown and isolate. What they were not told was that the input also started a two-hour blowdown timer. Someone heard something hissing in the flare piping. They thought it was a release so they activated the manual call point. As a result, all the alarms went off and everyone stood down.

People eventually realized that all that had really happened was that some condensate ice in the flare line had bubbled off and there really was nothing to worry about. This happened just before lunch, so everyone decided now would be a good time for a lunch break. No one knew that the two-hour blowdown timer was still running. Once the timer expired the entire plant started blowing down.

Now there really was gas flowing down the line to the base of the flare stack! The flare tip was a common ignition source for both the low and high-pressure flares. While the high-pressure flare was operating successfully, it was drawing oxygen and gas up through the open piping at the base of the low-pressure flare. The mixture exploded at the flare tip and flames shot out the pipe opening at the bottom of the stack. This cycle – an explosion and flames – repeated approximately every 15 seconds.

The open blowdown valves were near the base of the flare stack. The blowdown valves had manual resets on them, but personnel could not get anywhere near the valves to manually reset (close) them because of the recurring explosion and flames. The only thing left to do was abandon the platform. Approximately 200 people were evacuated using dozens of helicopters in the area. (Launching lifeboats was not desirable.) A crew of 20 remained on board overnight and the situation worked itself out. The event was covered by the local TV news. Fortunately, very little physical damage was actually done.

So how could this have happened? The original design (from the 1980s) called for over two dozen halon zones and a halon based flare snuffing system that would have been able to snuff out the flare and eliminate the source of ignition. However, by the time the systems were installed in the early 1990s there was a move within industry to reduce the amount of halon being used. The flare snuffing system was not deemed appropriate for halon so the bottles were never installed, *although the connections, piping and release button were*. An operator pressed the button for the halon release during the emergency, but there never was any halon to release. People later reported that the halon system did not work. It obviously *could not* work. Unfortunately not everyone was aware of the design change, nor was the design change thoroughly documented.

The platform was abandoned for 24 hours and down for seven weeks. The OIM (Offshore Installation Manager) and 12 other people lost their jobs that day.

5.2.3 Common cause failures

Common cause failure (CCF) is a term used to describe random and systematic events that cause multiple devices, systems, or layers to fail simultaneously. From a maintenance perspective, multiple failures may be detected during the same proof test, while the individual failures occurred randomly since the last proof test. The likelihood of multiple failures becomes more likely as the proof test interval gets longer. Thorough root cause analysis is necessary to determine whether the failures occurred randomly or were due to the same common cause problem.

Another term is “common mode” failure, which describes the simultaneous failure of two devices in the same mode. Common mode failure is related to the use of identical devices in the redundant subsystem. For example, two redundant differential pressure sensors can be simultaneously disabled due to loss of signal (common mode failure) originated from diaphragm damage (failure cause) caused by water hammer. Common mode failure is a subset of common cause failure.

Common cause failures are important considerations in predicting SIF performance. When common cause failures are not evaluated, there is an implicit assumption that there is perfect independence between the related devices regarding design, installation, operation, maintenance, and management of change. In reality, this is rarely an appropriate assumption to make. Good practice can result in a low common cause failure rate with little impact of the estimate of the PFD_{avg} . Poor practice can result in a high common cause failure, negatively impacting the achievable PFD_{avg} .

All common cause failures have the potential to reduce the SIF performance; however, they are addressed in different ways depending on whether the failure can be described deterministically (e.g., systematic) or probabilistically (i.e., random). Throughout the ISA-84.00.01 lifecycle, it is recommended that devices, systems, or protection layers be assessed for independence and the potential for common cause failure. Independence and common cause are often interrelated. A lack of independence means that there is a potential for a common cause failure. Likewise, an identified common cause indicates a lack of independence and therefore some dependency.

The approach taken to manage CCF is specific to the nature of the failure. Two types of CCF are addressed: 1) single points of failure where the failure of one device causes multiple SIFs to fail; and 2) single causes that lead to multiple failures in a redundant subsystem. Single points of failure can occur due to systematic or random events. Systematic failures are often related to human errors that violate design and MI program assumptions. For example, the devices were selected based on clean service conditions, but the process fluids actually contain hydrogen sulfide. Random failures can occur at any time during the device’s useful life and can be effectively managed with a rigorous MI program.

Redundant subsystems can fail due to systematic failures in the device manufacture, specification, design, installation, and maintenance. These errors typically happen due to lack of knowledge, information, and training and are generally unknown to personnel. Test procedures may not identify these errors, since they are not expected. Systematic failures are difficult to test even when easily

identified. For example, it is possible that the valve actuator is incorrectly specified, but how do you test to determine that the valve actuator will not close under emergency process conditions?

Diversity is often suggested as a means to reduce common cause failure. The use of different technologies (i.e., diversity) does reduce the potential for common mode failure. However, common cause can impact identical and diverse devices. For example, the process application or external environmental condition can affect different technologies simultaneously when the conditions trigger each device's failure mechanisms. These devices may eventually fail due to different reasons, but the abnormal process condition is root cause that initiated the failure mechanisms leading to device failures.

Specification errors must be caught during the design and engineering phases using independent verification. Checklists can be used to identify CCF. The list of questions guides the engineer through the design aspects examining opportunities for CCF. Installation, commissioning, and maintenance errors are reduced by independent checks, verifications, and audits.

Common cause failures should be considered in the PFD_{avg} calculation. The operating environment, the installation, and the interconnection to other systems affect the device operation. This system-induced random failure can be analyzed by explicit or implicit model depending on the specific common cause. (1) If the common cause(s) can be identified as a separate basic event/element in the reliability model, then explicit model should be used. For example, if fault tree analysis is being used, the CCF is modeled as a basic event with its own failure rate. (2) If redundant items share a number of root causes and coupling factors, or the explicit modeling would be unmanageable, the (residual) CCF is modeled as a "combined" basic event/element, i.e., an implicit model such as the beta factor model.

5.2.4 Data analysis

By observing the operation of a device over time, data can be collected about how often it breaks down. This information can be used to estimate how long a device is likely to last before it stops working properly. However, in the case of Programmable Electronic (PE) devices and logic solvers, the technology is evolving so rapidly that the reliability data collected on any device is often limited unless databases are pooled.

Collected data typically includes some systematic failures, which contribute to the observed failure rate. Since the intent of the quantitative analysis is to predict SIF performance, the systematic failures should be tracked and their potential impact considered when estimating the random failure rate. As more information is collected, trends can be identified and used to minimize random and systematic failures in new or modified designs. For example, it may take multiple failure reports before it is recognized that poor instrument air quality causes higher than expected equipment failure. But once the trend is recognized, action should be taken to improve the instrument air quality.

5.3 Failure classification

The consequence of the failures can be classified as safe or dangerous based on the impact or effect the failure has on the device's operation. The following definitions are derived from IEC 61511.

A safe failure is a failure which favors a given safety action: A failure is "safe" only with regard to a given safety function. When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip. When fault tolerance is implemented, safe failure can lead to either:

operation where the safety action is available but with a higher probability of success on demand (demand mode of operation) or a lower likelihood to cause a hazardous event (continuous mode of operation);

a spurious operation where the safety action is initiated.

A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function. Spurious trips may also have detrimental effects on the production availability of the process.

A dangerous failure is a failure which impedes or disables a given safety action: A failure is "dangerous" only with regard to a given SIF. When no fault tolerance is implemented, all dangerous failures lead to a disabled SIF. When fault tolerance is implemented, a dangerous failure can lead to either:

a degraded SIF where the safety action is available but there is either a higher PFD (demand mode of operation) or a higher likelihood of initiating a hazardous event (continuous mode of operation), or

a disabled SIF where the safety action is completely disabled (demand mode of operation) or the hazardous event has been induced (continuous mode of operation).

Detected failures are in relation to hardware and software failures, or faults, which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods. Undetected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. Revealed is used for failures or faults that become evident due to being overt or as a result of being detected.

In IEC 61511, the term dangerous detected failures/faults is related to dangerous failures detected by diagnostic tests. Overt is used for failures or faults, which announce themselves when they occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred. When the detection is very fast (e.g., by diagnostic tests) then the detected failures or faults can be considered to be overt failures or faults. When the detection is not very fast (e.g., by proof tests) the detected failures or faults cannot be considered to be overt failures or faults when addressing safety integrity levels. A dangerous revealed failure can only be treated as a safe failure if effective compensating measures, automatic or manual, are taken in a short enough time to ensure the safety integrity requirements are met for the safety function.

In contrast, undetected, unrevealed, and covert failures are not detected or not revealed or not overt. In IEC 61511, the term "dangerous undetected failures/faults" is related to dangerous failures/faults not detected by diagnostic tests.

Undetected failures are those failures that are not detected by the automated diagnostics, operator intervention (for example, physical inspection and manual tests), or through normal operation.

The IEC 61511 definitions are illustrated in Figure 5.1. The failure rate can be determined by calculating the device's mean time to failure (MTTF), which is the average time before a device's first failure. For a repairable device, the failure rate can be determined (e.g., mean time between work orders) based on the time between one failure and the next. The mean time between failure (MTBF) includes the MTTF and the mean time to repair (MTTR).

$$\text{MTBF} = \text{MTTF} + \text{MTTR} \quad 5.1$$

When the MTTR is small compared to the MTTF, the MTTF represents the average time that the device is in the operational condition.

$$\text{When } \text{MTTR} \ll \text{MTTF}, \text{ MTBF} = \text{MTTF} \quad 5.2$$

Work orders and proof test records can be used to estimate the complete failure rate, $\lambda_{\text{Complete}}$:

$$\lambda_{\text{Complete}} = 1 / \text{Mean Time to Failure} \quad 5.3$$

Refinement of the work order and proof test records system can allow failures to be further classified as failure to function or spurious operation. When the presence of the failure results in the device losing its ability to take its specified safe state (or a failure to operate), the failure is classified as dangerous. The dangerous failure rate, λ_D , is:

$$\lambda_D = 1/\text{Mean Time To Failure Dangerous (MTTF}^D) \quad 5.4$$

Diagnostics are used to detect both safe and dangerous failures. The diagnostic coverage (DC) is the fraction of failure detected by diagnostics. DC for safe failures may be different from DC for dangerous failures.

The fraction of dangerous failures detected by the diagnostics (DC) can be used to determine the dangerous detected failure rate, λ_{DD} :

$$\lambda_{DD} = DC \times \lambda_D \quad 5.5$$

The fraction of dangerous failures that cannot be detected by diagnostics (1-DC) can be used to determine the dangerous undetected failure rate, λ_{DU} :

$$\lambda_{DU} = (1-DC) \times \lambda_D \quad 5.6$$

When the presence of the failure results in the device taking its defined safe state, the failures are classified as safe. The safe failure rate, λ_S is:

$$\lambda_S = 1/\text{Mean Time To Failure Safe (MTTF}^S) \quad 5.7$$

The fraction of safe failures detected by the diagnostics (DC) can be used to determine the safe detected failure rate, λ_{SD} :

$$\lambda_{SD} = DC \times \lambda_S \quad 5.8$$

The fraction of safe failures that cannot be detected by diagnostics (1-DC) can be used to determine the safe undetected failure rate, λ_{SU} :

$$\lambda_{SU} = (1-DC) \times \lambda_S \quad 5.9$$

When detection of the failure, whether safe or dangerous, results in the device taking its defined safe state due to device configuration or fault handling in the application program logic, the spurious failure rate can be calculated from the λ_S and λ_{DD} :

$$\lambda_{SP} = \lambda_S + \lambda_{DD} \quad 5.10$$

In Equation 5.10, λ_{DD} is included to account for dangerous detected failures that become safe by design, because the fault response treats the failure as a vote to trip. For example, consider a high-pressure trip that uses 2oo3 voting transmitters. If inherently safer practices are followed, each transmitter is configured to fail high on detected fault (including high and low out-of-range reading), so that the application program logic treats the failure as a vote to trip. In this case, only one of the two (1oo2) remaining healthy transmitters needs to vote to trip to trigger the final element response. Until the faulted device is repaired, the SIF is still functional and its safety integrity is not negatively impacted. In this example, the subsystem after the first detected fault has a lower failure potential due to the fault detection and response strategy.

In contrast, when the detected failure is configured away from the trip state (within the device or application program logic), the configuration results in the loss of the device's ability to take its safe state action. So, the detected failure should be classified as dangerous until the device is repaired and returned to service:

$$\lambda_D = \lambda_{SD} + \lambda_{DD} + \lambda_{DU}$$

5.11

In Equation 5.11, λ_{SD} is included to account for safe detected failures that become dangerous by design. For example, consider the 2oo3 voting transmitters. If a transmitter is configured to fail low on detected fault and the application program does not treat an out of range signal as a vote to trip, the safe failure is converted into a dangerous one due to the fault response. With one transmitter incapable of voting, both of the remaining transmitters (2oo2) must issue trip signals. Until the failed transmitter is returned to service, the SIF is still functional as above, but it is operating in a degraded state since the resulting 2oo2 pressure transmitter subsystem has less safety integrity. In this example, compensating measures are likely to be required due to the loss of risk reduction provided by the transmitter subsystem.

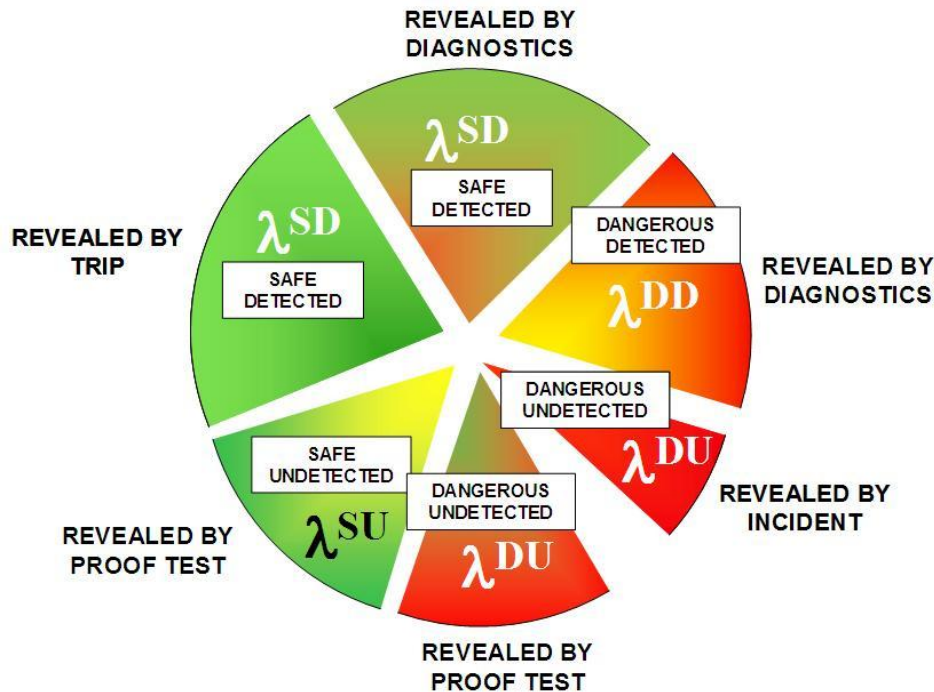


Figure 5.1 – Illustration of general failure classification

5.4 Failure rates

The failure behavior of many devices used in SIF applications can be represented by the “bathtub” curve as shown in Figure 5.2. The bathtub curve for an individual device is developed by counting the failures that occur in a population of identical (or sufficiently similar) devices over a specified time period. When the devices are operating within their useful life, the collected data set is used to estimate the failure rate.

The bathtub curve is in reality composed by three overlapping curves, one for each of three regions. The initial failure rate of the hypothetical device is driven by burn-in, infant mortality, or early failure. The frequency of these failures declines rapidly over time. The middle flat section of the curve represents the “useful life” of the device and is typically characterized by a constant failure rate. The SIL calculation is based on this middle section. The last part represents the “wear out” or “end-of-life” phase, which is characterized by an increasing failure rate. Regardless of their frequency of occurrence, once the failure has occurred, it remains until detected by Mechanical Integrity (MI) activities or a failure to operate on demand.

Manufacturing, assembly, test, installation, and commissioning errors cause some early failures. Manufacturing flaws in the components that comprise the device can cause early failure during the burn-in. Manufacturers affect the shape of this curve when they perform burn-in and rigorous function testing prior to release from production.

Poor device handling and installation often cause early failures. Devices can be damaged during shipment, unpacking, storage, transport to work site, and installation. Rough device handling, improper pre-installation storage, poor installation practices, and sloppy construction practices can also cause damage.

Materials used for installation activities, such as paint, pipe dope, insulation, and small pieces of a welding rod, have been shown to cause devices to fail by propagating into places where they are not supposed to be. Water and moisture intrusion during installation and commissioning can seriously damage SIS equipment. Missing conduit covers and poor grounding do not result in early failure, but are incipient conditions that could cause premature failure. Incipient conditions can propagate to complete failure at any time during the useful life of the device. This is indicated by the extension of the burn-in curve to the useful life and the wear out region. Rigorous inspection, commissioning and validation activities are necessary to identify and correct these conditions.

The transition between the burn-in and useful life occurs when the failure rate becomes constant. Failures during the useful life are caused mainly by random events that increase the stress on the device beyond its physical limits. When the wear-out failures become dominant, the overall failure rate increases. This indicates the end of the device's useful life.

The wear out period is characterized by an increased slope that is related to the device technology. Programmable devices tend to have a very sharp increase in the failure rate due to the large number of aging components. Fairly abrupt transitions are seen from equipment using electrochemical cells. Some devices tend to have a more gradual increase in failure rate as they age, such as electromechanical devices. The slope of the failure rate curve is heavily affected by how well their mechanical components are inspected and maintained.

A lack of inspection and preventive maintenance has been cited as a primary cause of early failure. A properly designed MI program involving inspection, testing and preventive maintenance can extend the useful life of equipment. When failures are detected via inspection, test, or through diagnostics, the equipment can be repaired and returned to what is considered "as good as new" condition, which simply means the equipment continues to be on the flat portion of the curve. The mathematics of taking credit for a proof test implicitly assumes the equipment is returned to this "as good as new" condition. In the case of the electrochemical cell, the useful life of the equipment systems in which it is employed can be extended if a preventive maintenance program is in place to replace the cell prior to the onset of wear out.

As early failures, not all wear-out failures occur after the end of the useful life; premature failure can occur at any time during the device's installed life. As time passes, the rate of failure increases. Devices should also be replaced when maintenance records demonstrate that it cannot support the required SIL. When early failure and wear-out is addressed within the device installation, commissioning and MI plans, the device failure rate is assumed to be constant. The useful life section of Figure 5.2 illustrates the predictable failure rate that is the goal of any effective MI program.

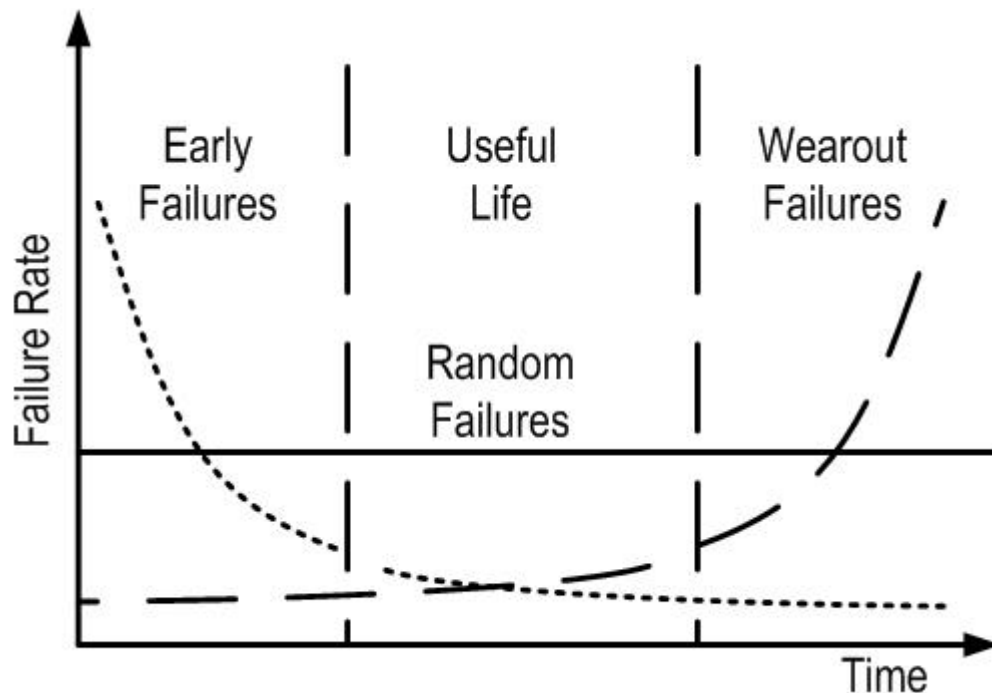


Figure 5.2 “bathtub” curve

It is common to assume a constant random failure rate; however, it has been demonstrated that this region does not exist for all devices. For example, block valves are characterized by dominant failure mechanisms, which are a function of time (i.e., low failure rate at initial installation, increased failure rate as the valve ages). Other statistical distributions may be considered, such as Weibull or log normal, when the failure rate varies significantly with time.

The random failure rate is characteristic to the device when it is operated in accordance with its specification and under the specific operational and MI conditions implicit in collected data. Reducing inspection and maintenance rigor affects timely detection of failures and may allow incipient conditions and degraded failures to propagate to complete failure. Reduced MI may also affect the device's failure rate. For example, mechanical equipment has a higher likelihood of failure when left in one position for extended periods of time. Periodic movement of mechanical equipment reduces the likelihood of some failure mechanisms.

Operating the device outside of the manufacturer's specification may damage or stress it, thereby causing early failure. Unexpected process application impact, such as chemical attack, corrosion, and deposition, or external environmental impact, such as electromagnetic interference, vibration, and heat, can also shorten its useful life.

Reliability practitioners often work with failure rates expressed as failures per million hours. The complete failure rate $\lambda_{\text{Complete}}$ can be determined by examining a pool of equipment N for the number of failures N_f over a time interval Δt .

$$\lambda_{\text{Complete}} = N_f / N \Delta t$$

Failure rates may be inverted and expressed as mean time to failure (MTTF) and may be expressed in years. MTTF and component life are not the same. If 2 in 100 devices fail the annual proof test, the MTTF is 50 years. The devices may have components that limit their in-service life. If all of the devices must be replaced within 10 years due to failure, the service life is 10 years.

5.4.1 PES failure rates

Table 5.1 represents data for logic solver components submitted by 7 logic solver suppliers that have a global presence in the process sector. The data provided is an average of the values submitted.

Table 5.1—Hardware failure rates

Item	Failure Rate failures/million hours		
	Low	Typical	High
Main Processor Board (memory, bus logic, communication)	12.00	25.00	50.00
Backup Control Unit	2.50	5.00	10.00
I/O Processor/Common logic I/O module	2.50	5.00	10.00
Single Digital Input Circuit	0.10	0.20	0.40
Single Digital Output Circuit	0.10	0.20	0.40
Single Analog Input Circuit	0.05	0.10	0.20
Single Analog Output Circuit	0.25	0.50	1.00
Relay (industrial type)	0.20	0.50	2.00
Electromechanical Timer	1.50	2.50	5.00
Solid state: Input circuit	0.10	0.20	0.40
Solid state: Output circuit	0.10	0.20	0.40
Solid state: Logic gate	0.01	0.10	0.20
Solid state: Timer	0.10	1.00	2.00
Inherently fail-safe solid state: Input circuit	0.05	0.10	0.20
Inherently fail-safe solid state: Output circuit	0.10	0.20	0.40
Inherently fail-safe solid state: Logic gate	0.001	0.01	0.10
Inherently fail-safe solid state: Off delay timer	0.05	0.50	1.00
Analog Trip Amplifier	0.20	0.40	0.80
Power supply	2.50	5.00	10.00
Common Cause Failures		Fractions	
Common Cause Factor -- β factor ¹	0.005	0.01	0.05

5.4.2 Failure rate data for commonly used field instrumentation

In order to predict the $MTTF^{SP}$ and PFD_{avg} of a SIS, the failure rates of the different devices, such as the sensor, logic solver, and final elements, is estimated. Failure rate data may come from a variety of different sources, such as public databases, user compiled maintenance records, vendor compiled field returns, reliability⁽¹³⁻¹⁸⁾ calculations or operating experience. Table 5.2 provides data submitted by users for various technologies.

Data Collection Efforts

1. *Process Equipment Reliability Database (PERD)*. CCPS supports this subscriber-based data collection effort. PERD has data taxonomies for collecting data associated with process events, process equipment failures and safeguard failures. PERD has published a guidelines book on data collection,

¹ The β factors are not associated with failure rates, e.g., a low failure rate does not necessarily have allow β factor.

has released a detailed analysis of pressure relief valves, and is currently taking data submissions from subscribers. <http://www.aiche.org/CCPS/ActiveProjects/PERD/index.aspx>

2. *PDS Forum*. This effort was initiated in 1995 to provide a forum for development of safety systems for off-shore applications and for exchanging lessons learned in operating equipment. This organization has published guidance on using the PDS method for quantifying the reliability and availability of SIS and periodically releases data to the public in the PDS Data Handbook. <http://www.sintef.no/Projectweb/PDS-Main-Page/>
3. *OREDA*. The Offshore Reliability Data (OREDA) project was established in 1981 with the objective to collect reliability data for safety equipment used in offshore and subsea applications. Publishes the OREDA data handbooks. <http://www.oreda.com>
4. *Instrument Reliability Network*. This collaborative network was established in 2012 at the Mary Kay O'Connor Process Safety Center at Texas A&M University. This network's mission is to benchmark current performance of instrumentation and controls in process industry applications, define a common taxonomy to support consistent collection of quality data from maintenance and proof test activities, and share lessons learned in improving instrumentation and controls reliability. Intend to publish and share data collected from user applications. <https://irn.tamu.edu>
5. *WIB (International Instrument Users' Association)*. This association has members in various European countries, the Middle East, Japan, Africa and North America, who are concerned with industrial automation, measurement and control. Companies that are involved in the manufacture or sale of instrumentation or control equipment for commercial purposes are excluded. This association collects data on instrumentation and controls in safety applications. <http://www.wib.nl>

Data Handbooks Available Commercially

1. *OREDA Offshore Reliability Data Handbook 5th Edition, Volume 1 – Topside Equipment, Volume 2 – Subsea Equipment, 5th Edition* (OREDA 2009). This reference contains data for a large range of process and control system equipment used on offshore platforms. The data is contributed by operating companies and can be considered “prior use” for off-shore applications; however, they may be appropriate for many other services since the internal environment is similar to that in many petrochemical and refining processes. Each edition [1st, 2nd, 3rd, and 4th] covers different years of data from the contributing companies.
2. IEEE Standard-493-2007, *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems* (2007). This reference contains data for electrical equipment. This data was determined through surveys of industrial and commercial installations. In the past, this reference has been referred to as the “Gold Book” due to its shiny gold dust cover.
3. *PDS Data Handbook* (SINTEF 2013). This handbook contains reliability data estimates for components used in control and safety systems implemented in off-shore and subsea applications. The database covers input devices (e.g., sensors, analyzers), logic controllers (e.g., electrical and electronic), and final elements (e.g., valves). The tables provide recommended data with references to expert judgment and other external data sources. Data is intended for use in SIS reliability analysis.
4. *Safety Equipment Reliability Handbook*, (exida 2007). This handbook provides data derived from theoretical analysis of the design of SIS equipment using failure modes, effects, and diagnostic analysis.
5. *SIL Solver®* (SIS-TECH 2015). This database is the result of a Delphi process that uses expert judgment to select appropriate failure rate values for typical process operating environments. The database covers electrical, electronic, programmable electronic, pneumatic and hydraulic equipment used in control and safety system applications. The database supports prior use assessments and

provides estimates of dangerous and spurious failure rates to support the calculation of the probability of failure on demand and spurious trip rate for instrumented systems.

6. *Electrical & Mechanical Component Handbook* (exida 2006). This handbook provides data derived from predictive analysis using IEC 62380 (2004). This database provides estimates of useful life values and failure rates.
7. *EPRD — Electronic Parts Reliability Data* (RIAC 2014). This database contains reliability data on electronic components used in commercial and military applications. It contains failure rate data on integrated circuits, discrete semiconductors (diodes, transistors), resistors, capacitors, and inductors/transformers.
8. *NPRD-95 — Non-electronic Parts Reliability Data* (RIAC 2011). This document contains failure rates for a variety of electrical, electro-mechanical and mechanical parts and assemblies.

Table 4.2—Example MTTF^D and MTTF^S for common field instrumentation (Years)

	Company A		Company B		Company C		Company D		Company E		Company F	
	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^S	MTTF ^S
Sensors												
Flow Switch			20-30	10-15	10	5	7	8	50	25	25	
Pressure Switch			20-30	10-15	35	15	16	20	75	60	35	20
Level Switch			20-30	10-15	25	5-10	80	60	100	50	30	60
Temp. Switch			20-30	10-15	15	5	10	20	100	25	10	12
Pressure Transmitter (service < 1500 psig)	100	100	40-60	20-30	50	25	60	60	150	80	55	55
Pressure Transmitter (service ≥ 1500 psig)	100	100	40-60	20-30			60	60	150	80	55	55
Level Transmitter	50	50	40-60	20-30	30	15	25	25	75	40	35	15
Flow Transmitter									75	60		
Orifice Meter	75	75	30-50	15-25	40	20	20	2	75	60	35	15
Mag Meter			40-50	20-25	100	25	150	150	75	40		
Coriolis Meter			40-60	20-30	40	15	76.1		75	40		
Vortex Shedding			40-60	20-30	50	10			100	60		
Temp. Transmitter	75	75	40-60	20-30	40	20	160	100	200	23	65	50
Flame Detector	10,000	1	15-30	5-15					30	24		
Thermocouple			60-80	30-40	40	20	20	10	200	23	100	20
RTD (Resistance Temp. Detect.)			60-80	30-40	30	15			150	40		
Vibration Proximitior	20	20	40-60	20-30	10	5			50	70		
Combustible Gas Detector									50	15	2.8	
Final Elements	(See Next Page)											

	Company A		Company B		Company C		Company D		Company E		Company F	
	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S	MTTF ^D	MTTF ^S
Final Elements												
Air Operate Gate Valve	50	50	30-50	15-25	50	25	40	40	50	100	40	40
Air Operate Globe Valve	50	50	40-60	20-30	60	25	40	40	50	100	40	40
Air Operate Ball Valve	50	50	40-60	20-30	50	25	40	120	60	150	40	40
Solenoid (DTT)	100	10	25-35	12-15	50	25	100	15	60	30	125	
Solenoid (ETT)	30	100							20			
Motor Starter			1000-1500						761	229		
Hydraulic Operated Ball Valve							25	80	100	100		
Motor Operated Ball Valve							15	135	15	134	30	
Annunciator							4	10	300	143		
Current Switch			25-35						62	62		
Relay			1500-2500				70	40	500	400		
Trip Amplifier									713	196		

6 Average probability of failure on demand

The probability of failure on demand is the metric used to describe the safety integrity for the SIF. It is the probability that the safety instrumented function will fail in a manner that renders it incapable of performing its intended safety function when a process demand occurs. As such, the SIF will be unable to respond to a demand and no safety action (e.g., shutdown) will be initiated. For a SIF, the average probability of failure on demand (PFD_{avg}) is related to one of four discrete SILs as given in ISA-84.00.01. To satisfy the requirements of a given SIL, the PFD_{avg} should be less than the upper limit provided in ISA-84.00.01.

Since this failure probability is based “on demand” of the SIF, the frequency of demands becomes important. This clause addresses SIF operating in “low demand” mode that as a rule of thumb means less than one demand per year. More frequent demands should be considered “high demand.” A high demand mode SIF must be demonstrated to provide a specified failure frequency, which requires a different analysis that is outside the scope of this technical report. Refer to ISA-TR84.00.04 Annex I for more guidance on low and high demand mode.

In general, the probability of failure on demand is a function of the failure rate, diagnostics, repair rate, test interval, common cause, architecture, and configuration. The dangerous undetected failure rate is strongly impacted by the diagnostic coverage provided for random hardware failures. Comprehensive diagnostics dramatically improve the diagnostic coverage, thereby reducing the possibility of a dangerous undetected failure, and consequently minimizing the PFD_{avg} . Identified device failures, whether found through diagnostics or proof testing, should be repaired after detection and the device should be returned to service in the “as good as new” condition.

It is important to recognize that the SIF architecture, including the number and quality of field devices, has a major impact on the PFD_{avg} for the SIF. If one assumes a single input with a $MTTF^{DU}$ of 30 years, a single output with a $MTTF^{DU}$ of 50 years, and a logic solver with a $MTTF^{DU}$ of 100 years, about 85% of the SIF PFD_{avg} will fall in the field devices and about 15% in the logic solver, see example in Figure 6.1. On the other hand, using redundant inputs and outputs with the same $MTTF^{DU}$, configured for high safety availability and with the same logic solver, the PFD_{avg} for the field devices may account for only 25% and the logic solver may account for 75% of the SIF PFD_{avg} , see example in Figure 6.2. The distribution of SIF PFD_{avg} will change as the number and type of system elements and the subsystem architectures vary. Therefore, enhancing the PFD_{avg} of the logic solver (E/E/PES) of the SIF without corresponding enhancement of the field devices may not be effective in improving the SIF SIL. On the other hand, when a single logic solver supports multiple SIFs, improvements in the integrity of the logic solver will lower the overall risk.

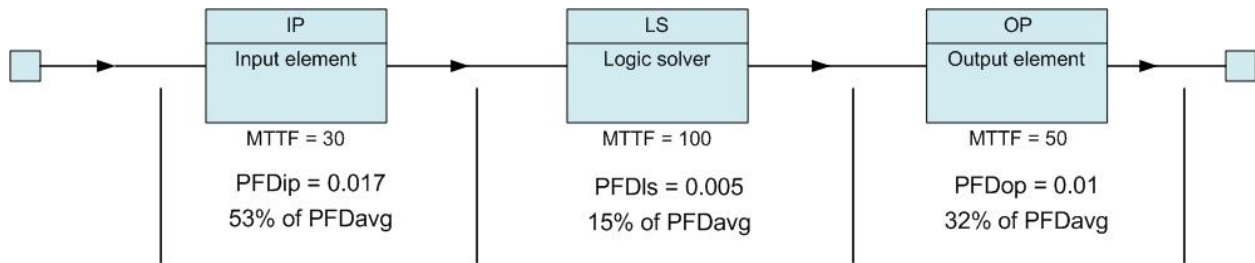


Figure 6.1 – Reliability block diagram (RBD)² for SIF with single input, output and logic solver, with 1 year proof test interval,

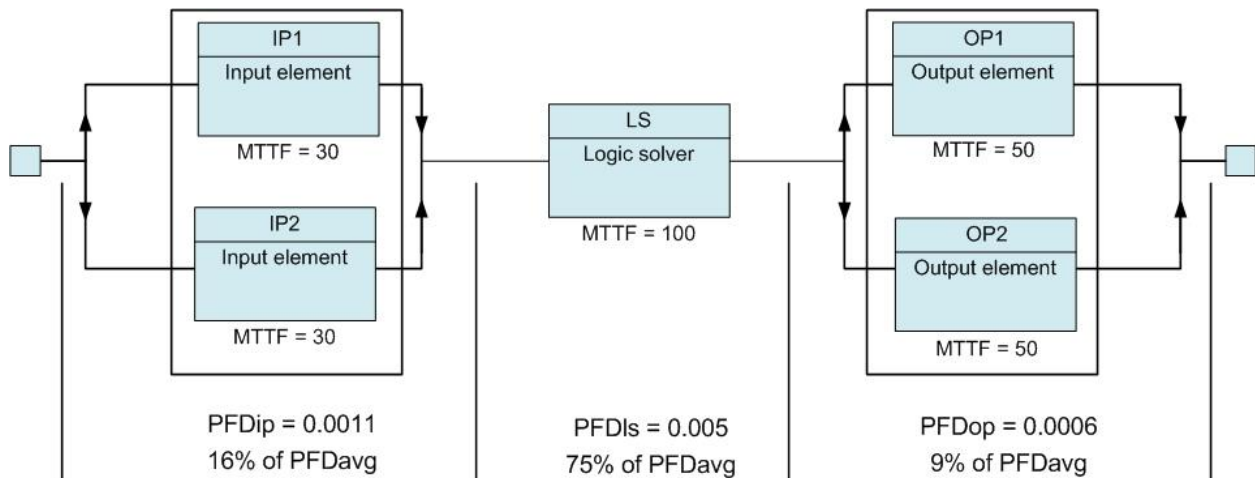


Figure 6.2–SIF with 1oo2 input, 1oo2 output and single logic solver, with 1 year proof test interval and 5% beta factor

As shown previously, the dangerous failure rate can be determined from the mean time to failure dangerous (MTTF^D):

$$\lambda_D = \frac{1}{MTTF^D} \quad 6.1$$

The PFD_{avg} calculation generally assumes that this failure rate is constant. Since all things degrade with time, a constant failure rate can only be achieved when the device is subjected to a rigorous mechanical integrity program involving regularly scheduled inspection, preventive maintenance, and proof testing. The required rigor of inspection and preventive maintenance is affected by many factors, such as the device manufacture, operating environment, and support system quality.

When N devices are installed, voting subsystems can be created, where M represents the number of devices that must agree out of the total N. The PFD_{avg} of MooN (M out of N) voting subsystems can be estimated using Markovian or Boolean algebra averaging. These approaches yield different numerical results for architectures where M≠N. Both approaches are considered acceptable for

² A RBD shows component success states rather than the typical failed states of a Fault Tree.