TECHNICAL REPORT
ISA-TR84.00.03-2012

Mechanical Integrity of Safety Instrumented Systems (SIS)

Approved 28 August 2012

ISA-TR84.00.03-2012
Mechanical Integrity of Safety Instrumented Systems (SIS)

ISBN: 978-1-937560-57-7

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-TR84.00.03-2012.

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

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

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

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

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

HOWEVER, ISA ASKS 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 served as members of ISA84 in developing this technical report:

NAME	COMPANY
W. Johnson, Chair	Consultant
V. Maggioli, Co-Managing Director	Feltronics Corp
D. Zetterberg, Co-Managing Director	Chevron Energy Technology Company
K. Gandhi, Working Group Chair	KBR
A. Summers, Working Group Editor	SIS-TECH Solutions LP
R. Adamski	RA Safety Consulting LLC
T. Ando	Yokogawa Electric Co
R. Avali	Westinghouse Electric Corp
L. Beckman	Safeplex Systems Inc
J. Campbell	Consultant
I. Chen	Aramco
R. Chittilapilly	Oil & Natural Gas Corp
M. Coppler	Det Norske Veritas Certification Inc
M. Corbo	ExxonMobil
P. Early	Langdon Coffman Services
C. Fialkowski	Siemens Inc
I. Gibson	Consultant
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida Com LLC
P. Gruhn	ICS Triplex
B. Hampshire	BP
J. Harris	UOP A Honeywell Company
J. Jamison	EnCana Corporation Ltd
R. Johnson	Consultant
K. Klein	Chevron
T. Layer	Emerson Process Management
E. Marszal	Kenexis Consulting Corp
N. McLeod	ARKEMA
M. Mollicone	SYM Consultoria
G. Ramachandran	Systems Research Intl Inc
R. Roberts	Suncor Energy Inc
M. Scott	AE Solutions
D. Sniezek	Lockheed Martin Federal Services
C. Sossman	CLS Tech-Reg Consultants
R. Strube	Universal Instruments Corporation
L. Suttinger	Savannah River Nuclear Solutions
T. Walczak	Conversions Inc
M. Weber	System Safety Inc
A. Woltman	Shell Projects and Technology-Engineering
P. Wright	BHP Engineering & Construction Inc

This technical report was approved for publication by the ISA Standards and Practices Board on 28 August 2012.

NAME	COMPANY
D. Dunn, Vice President	Aramco Services Co.
D. Bartusiak	ExxonMobil Chemical Co.
P. Brett	Honeywell Inc.
J. Campbell	Consultant
M. Coppler	Det Norske Veritas Certification Inc.
E. Cosman	The Dow Chemical Company
B. Dumortier	Schneider Electric
J. Federlein	Federlein & Assoc. Inc.
J. Gilsinn	NIST/EL
E. Icayan	ACES Inc.
J. Jamison	EnCana Corporation Ltd.
K. P. Lindner	Endress + Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
T. McAvinew	Instrumentation and Control Engineering, LLC
R. Reimer	Rockwell Automation
S. Russell	Valero Energy Corp.
N. Sands	DuPont
H. Sasajima	Azbil Corp.
T. Schnaare	Rosemount Inc.
J. Tatera	Tatera & Associates Inc.
I. Verhappen	Yokogawa Canada Inc.
W. Weidman	WCW Consulting
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa IA Global Marketing (USMK)
D. Zetterberg	Chevron Energy Technology Co.

This page intentionally left blank.

Contents

Foreword

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

The ISA84 committee has developed a series of complementary technical reports to provide guidance, as well as practical examples of implementation, on various topics and applications. Three of these technical reports, ISA-TR84.00.02, ISA-TR84.00.03, and ISA-TR84.00.04, provide informative guidance related to specific phases of the Safety Instrumented System (SIS) lifecycle. Figure 8 and Table 2 have been adapted for this foreword as shown in ISA-TR84.00.04 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.

ISA-TR84.00.02—Safety Integrity Level (SIL) Verification of Safety Instrumented Functions—Lifecycle phase 4 requires verification that the intended or installed SIS meets its specified SIL. To support the calculation of the average probability of failure on demand as required by ANSI/ISA-84.00.01 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 an SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured MI program as described in ISA-TR84.00.03.

ISA-TR84.00.03—Mechanical Integrity of Safety Instrumented Systems (SIS)—Lifecycle phases 5 and 6 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 ISA-TR84.00.02 and the selection and continued use of devices as discussed in ISA-TR84.00.04 Annex L.

ISA-TR84.00.04—Guidelines for the Implementation of ANSI/ISA-84.00.01—Lifecycle phases 2, 4, 9 and 10 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 ANSI/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 Basic Process Control System (BPCS) and SIS (Annex F), field device and logic solver selection (Annex L), manual shutdown

considerations (Annex P), and design/installation considerations (e.g., wiring, power, relationship to BPCS, common mode impacts, fault tolerance, etc. – Annex N). ISA-TR84.00.02 expands Annex G, which only provides a brief introduction to the topic of failure calculations. ISA-TR84.00.04 does not address the MI program, which is discussed in ISA-TR84.00.03.

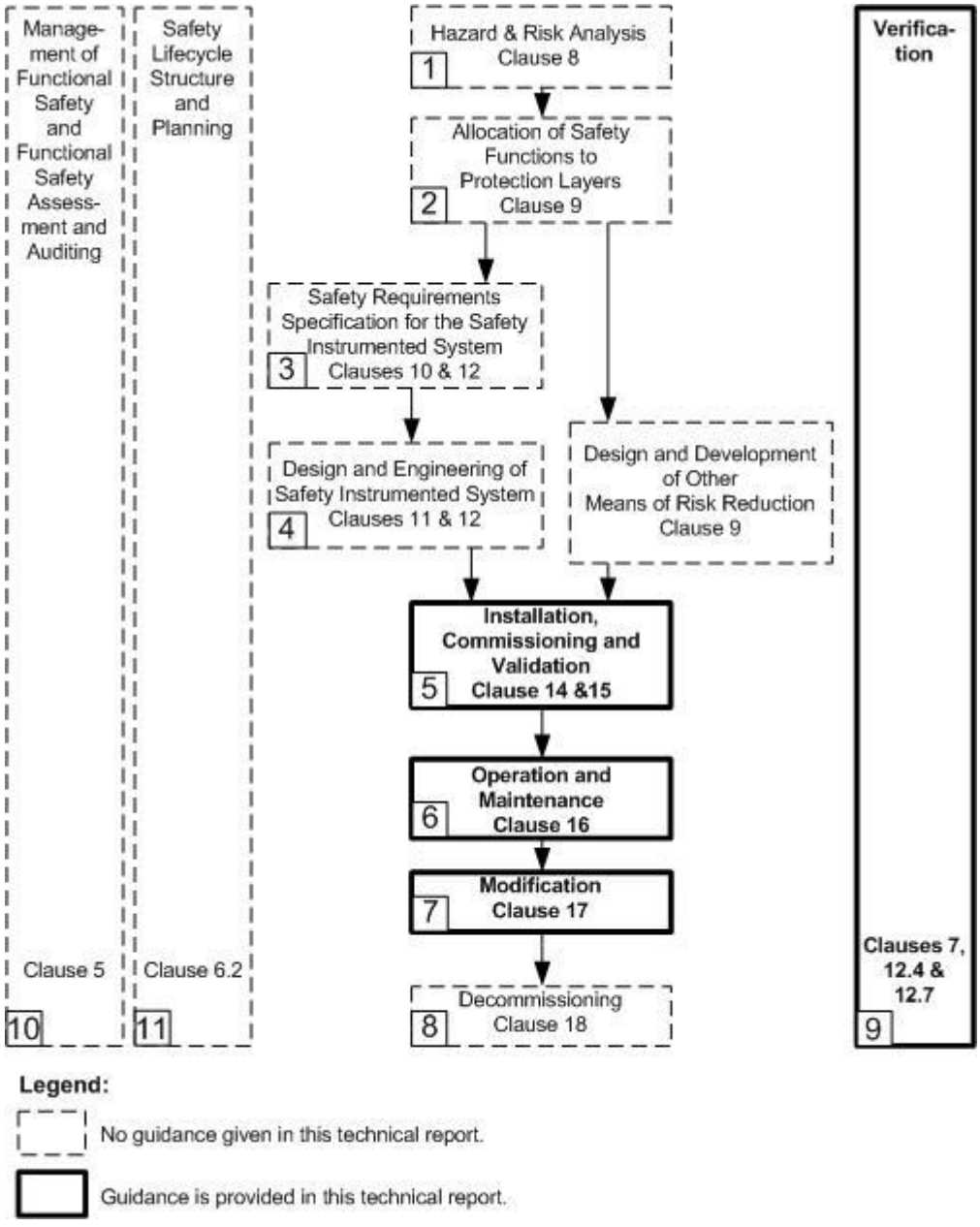


Figure 1 — SIS safety lifecycle phases (modified ANSI/ISA-84.00.01-1 Figure 8)

Table 1 — SIS safety lifecycle overview (modified ANSI/ISA-84.00.01-1 Table 2)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 requirements clause	ISA-84 Technical Report reference
Figure 1 box number	Title			
1	Hazard and risk analysis	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	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 on documenting the SRS. An example is shown in ISA-TR84.00.04 Part 2. All three technical reports (ISA-TR84.00.02, 03, and 04) provide fundamental considerations for SRS development
4	SIS design and 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 and 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**

(Continued on next page)

(Table 1 cont'd from previous page)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 requirements clause	ISA-84 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 judgement on the functional safety achieved by the SIS.	5	ISA-TR84.00.04 Clause 3 and Annexes A, C, D, E, and S

1 Scope and purpose

A process hazards analysis is used to identify the safety functions necessary to reduce the risk of identified hazardous events. When a safety function is implemented in a safety instrumented system (SIS), the risk reduction required from the safety instrumented function (SIF) is related to one of four discrete safety integrity levels (SIL). The function and system are designed and managed according to ANSI/ISA-84.00.01, which establishes requirements necessary to claim the specified SIL for the SIS throughout its life.

A critical aspect of maintaining the SIL is the implementation of a mechanical integrity (MI) program that monitors the installed performance of the SIS equipment and takes corrective action when the performance does not meet the requirements. 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 is maintained in the “as good as new” condition

This edition of ISA-TR84.00.03 provides considerations for establishing an MI program for SIS; it focuses on how to plan and implement a comprehensive MI program rather than including specific test procedures as in the previous edition. This technical report does not provide complete details on how to safely or fully execute all MI activities in an operating facility. Individuals who are assigned responsibility for MI activities must determine what is necessary to maintain the safety integrity of a specific SIS.

The MI program involves many activities that occur throughout the SIS lifecycle, but it predominantly focuses on the timely detection and correction of incipient/degraded conditions and complete failures to ensure that the SIS operates as specified when required. Rigorous inspection and complete proof testing is required for all SIS equipment whether existing or new. While the frequency of these activities may vary due to the required SIL, the purpose and goal of inspection and proof testing are not affected by the SIL.

Inspection and proof testing is required to:

- meet regulatory requirements
- meet ANSI/ISA-84.00.01 requirements
- meet equipment manufacturer requirements (e.g., safety manual)
- demonstrate through witnessed test and preventive maintenance records that the equipment is being maintained in the “as good as new” condition
- detect and correct unrevealed failures
- verify that the MI program and test interval are sufficient to ensure functional and integrity requirements are met for the equipment life
- monitor equipment for degradation mechanisms (incipient and degraded) which may compromise future performance
- identify when equipment has reached wear-out and requires replacement
- provide data and information to facilitate the evaluation of MI program success and to support continuous improvement

The technical report addresses:

- the identification of personnel roles and responsibilities when developing an MI plan,
- important considerations in establishing an effective MI program, and
- detailed guidance and examples to support user-specific work processes as part of an overall MI program.

2 Audience

The successful design and management of SIS is dependent on many departments within an operating facility. Likewise, an effective MI program is a fundamental element of the SIS lifecycle with many departments having responsibility. Consequently, the target audience of this technical report is very broad and includes all personnel who impact program success. These personnel perform certain roles and have responsibility for execution of many different tasks during various lifecycle phases. Typical roles and responsibilities include:

- Engineering Manager --- Ensures that engineering work processes are in place to determine the required rigor of the MI program for all SIS, and subsequently to ensure that Operations and Maintenance departments are engaged in determining how this testing can be accommodated in a practical and effective manner.
- Design Engineer --- Ensures maintenance provisions for safe and cost effective inspections and testing are met as the SIS proceeds through the design phase.
- Project Manufacturing/Operations Representative --- Ensures all roles communicate and fulfill their responsibilities on projects, including development of validation, commissioning, proof test procedures and documentation handoffs.
- Process Automation/Control System Engineer --- Ensures all aspects of on-line testing, demand tracking, bypassing are adequately addressed in design phase to deliver necessary functionally across operations lifecycle including appropriate use of process historians to track demands on the SIS.
- Process Engineer --- Provides operation and technical information to ensure testing and associated procedures are completed satisfactorily and no new hazards are introduced during this process.
- PSM Manager --- Ensures that recommendations related to the SIS are tracked to completion and that an effective Management of Change (MOC) process is in place, which involves review and approval of proposed changes to SIS by competent personnel.
- Maintenance Manager --- Ensures that an effective management system is in place to execute reliability and maintenance activities required to ensure SIS integrity including a training program for maintenance personnel to maintain qualifications.
- Operations Manager --- Ensures that Operating personnel are committed to providing the opportunity for identified MI activities to take place in a planned manner including a training program for Operations personnel to maintain qualifications. This role has the ultimate responsibility to ensure the lifecycle management rigor and SIS integrity within the operating facility.
- Management Team --- Consists of the Project Manager, Maintenance Manager and Operations Manager and ensures that competent and trained personnel receive the appropriate level of support are available to carry out the identified activities and that SIS installations are maintained inspected, tested and operated in accordance with ANSI/ISA-84.00.01.
- SIS Specialist/Engineer --- Works with both Engineering and Maintenance personnel to develop and maintain the SIS equipment list and to define the MI requirements necessary to ensure SIS integrity throughout the lifecycle of the facility. To ensure that SIS are appropriately installed, inspected, tested and validated to demonstrate correct functionality and performance prior to handover to Operations.
- Reliability Specialist --- Advises the SIS Specialist/Engineer on appropriate testing and reliability techniques. To apply the management system and ensure that testing activities are performed effectively with appropriate supporting documentation including procedures and results records. To address any non-compliance/failures in a timely and effective manner that addresses the root cause of the failure to minimize repeat failures. To facilitate data capture and analysis in support of on-going demonstration of SIS MI and continuous improvement.

- Maintenance (and Construction) Supervision --- Understands the importance of SIS MI and provides the necessary resources to ensure that all identified MI activities are completed in a planned manner.
- Maintenance (and Construction) Technician --- Understands purpose and function of the SIS, the importance of inspection, preventive maintenance and testing plans, and how to complete the required documentation to support data collection.
- Testing Personnel --- Appreciate the concepts of SIS MI and the rigor required in the identification and reporting of SIS failures.
- Training Coordinators --- Ensures training of all roles impacting or impacted by SIS across the plant operating lifecycle occurs in a timely manner.

It is expected that those persons identified as the audience possess an understanding of the requirements of ANSI/ISA-84.00.01 appropriate to their level of responsibility and technical expectation.

3 Definitions

Definitions which are new and not previously documented in ANSI/ISA-84.00.01 are indicated with (*).

3.1
allowable time to repair*
length of time that has been determined by hazard and risk analysis to be acceptable for continued process operation with degraded or disabled equipment. Time is often constrained by Operations ability to maintain the necessary compensating measure.

3.1.1
application program
program specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the input, output, calculations, and decisions necessary to meet the SIS functional requirements.

3.1.2
Application Program Factory Acceptance Test (APFAT)*
formal testing of the configuration. The advantage of this type of test is that it can be independent of all or most of the physical hardware, thereby supporting the concept of an HWFAT. See FAT.

3.1.3
as good as new*
equipment is maintained in a manner that sustains its useful life. “As good as new” often refers to the initial condition after proof test and subsequent repair/overhaul (as needed) so that the probability of failure at time 0 is zero and the failure rate expected during the useful life is unchanged.

NOTE When a device is returned to its “as good as new condition,” the expectation is that the as-left condition will support operation within specification until the next scheduled proof test.

3.1.4
compensating measure*
planned and documented means for managing risk that are implemented during any period of maintenance or process operation with known faults or failures in the SIS, which result in increased risk

3.1.5
complete failure*
failure that results in a 100% loss of a required function. The failure can be further classified as safe or dangerous depending on the application and desired operation.

3.1.6
degraded condition*
failure that results in a partial loss of function, that is less than “as good as new,” but does not result in a complete loss of the function. Degraded condition also includes any time a portion of the SIF is bypassed, but is still able to perform its function automatically.

3.1.7
detected failure
in relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation. Synonyms include announced, revealed and overt.

NOTE* Software faults can include errors within the application program, embedded program (operating system), embedded firmware, or utility software (programming panel).

3.1.8
failure
the termination of the ability of equipment a functional unit to perform a required function

3.1.9
failure cause*
the circumstances during design, manufacture, or use which led to failure

3.1.10
failure mechanism*
the physical, chemical, or other process, or combination of processes, that has led to failure

3.1.11
failure mode*
the observed manner of failure. The failure modes describe the loss of required system function(s) that result from failures.

3.1.12
failure to activate*
occurs when the SIS does not respond to the process deviation and an event occurs or the SIS needs to be manually activated

3.1.13
fitness for service*
management system used to assess the current condition of equipment to determine whether it is capable of continuing operation within equipment specification until the next opportunity to test or perform maintenance

3.1.14
Hardware Factory Acceptance Test (HWFAT)*
testing of SIS equipment, panels I/O, power supplies, panel grounding, and related equipment at the manufacturer's fabrication facility to insure that the SIS equipment has been installed and wired properly

3.1.15
Integrated Factory Acceptance Test (IFAT)*
formal testing of SIS and BPCS simultaneously to insure that the combine actions result in the desired safe automation of the process

3.1.16
incipient condition*
the equipment operates within specification but in its current state is likely to result in a degraded condition or complete failure if corrective action is not taken

3.1.17
integrity*
ability of the SIS to perform the required SIF as and when required

3.1.18
Mean Repair Time (MRT)*
expected overall repair time

NOTE MRT encompasses the times (b), (c) and (d) of the times for MTTR.

3.1.19
Mean Time between Failure (MTBF)*
for a repairable device, mean time to failure + the mean time to restoration

3.1.20
Mean Time to Failure (MTTF)*
the average time before equipment's first failure. May refer to all failures, specific failure classifications, specific failure modes, or specific failure causes.

3.1.21
Mean Time to Repair*
term has been replaced by Mean Time to Restoration or Mean Repair Time

3.1.22
Mean Time to Restoration (MTTR)*
expected time to achieve restoration

NOTE MTTR encompasses:

a) the time to detect the failure; and

b) the time spent before starting the repair; and

c) the effective time to repair; and

d) the time before the device is put back into operation.

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

3.1.23
mechanical integrity*
management system assuring equipment is inspected, maintained, tested and operated in a safe manner consistent with its risk reduction allocation

3.1.24
out of service*
includes any time the SIF is unavailable during an operating mode where the hazard exists

3.1.25
partial testing*
method of proof testing that checks a portion of the failures of a device, e.g., partial stroke testing of valves and simulation of input or output signals

3.1.26
pass/fail criteria*
pre-established criteria that define the acceptability of equipment operation relative to the SRS and equipment specification

3.1.27
proof test
test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality

3.1.28
proof test coverage*
expressed as the percentage of failures that can be detected by the proof test. A complete proof test should provide 100% coverage of the failures.

3.1.29
reliability*
ability of a system or device to perform its specified function under stated conditions for a specified period of time

3.1.30
safety instrumented function (SIF)
safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function

3.1.31
safety instrumented system (SIS)
instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s) and final elements (s).

3.1.32
site integration test (SIT)
formal testing of the ability of the SIS and BPCS to be able to properly communicate with each other once those systems have been installed in the field. It also can include any third party systems that need to interface with the BPCS.

3.1.33
useful life*
the portion of equipment's life where the failure rate can be considered constant where early life failures have been corrected and end of life failures have not begun

3.1.34
wear-out*
the time when equipment's failure rate begins to increase due to various failure mechanisms

4 Abbreviations/Acronyms

Abbreviations which are new and not previously documented in ANSI/ISA-84.00.01 are indicated with (*)

AC/DC	Alternating Current/Direct Current
ANSI	American National Standards Institute
APFAT*	Application Program Factory Acceptance Test
BPCS	Basic Process Control System
CCPS*	Center for Chemical Process Safety
EH&S	Environment Health and Safety
ESD	Emergency Shutdown System
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FMEA*	Failure Mode and Effects Analysis
HMI	Human Machine Interface
HSE	Health and Safety Executive
HWFAT*	Hardware Factory Acceptance Test
IEC	International Electrotechnical Commission
IFAT*	Integrated Factory Acceptance Test
I/O*	Input/Output
ISA	International Society of Automation
IT	Information Technology
MI	Mechanical Integrity
MOC	Management of Change
MTBF*	Mean Time between Failure
MTTF*	Mean Time to Failure
MTTR*	Mean Time to Repair (also known as Mean Time to Restoration)
NIST	National Institute of Standards and Technology
OSHA*	Occupational Safety and Health Administration
PERD*	Process Equipment Reliability Database
PES	Programmable Electronic Systems

PFD_{avg}	Average Probability of Failure on Demand
P&IDs*	Piping and Instrumentation Diagrams
PHA*	Process Hazard Analysis
PLC	Programmable Logic Controller
PPE*	Personal Protective Equipment
PSD	Process Shutdown System
PSM*	Process Safety Management
RTD	Resistance Temperature Detector
SAT	Site Acceptance Test
S/D	Shutdown
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SIT*	Site Integration Test
SOE	Sequence of Events
SRS	Safety Requirements Specification
TC	Thermocouple
UPS*	Uninterruptible Power Supply
1oo1	one-out-of-one
1oo2	one-out-of-two
2oo3	two-out-of-three

5 MI planning considerations

For SIS, planning is covered in ANSI/ISA-84.00.01 Clauses 5, 6, 7 15, 16, and 17. MI planning involves establishing the management system and the maintenance requirements (e.g., inspection, preventive maintenance, and proof testing) for the SIS equipment. With limited resources, it is important to identify and classify instrumentation and controls, so that plant personnel know what equipment must be managed as safety. Fundamentally, all equipment is covered by MI but only a portion of the equipment must be rigorously managed according to ANSI/ISA-84.00.01. Classification is performed and documented during the process hazards analysis as discussed in the standard ISA-84.91.01 and technical report ISA-TR91.00.02. The MI program should cover all equipment required to support the SIF integrity and reliability, including sensors, logic solvers, final elements, utilities, communications, and diagnostic equipment.

The facility safety and operating culture should be considered when designing the SIS, because the culture affects the MI program, which must be capable of supporting the SIS functional and integrity requirements defined in the safety requirements specification (SRS). Once an SIS is designed and implemented, independence, integrity, functionality and reliability become inherent attributes of the installation, which are proven through periodic MI activities, such as inspection and testing, and supported through preventive maintenance and planned replacement/upgrade. Auditability, access security, and management of change are attributes of the management system, which are proven through periodic assessment and auditing activities. These core attributes, namely independence, integrity, functionality, reliability, auditability, access security, and management of change, must be managed throughout the SIS lifecycle with sufficient rigor so that the SIS achieves and maintains the required safety integrity.

The planning phase of the ANSI/ISA-84.00.01 lifecycle includes development of MI procedures and implementation of training programs for a variety of activities:

- documentation transfer and lifecycle management from Design Engineering to Facility Maintenance and Operations,
- identification of the minimum data fields to be included in the facility maintenance management system,

  NOTE These data fields are intended to support scheduling of inspections and tests and the capture of data and information for tracking failures impacting integrity and reliability
- commissioning procedures and documentation of corrective actions,
- identification and tagging of SIS equipment in the field,
- managing failure conditions during plant operation, inspection, preventive maintenance, and proof testing,
- controlling and monitoring the use of bypasses,
- investigation of process demands, spurious trips, and dangerous failures,
- performing follow-up failure investigations and communicating findings for continuous improvement,
- minimum required inspection and preventive maintenance practices to maintain equipment MI,
- minimum required proof testing to ensure correct operation of equipment,
- minimum requirements for proof testing following modification and repair,
- change management, including specific provisions for access security, configuration management, planned modification, temporary modification, and decommissioning, and
- appropriate degree of training for impacted personnel within Operations and Maintenance.

Figure 2 provides an illustration of the safety lifecycle relative to MI activities. As the project moves from concept through detailed design, a validation plan is developed to ensure the SIS

meets the desired functionality and integrity. Validation demonstrates that each SIF and its supporting utilities/diagnostics fully achieve the SRS prior to being placed into service. Validation is required for any new or modified SIS.

A Factory Acceptance Test (FAT) of the SIS logic solver and other packaged equipment is generally conducted prior to site installation. An FAT allows rigorous testing of the equipment in a controlled environment without the time pressure that often occurs during on-site testing. ANSI/ISA-84.00.01 does not require an FAT to be performed, but many users consider the FAT a cost effective means of ensuring that packaged equipment, such as logic solvers, work according to specification.

During construction and commissioning, the SIF sensors, final elements and ancillary support equipment (e.g., air supplies, power supplies, communications, and interfaces) are installed according to design documents and installation details. Inspection and commissioning procedures are used to ensure the SIS equipment is installed and operating properly. Following equipment commissioning, validation is conducted. Validation includes evidence from an end-to-end test of the installed SIS and its SIF operate as required. Validation should be performed after major process or SIS modifications.

Once operational and for as long as the plant continues to operate, the SIS equipment should be periodically inspected to detect incipient and degraded conditions and to initiate corrective action through equipment repair or replacement. Preventive maintenance whether on a fixed schedule or based on condition is conducted to replace wearable or short-life parts to extend the useful life of the equipment. Proof testing is required to demonstrate that the SIS equipment is operating as specified and to identify deviations from acceptable operation so they can be corrected. Test records provide documented proof that the SIS is achieving the required safety integrity level (SIL). All SIS equipment should be tested, including field sensors, final control elements, logic solvers, Human Machine Interfaces (HMI), communication links with other systems, user application program, and any required support systems, such as power or instrument air.

Many processes have operating cycles that are longer than the test interval necessary to theoretically achieve the SIL. Therefore, the ability to perform testing while the process remains in operation (e.g., on-line) is often desirable. The requirements of ANSI/ISA-84.00.01 can be met using off-line testing with the process shutdown, on-line testing with the process in operation or a combination of on-line and off-line testing. All means of testing can be supported by manual and automated procedures and techniques.

This technical report provides guidance and examples for off-line and on-line testing based on the experience of the working group members, but these examples should not be considered the only means for achieving the objectives of ANSI/ISA-84.00.01.

There are several considerations that go into developing a holistic MI program. Each of these considerations is discussed in more detail in later clauses:

- identification of the equipment and systems to be covered by SIS MI
- determination of the maintenance strategy to be used for each type of equipment
- collection and retention of lifecycle documentation
- defining personnel roles and responsibilities and ensuring competency
- defining management system and performance metrics
- implementing configuration management and management of change
- performing audits to determine MI program compliance

5.1 Identification of the equipment and systems to be covered by SIS MI

The following information at a minimum should be transferred from the design information to the organization responsible for facility maintenance and record system to ensure proper scheduling and completion of inspections, preventive maintenance, proof tests and reliability improvement:

- production unit or plant identification (e.g., hydrocarbon alpha 1)
- process unit within the production unit (e.g., quench unit)
- tag item number (e.g., FT-10001)

  NOTE Any facility testing or calibration equipment used to validate or test SIS devices should also be identified in the maintenance management system to ensure calibration certifications are performed as required.
- location description (e.g., T-630 discharge)
- manufacturer (e.g. XYZ Instruments, Inc.)
- model number (e.g.,1234DP)
- pipe spec or process description (e.g., river water)
- equipment group or family (e.g., flow)
- equipment type (e.g., vortex)
- serial number
- SIF identification number
- date installed
- calibration, tolerance, and configuration values (e.g., span, filtering, square root extraction, fail-direction on detected fault, leak tightness)
- inspection/proof test interval

  NOTE The maintenance management system is used to generate notifications for inspections, preventive maintenance, and proof tests based on last maintenance date and specified interval.

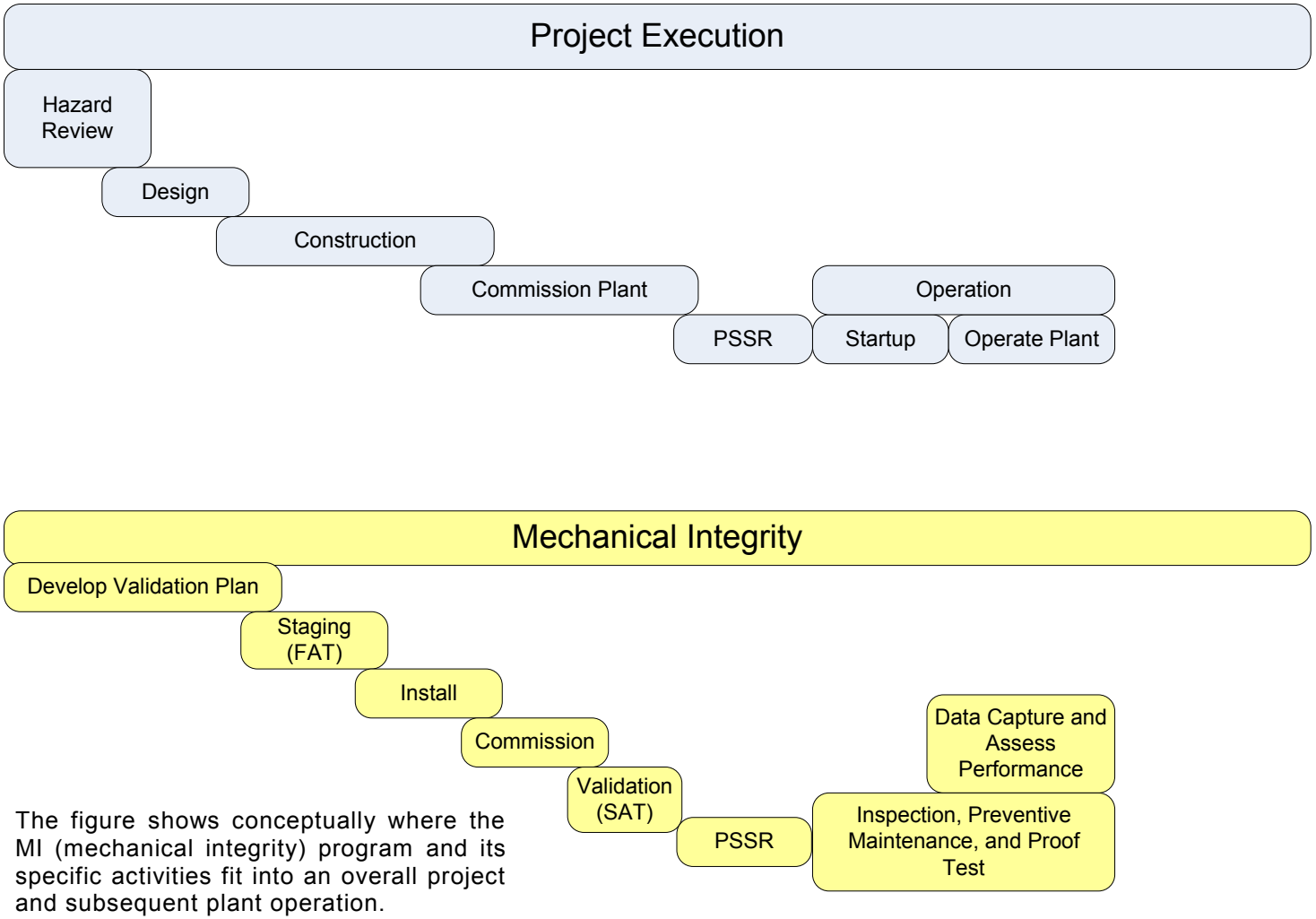


Figure 2 — Mechanical integrity across the lifecycle

5.2 Determination of the maintenance strategy to be used for each type of equipment

The MI plan ensures that the facility maintenance strategy is in agreement with the intent of the SIS MI program – that the equipment is maintained in the "as good as new" condition through its lifecycle. There are three basic maintenance strategies employed within the process industry, depending on the type of equipment:

- Preventive (planned) maintenance: Specifically defined maintenance is performed on a periodic schedule, e.g., annual change out of air supply filters on automated valves.
- Predictive (condition-based) maintenance: Applicable maintenance is initiated based on monitoring equipment condition through inspection, diagnostics, and observation, e.g., valve response to control signal is sluggish, indicating that a particular type of maintenance such as an air filter change out is required.
- Corrective (reactive) maintenance, also known as "run to failure": Neither preventive nor predictive maintenance is performed. Repair or replacement is initiated based on detecting equipment failure. ***Though a viable maintenance strategy for some general equipment population, it should not be used for SIS equipment where dangerous undetected failures can occur.***

Effective MI planning ensures that the maintenance strategy is consistent with maintaining the SIS integrity. The SIS MI plan should be a component of the facility's overall MI plan. The plan begins its development in the early stages of design to ensure the needs of the operating facility are addressed and that test and maintenance facilities are implemented to meet procedure requirements. MI planning includes the development of procedures on how to plan, perform and document the following:

- inspections
- repairs
- preventive maintenance
- calibrations
- proof tests
- reliability data capture and analysis
- loop check/commissioning procedures
- validation procedures
- feedback to ensure continuous improvement

5.3 Collection and retention of lifecycle documentation

Various disciplines are involved in developing lifecycle documentation, including Operations, Maintenance, and Design Engineering. The owner/operator is the ultimate owner of documentation generated by Engineering and Maintenance. Documentation should be treated as a long-term asset similar to the equipment within the operating facility. Engineering and Maintenance uses and maintains the various documents described within the technical report. The MI plan should define which documents will be transferred from Engineering to Maintenance/Operations, where and in what form the master documents will be stored, who will be the custodian, role(s) or person(s) who will maintain the master documents as evergreen. The MI plan sets the foundation on how procedures such as those for proof testing and reliability are accessed and maintained to provide for continuous improvement and value delivery.

All operating facilities should comply with their respective corporate records retention guidelines and policies. The records may be maintained electronically or hard copy in on-site or off-site storage. MI records are needed for tracking and trending equipment failure. These records are typically reviewed whenever a functional safety assessment (see ISA-TR84.00.04 Annex D), prior use assessment (see ISA-TR84.00.04 Annex L User approval) or audit (see ISA-

TR84.00.04 Annex E) is performed. Regulatory authorities may establish the minimum retention period for MI records. For example, OSHA PSM requires that records to be maintained for the facility life. Practically, records should be retained in a form and for a period of time sufficient to support user approval and reliability assessment of equipment.

5.4 Defining personnel roles and responsibilities and ensuring competency

MI planning also ensures that personnel understand their roles and responsibilities in supporting the maintenance strategy. Maintenance/Reliability personnel have a significant role in MI planning and execution, but Operations and Engineering must support many specific tasks. Maintenance/Reliability, including supervision, engineers, mechanics, and I&E technicians, develop the SIS MI plan with dialogue and input from Operations and Design Engineering. Successful completion of tasks defined in planning requires the active involvement of various disciplines.

All personnel associated with the SIS, including Management, Operations, Maintenance, and Engineering, should be competent in performing their assigned tasks. Management should understand how the SIS operates to reduce risk and how their decisions affect its integrity. Engineering choices influence the SIS design, test facilities, and proof test interval, so they should understand how their choices affect long-term operation and maintenance. Maintenance and Operations personnel need to have the knowledge, training and skills necessary to ensure the SIS integrity is maintained throughout its installed life. Competency for all personnel extends beyond simple knowledge of how to perform basic tasks; it also includes knowledge of how the SIS equipment functions to achieve or maintain a safe state of the process.

Consequently, unlike other process safety programs, the training and skills for SIS MI cover a significant range of subjects. It is generally not possible to provide a single training package for everyone. Rather it requires the training program to be tailored to support the site culture and the specific SIS equipment.

5.5 Ensuring maintenance personnel skills and training

This subclause specifically addresses the skills and training necessary for Maintenance personnel who support SIS MI. Maintenance training includes maintenance management that directs and funds the maintenance activities, the instrumentation technicians, the electricians, and the mechanics. Maintenance personnel need to have an understanding of the importance of the SIS, how they affect the performance of those systems, what skills they should have before working on SIS, and how they should identify, correct and report failures of SIS equipment.

The goal of the training program is to give the maintenance personnel the skills and knowledge needed to maintain the SIS equipment. The training program typically covers three subject areas 1) safe work practices and procedures, 2) basic skills required to be an instrumentation and electrical technician, and 3) SIS specific training. In the performance of maintenance work, consistency and quality of work execution is important in minimizing systematic failures. A procedure for all aspects of the maintenance work helps ensure that consistency. This will be the basis for the training program.

For basic skills, community colleges and private training centers offer varying training programs. There are many resources available to a user who is developing a training program, for example: ISA Certified Control Systems Technician Program, ISA-67.14.01-2000, Qualifications and Certification of Instrumentation and Control Technicians in Nuclear Facilities, and ISA-TR98.00.02-2006, Skill Standards for Control Systems Technicians.

SIS specific training focuses on the activities performed by maintenance personnel:

- understanding pass-fail criteria
- documenting as-found/as-left

- recording and reporting failure
- recognizing common cause failure
- permitting
- bypassing
- use of safety approved equipment for repair or replacement
- use of approved and standardized equipment, such as calibration equipment
- inspection and testing
- management of change, including configuration management
- preventive maintenance techniques
- troubleshooting skills

The training can be provided in many different forms, such as classroom, hands on, self-study, and computer-based training. Training can be conducted internally or externally. Classroom or computer-based training is generally not sufficient, because skill development requires exposure to the equipment and hands-on practice. Basic skills training should incorporate actual demonstration of the required tasks, such as transmitter calibration, to ensure comprehension. Documentation of maintenance training can be a challenge, especially for large sites or sites relying on contract personnel. Annex A – Example training documentation shows an example of how some users approach training documentation.

5.6 Defining management system and performance metrics

Throughout the process equipment life, numerous assumptions are made about the SIS equipment used to achieve or maintain a safe state of the process with respect to identified hazardous events. The process hazards analysis made assumptions about the initiating cause frequency and SIF risk reduction. These expectations led to a SRS where SIF functional and MI requirements were specified. The SIL verification calculations made assumptions about the failure modes and failure rates of the SIS equipment.

A health and safety executive (HSE) study found that 32% of loss-of-containment events were caused by process and safety equipment failure due to inadequate design and maintenance (HSE, 2005). Safety equipment performance is limited by the rigor, timeliness, and repeatability of MI activities. Metrics, including leading and lagging indicators, are used as a means for assessing work execution and SIS performance against requirements. When implementing metrics, always ensure that the intent of the metric is understood – the SIS is demonstrated to meet the functional and integrity requirements – rather than simply managing the metric itself.

5.6.1 Management system metrics

Most management system metrics focus on schedules, which are not indicative of work quality. A proof-test schedule can be developed with an unreasonably long interval or testing can be performed inadequately, creating an illusion where the metrics indicate a well-maintained system while equipment is failing in the field. A focus on the percentage of success or failure of various activities can lead to normalization of some failures, which is unacceptable for SIS. Any piece of failed SIS equipment represents a degradation of the risk reduction strategy. Consideration should also be given to out-of-service periods where equipment has failed and is awaiting repair or is bypassed for maintenance and testing.

5.6.2 Performance metrics

The success of the MI program is proven by its MI data, which demonstrates that the SIS can achieve the performance assumed during the process hazards analysis. Inspection, preventive maintenance and proof testing are activities used to identify deviation from acceptable operation, so that maintenance can be performed to ensure the SIS integrity. Understanding what to test

and how to judge pass/fail criteria is critical to MI program success. The proper documentation and analysis of equipment failure is necessary to ensure the assumptions in the SRS are achieved and to drive continuous improvement long-term.

Periodically the actual equipment performance should be compared to the expected performance to determine whether the SIS equipment is suitable for continued use as is or whether improvement should be initiated. Repeated SIS failures indicate that the MI program is not achieving its intent – to maintain the SIS equipment in the “as good as new” condition. There are five facets of SIF performance to monitor:

- process demands,
- detected faults,
- dangerous failures,
- spurious operation, and
- personnel conformance to work practices.

When performance gaps are identified, root cause analysis should be conducted to (1) describe what caused the identified failure, (2) determine the failure impact (3) identify the underlying reasons for the failure, (4) implement corrective actions, and 5) verify that the corrective actions addressed the cause. Consideration should then be given to changing the design, installation, operation, and maintenance practices to reduce the likelihood of failure re-occurrence. Annex B – Example demand logs provides examples of demand logs and trip reports. Annex C – Example failure reports provides examples of device failure reports.

The data necessary to perform reliability analysis can come from any of the tasks, which are part of the maintenance strategy. The most difficult part of instituting reliability improvement is the culture change necessary for data capture and classification, which must be supported by Maintenance, Testing, and Operations personnel. Training and positive re-enforcement is necessary to maintain this effort. Failure reports can be collected from across a facility or a company and used to identify patterns of failure, indicating systematic or common cause problems. One means of monitoring failures is provided by the CCPS/AIChE Process Equipment Reliability Database (PERD) initiative. This program develops and distributes failure classification taxonomies.

Table 2 — Key performance indicators (excerpted from ISA-TR84.00.04 Annex R)

The following metrics are recommended for the SIS MI program

Key performance indicator	Formula - Deliverable
Inspections: Percent SIF overdue	% KPI = 100 X (No. overdue / No. scheduled)
Inspections: Days overdue	Pareto chart listing days behind schedule - This may be used to measure currently overdue inspections or completed inspections for comparison purposes
Inspections: Percent failed	% KPI = 100 X (No. failed / No. performed)
Proof tests: Percent SIF overdue	% KPI = 100 X (No. overdue / No. scheduled)
Proof tests: Days SIF overdue	Pareto chart listing days behind schedule - This may be used to measure currently overdue proof tests or completed proof tests for comparison purposes
Proof tests: Percent SIF failed	% KPI = 100 X (No. failed / No. performed)
Corrective maintenance: Percent SIF overdue	% KPI = 100 X (No. overdue / No. scheduled)
Corrective maintenance: Days SIF overdue	Pareto chart listing days corrective maintenance behind schedule - This may be used to measure currently overdue corrective maintenance or completed corrective maintenance for comparison purposes
Corrective maintenance: Percent failed specification criteria	% KPI = 100 X (No. failed specification criteria / No. performed)
Failure to activate: Percent SIF failed	% KPI = 100 X (No. SIF failed to activate / Total no. of SIF)
Shutdowns: Percent SIF spurious	% KPI = 100 X (No. spurious SIF initiated shutdowns / Total No. of SIF systems)
SIF out of service: Total hours	Pareto chart listing hours out of service - This may be used to measure SIF currently out of service or restored out of service SIF for comparison purposes
SIF out of service: Percent	% KPI = 100 X (No. out of service hours / Total no. process hours)
SIF degraded: Percent	% KPI = 100 X (No. hours SIF degraded/ Total number of process hours)
SIF out of service: Hours beyond specified repair time	Pareto chart listing hours beyond specified repair time - This may be used to measure SIF currently beyond specified repair time or repaired SIF that had exceeded specified repair time for comparison purposes
SIF out of service: Percent beyond specified repair time	% KPI = 100 X (No. SIF beyond specified repair time / Total no. of SIF out of service during measurement interval)
SIF out of service: Percent not approved by MOC	% KPI = 100 X (No. out of service & not approved by MOC / Total out of service SIF)

5.7 Implementing configuration management and management of change

Change is inevitable and equipment occasionally needs to be replaced, repaired, or upgraded. The process facility may be expanded, leading to additional hazardous events requiring new SIF or placing new requirements on existing SIF. Process and operational changes should be reviewed through management of change to determine how these changes affect the SIS design and operating basis. The manufacturer may discontinue or obsolete SIS equipment so replacement-in-kind is no longer feasible. Planning must be put in place to ensure that necessary changes do not increase the risk of hazardous events.

No SIS equipment or program modification should be made without first carrying out a review to ensure the change does not affect the functionality of the SIF or reduce the risk reduction provided by the SIF. Validation testing should be done to ensure correct operation when the SIF or SIS equipment is changed.

For SIS, management of change includes configuration management and replacement-in-kind to ensure:

- appropriate analysis is conducted prior to change implementation,
- approval is obtained from affected parties,
- change is consistent with current practices,
- documentation is completed and consistent with field application, and
- risk is not adversely affected.

Effective management of change requires the use of administrative and physical means to prevent unauthorized or inadvertent changes. Since the SRS involved input from many disciplines, changes should be assessed and approved by similar disciplines. Such evaluation is needed for any change, other than replacement in kind, such as:

- adding new SIS equipment,
- changing functional operation of the SIF,
- changing the integrity requirements for the SIF,
- changing the materials of construction,
- changing the required speed of response,
- removing or decommissioning SIS equipment,
- changing the SIS equipment specification,
- changing the brand or model of SIS equipment,
- modifying the SIS equipment installation details,
- changing the SIS alarm or trip setpoints,
- changing SIS equipment firmware,
- changing the SIS application program, and
- modifying SIS inspection, preventive maintenance, and proof test procedures.

5.8 Performing audits to determine MI program compliance

ISA-TR84.00.04 Annex E provides guidance on developing and implementing an auditing program to ensure ANSI/ISA-84.00.01 compliance. Periodic auditing of the operating, maintenance, and engineering procedures should be performed to ensure that procedures are consistent with actual work practices, personnel are receiving training as required, training is up-to-date with latest practices, and training is comprehensive and technically appropriate.

Furthermore, it is important to verify that the training is occurring at the designated time intervals, and training records are being maintained.

Audits should follow a protocol that ensures procedures are up-to-date, personnel are familiar with the procedures, and the instructions are being followed. Auditing is generally performed at a 3-5 year interval, typically corresponding with the process safety management audit schedule. More frequent auditing may be required if there are numerous or repeated findings.

The audit should review records, information, and documentation to determine whether procedures are being adhered to. Audit findings should be addressed in a timely manner and tracked to completion. Shortcomings identified in the audit should be addressed with an action plan that establishes a schedule and assigns responsibility for correcting deficiencies to specific personnel or departments.

Audits should be performed to verify that the procedures related to SIF and, in particular, those outlined in the MI plan remain in force throughout the life of the SIF. Records of audits and their results should be documented and maintained in plant records.

6 MI activity considerations

The MI program is intended to ensure that SIS equipment is maintained in the “as good as new” condition throughout its installed life. Inspection, preventive maintenance and proof testing are activities used to identify deviation from acceptable operation, so that repair or replacement can be performed to ensure safe and reliable operation. MI activities should be covered by written procedures that specify the steps required to ensure that the activity is consistently performed and documented (see Annex D – Effective procedure writing, verification, and implementation). Procedures should include safe work practices, permitting, and notification requirements.

An effective mechanical integrity (MI) program is required to detect failure so that it can be corrected in a timely manner. Incipient and degraded conditions can be identified through inspection or diagnostics, while complete failures are often identified by proof test. The MI program also includes preventive maintenance activities. When equipment is known to have consumable components (e.g., batteries, catalytic bead sensor, etc.), preventive maintenance activities ensure that these components are replaced on a periodic basis. Inspection and automated diagnostics can identify degraded device conditions triggering maintenance. Inspection, diagnostics and preventive maintenance complement periodic proof testing, which is necessary to identify undetected failures prior to a demand being placed upon the SIF. Together, MI activities increase the likelihood that the SIF functions correctly throughout its installed life.

Without a sound MI program incorporating periodic inspection, appropriate response to diagnostics, preventive maintenance and proof testing, one runs the risk of running equipment to dangerous failure. It is essential that equipment be maintained such that it meets the functional and integrity requirements defined in the SRS. Inspection and preventive maintenance programs are necessary for achieving the equipment’s assumed performance criteria in the SIL verification calculations. The lack of a good MI program for the SIS devices, the SIF and associated utilities supporting the SIS will result in increased spurious and dangerous failure rates for the SIS.

The SIF design should consider the requirements for testing including on-line and off-line test facilities, and the SRS should identify the required test intervals for the SIS equipment. The required test time can be significantly reduced if test requirements are considered an integral part of the SIS design. Test facilities should be designed to minimize the physical modifications required for testing (e.g., jumpers or lifting wires) and the operation of test facilities should be addressed during validation planning.

Personnel should know what to inspect, test, and document and the differences between how these activities are executed for safety equipment versus non-safety equipment. Understanding how to judge pass/fail criteria and the current condition of the equipment is critical to MI program

success. Before one can define pass/fail criteria, it is necessary to understand what failures and failure modes are critical with respect to the required SIF performance. A significant activity within the MI program is the documentation of the “as-found” and “as-left” condition during the inspections and tests. This enables analysis of actual performance versus the required performance over time so that the installed integrity is periodically verified.

MI consists of many activities involving multiple departments and roles, which must be planned and coordinated throughout the facility life. This clause briefly describes those activities following a chronological sequence as practically feasible. There are some tasks that need to be performed concurrently. Management of the work process and tasks is important, as the MI activities must be reconciled with the planned and scheduled outages. Good planning and effective management of change procedures are needed to deal with the real-world needs of the operating facility, including deferred turnarounds, unplanned forces of nature, random equipment failures, etc. For the overall MI program to accomplish its mission, the personnel involved need to be sufficiently competent to successfully execute the MI activities.

This clause provides guidance related to the following MI activities:

- planning and performing inspections
- planning and performing repair
- planning and performing preventive maintenance
- planning and performing calibrations
- planning and performing proof tests
- planning and performing reliability analysis

6.1 Planning and performing inspections

The physical condition of the SIS equipment should receive a thorough mechanical inspection on a regular scheduled basis as determined by the historical performance of the installed equipment in the operating environment. This is especially true for field equipment exposed to environmental conditions and operating impact such as corrosion, process spills, leaks, etc. Inspections should be documented and any corrective action needed should be initiated immediately through site work order processes as discussed in 6.2).

As a general practice, a thorough inspection should be performed each time a proof test is performed, but this is generally not the only time an inspection is performed, since proof test intervals may extend beyond the interval required to detect and correct incipient and degraded conditions. The inspection interval should take into consideration ambient conditions such as heat, cold, salt, dust, dirt, rain, wind, insect activity and plant painting programs.

An inspection program is intended to monitor the apparent condition of equipment and its capability to operate as required to meet the SRS. An example of a condition that could limit the performance capability of SIS equipment would be corrosion build-up around the stem of a rising stem valve used to isolate a process stream. The build-up, if not identified and corrected, could prevent the valve from stroking all the way or even at all. Consequently, visual inspection should be performed periodically to verify installation quality and correctness, enhancing the integrity and reliability of the SIF.

Annex E – Example inspection items and forms provides additional examples of items to inspect associated with sensors, logic solvers, final elements, and wiring, typical problems that might be found with these items, and an inspection form. If a defect is found during the inspection it should be corrected at the time of the finding if possible. If the defect cannot be corrected immediately then a work order should be generated to repair the defect as soon as practical. The nature of the defect should be described on the inspection form.

6.2 Planning and performing repair

Repair work is performed to correct revealed faults in a timely manner. In general, this means that the repair should be done as soon as it can be scheduled and safely executed. As faults are found and corrected, the repair information should be recorded for later review as part of continuous improvement. A repair work order can be generated as a result of any of the following:

- Shift operator identifies potential problem/failure during normal daily field rounds.
- Maintenance personnel identify potential problem/failure during scheduled inspection.
- Testing or maintenance personnel identify potential problem/failure during execution of proof test.
- On-line diagnostics identifies potential problem/failure.
- Problem/failure is identified due to spurious trip.

Testing after repair should include the following activities, depending on what repair work has been completed.

1) Sensor: Exercise sensor input and verify alarm and trip setpoints are correct. Use the applicable section of the SIF test procedure and complete the required documentation for the equipment checked.
2) Final element: Exercise all outputs that actuate final control elements and observe output actions. Verify any feedback (limit switches, position indication, etc.) associated with the final control elements is functional. Use the applicable section of the SIF test procedure and complete the required documentation for the equipment checked.
3) Logic solver: The test will vary depending on the extent of the repair and its potential effect on the logic solver hardware or application program. Perform test of affected hardware, application program, or configuration to ensure proper operation and complete the required documentation.

   Upon completion of the work and any required repairs, the work order and any test documentation should be signed by the person performing the work. It should be understood that the Reliability Engineer may need to dialogue with the person who signed off the form. Repeat maintenance offenders such as repeat work orders to address performance issues should be investigated so that action can be taken to minimize failure. These actions may include recommendations to change the MI plan, such as shortening the test interval and even re-evaluating the design, specification or installation.

6.3 Planning and performing preventive maintenance

Preventive maintenance may be required to extend the useful life of the overall equipment when some part has a shorter life, such as soft goods in sealing service. The failure rate of a linkage may be quite different in the case of periodic oiling (i.e., preventive or predictive maintenance) versus no oiling (i.e., corrective maintenance). Today's SISs employ a great deal of diagnostics, which support preventive maintenance based on the observed condition of the equipment. Routine visual inspections may also initiate preventive maintenance, as those inspections can uncover incipient/degraded conditions that need to be corrected. The periodic proof test is intended to identify and to correct degradation and complete failures, but not all degradation and failures can be identified through testing alone. Thus, proof tests activities are often supplemented with thorough physical inspection and preventive maintenance tasks. As the time interval between periodic proof testing is increased, there is a need to improve the effectiveness of preventive maintenance. Refer to Annex E for more guidance on inspection and Annex G for more guidance on preventive maintenance.

Preventive maintenance is performed based on manufacturer recommendations and past experience with the equipment in similar operating environments that indicates equipment

reliability is maintained when certain items are proactively repaired or overhauled. The preventive maintenance schedule and procedure may be modified over the equipment life due to information collected during inspections, proof tests and repair work. Activities must include proper documentation and retention of preventive maintenance actions, e.g., what part needed corrective action/repair and why.

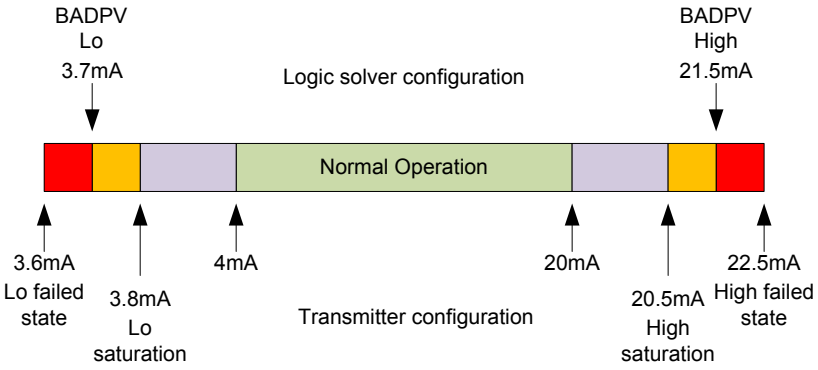
6.4 Planning and performing calibrations

All SIS equipment should be calibrated prior to placing the SIF in service. Calibration can be performed by the manufacturer or by the user in the workshop or field. Calibration test equipment traceable to a recognized standards performance organization should be used to perform a minimum three-point calibration (e.g., 5%, 50%, 95% to prevent scaling errors) over the full signal range of the loop's sensor/transmitter to the final readout device. Valves should be calibrated to proper stroke length for full open and full closed positions. Any valve that is not required to close or open to full stroke position should be calibrated at the appropriate position prior to placing in service.

Correct functionality between transmitters and the SIS logic solver is essential to effective SIF operation. Failure to ensure that this has been installed and configured correctly can lead to SIF failure in the event of a demand. The configuration of all analog transmitters should be tested to ensure that they function in accordance with how the logic solver is configured. The following items should be confirmed:

- Calibrated range of the transmitter should be the same as the range configured in the logic solver.
- Saturation HI/LO current value parameters in the transmitter should be configured to specified values.
- The BADPV HI/LO current value thresholds in the logic solver should be configured to specified values that are outside of the saturation HI/LO parameter range in the respective transmitter.
- The Fail HI/LO direction in the transmitter should be confirmed to be configured as specified.
- The Fail current value that the transmitter defaults to when a fault is detected should be configured to a value above/below the BADPV HI/LO thresholds in the logic solver.

Figure 3 depicts a suggested transmitter and logic solver analogue input configuration.



NOTE: Tx configuration parameters are NAMUR suggested values. Logic solver BADPV settings are suggested to align with NAMUR Tx configuration.

Figure 3 — Example of transmitter and logic solver analogue input configuration

An instrument calibration record should contain the following data fields at a minimum:

- tag number/identification number
- manufacturer model number
- serial number
- process location
- calibration range and tolerance
- calibration date
- test standard
- as-found/as-left
- comments
- special consideration, e.g., signal filtering, dampening, failure detection hi/low, etc.
- technician name, signature and date
- supervisor/approver name, signature, and date

Calibration procedures should be available for each type of SIS equipment (See Annex F – Example calibration forms). In general, calibration procedures recommended by the manufacturer should be followed. Where additional requirements (e.g., response time of instruments or valves) are necessary to perform the specified function, these should be taken into account in the calibration procedures.

A good practice is to include “reasonableness” checks as part of the calibration procedure. For example, on-line calibration procedures may include a step in which Operations compares the process variable readings from newly calibrated field sensors to other process measurements. Similarly, a reasonableness check for off-line calibration can be performed after the unit has been re-started. This additional step minimizes the likelihood of a systematic failure during calibration.

NOTE Common cause failure can arise when redundant sensors are calibrated at the same time by the same person using the same test equipment or standard. Where an instrument technician miscalibrates one sensor, he/she is very likely to miscalibrate the others. Special concerns for these failures arise in calibration of redundant process analyzers using a single mixed sample and in SIL 3 SISs with non-diverse process measurements.

6.5 Planning and performing proof tests

Personnel associated with the Maintenance, Operations, Design Engineering, and Process Control organizations support the planning, development and execution of proof tests. Periodic proof tests are executed to detect unrevealed failures - failures that may have existed since the last periodic test. This activity is a quality control check that verifies that the facility is operating with its intended safety integrity. Inspection and proof testing is not a substitute for preventive maintenance and repair. Detailed recording of inspection and test observations are essential for supporting failure tracking and investigation. Proof tests include checking not only the SIS functionality, but also any SIS alarms and indications (e.g., diagnostic, pre-trip, and trip alarms). Similar tests should be periodically performed on the overall system, including main processors, input/output modules, communications links, power, relays, and SIS grounding. Each test serves as an opportunity for personnel to see the SIS equipment in action and to validate the procedures associated with its operation.

Procedures should be in place to assure that all test and calibration equipment used on the SIS equipment is properly maintained, calibrated (certified per standard, if necessary), and fully operational (See Annex H – Example proof test template and procedures and Annex I – Proof test examples for various SIF technologies). Calibration cycles of test equipment should follow manufacturer recommendations and methods to assure the accuracy of the equipment. It is recommended that field test/calibration equipment be checked/calibrated against a National Institute of Standards and Technology (NIST) traceable standard on an annual basis. Calibration labs will normally provide a calibration stamp along with calibration documentation for the device being calibrated. In general, field test/calibration equipment that is found to be out of calibration, past established calibration dates, poorly maintained, or in poor physical condition should not be used on SIS systems. If a facility owns test/calibration devices, the devices should be assigned a tag name, which should be entered into the maintenance management system to ensure calibrations are performed in the recommended time frame.

Proof test procedure development should begin in the design phase so that any considerations or issues associated with the test interval or bypassing can be addressed properly. Good communications with maintenance is necessary to provide the most effective and efficient proof test procedure to guard against the need for unnecessary shutdowns or extended test deferrals.

In addition to providing a step-by-step procedure on how to test the SIF or SIS equipment against the SRS, the proof test procedure should address:

- approvals and notifications required for test execution, e.g., notification of operators
- description of the expected SIF or SIS equipment operation, as appropriate
- work scope, e.g., what will be checked, such as flow rate, valve closure, etc.
- when applicable, how tests may affect other SIF or operating systems and how to address impact
- where applicable, how the SIF or SIS equipment is affected by bypasses
- required notifications during test, such as notifying the operator when alarms are activated
- once the test is complete, how the SIF or SIS equipment is brought back on line

To support any on-line tests, operating procedures should ensure that any loss of risk reduction due to the SIF or SIS equipment being out of service is provided by compensating measures (refer to ISA-TR84.00.04 Annex P). Prior to approving bypassing or performing the test, operations should review any special precautions or compensating measures required during the bypass or test period.

- Does Operations have an equivalent process variable to monitor when the SIF process sensor is in bypass?

- Does Operations have control of a final element that can be used to shutdown the process independently during testing when the output is in bypass?
- Discuss what if a process demand occurs while in bypass? What should Operations do? What should Maintenance do?
  - Is there sufficient time for the operator to take action?
  - Is there communication with Maintenance on when to evacuate to a safe location?
- Discuss what if an operator-initiated trip is required while bypassed. What should Operations do? What should Maintenance do?

The test procedure should include return to service provisions to assure proper transfer of SIS equipment responsibility from Maintenance to Operations. The operator should confirm by process condition or equipment observation that the SIS equipment is on-line. Operations should approve work completion closing the work permit. Additional supervisory sign off may be appropriate in some cases.

6.5.1 Proof test planning

Performing proof tests can be costly if not appropriately planned. When the SIF is designed such that off-line testing is required, additional costs are incurred due to loss of production and environmental/safety impacts during the shutdown and subsequent start-up. It is therefore highly recommended that proof testing be discussed and planned for during the project design phase with input from Maintenance and Operations.

Proof testing is often accomplished through a number of discrete activities that test parts of the SIF at different times with sufficient overlap of the tests that all parts are demonstrated to function as intended. Fortunately, increased levels of automation, enhanced programming techniques, and new test techniques can be used to execute safe and comprehensive testing of individual devices or segments (e.g., input to logic solver) of the SIS while the process is running.

A periodic end-to-end test should be considered to ensure proper functioning of the entire system. Where the dynamics of the entire end-to-end SIF is crucial, the complete SIF should be tested together to ensure specification compliance, e.g., the thermowell, the thermocouple, the transmitter, the input cycle time, the logic cycle time, the output signal cycle time and all of the components required for operation of the final elements, such as volume boosters, pneumatic tubing size and length.

A key question concerns whether SIF testing must be done as an integrated test or whether various parts of the SIF can be tested at different times as necessary to achieve the SIL. Testing is performed to identify incipient/degraded conditions and equipment failure. Whether these issues are found piecemeal or through an end-to-end test is not important. Their timely detection and correction is. ANSI/ISA-84.00.01 does not specify that all proof testing must take place at the same time. It does require full validation using an end-to-end test prior to placing a new or modified SIF in service. However after that, the user is free to structure proof testing to achieve the SIL and reliability requirements for each SIF, e.g., individual SIS equipment or SIF segment tests.

Personnel and resource requirements should consider whether workshop or calibration/test lab facilities will be provided on-site, off-site, or at a manufacturer's premises, so the time required for troubleshooting, repair, and proof testing can be estimated. Tool availability and personnel competency in these tools affect how quickly MI activities can be conducted and the achievable installation quality and equipment integrity. Therefore, planning is an important activity to address both the safety requirements necessary to maintain the required SIL and to minimize the cost. Once a plan has been documented, the various activities can be scheduled.

When performing segment testing rather than end-to-end testing, it is critical to ensure that the discrete activities account for, or overlap, all interfaces. For example, SIF proof tests should cover the sensor, input wiring, input systems, communications, logic solver operation, output systems, relays (especially for voted relay outputs), output wiring, and final element, so that the operation of the entire circuit is demonstrated. Figure 4 illustrates an SIF that has been divided into 3 overlapping segments for testing. Any project or change impacting the SIS should address test requirements and the provision for competent resources to analyze discrepancies or changes.

Test plan documentation should include:

- procedures to test each SIF or SIS equipment
- descriptions of the common aspects of the SIS (e.g., PE logic solver and associated equipment) and its associated safety requirements or references to the SRS
- procedures that defines testing following on-line repair or modification
- reporting requirements

NOTE Current standards require documentation of as-found/as-left test results. This information is used to verify the assumptions used in the reliability calculations.

- who will review proof test results and records to ensure completeness and work quality
- competency requirements for persons performing the inspections, tests and repairs

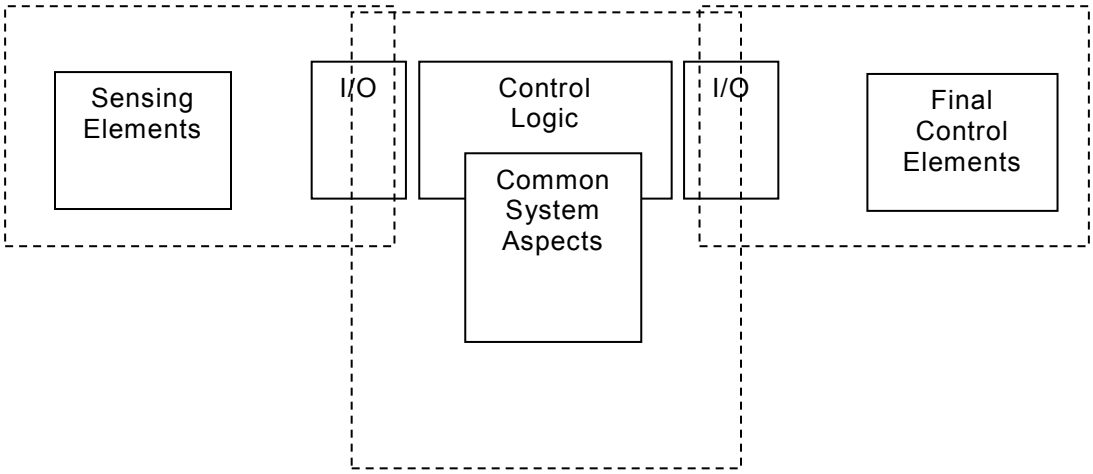


Figure 4 — Example of SIF segment tests illustrating overlapping segments

6.5.2 Test interval basis

The SRS should specify the required proof test intervals for the SIS equipment, which are necessary to support quality assurance of the MI plan. The proof test intervals for the sensors, logic solvers, and final elements may be different due to the individual device technology integrity and reliability. Some devices may be tested using manual or automated on-line testing. Others may require a plant turnaround in order to fully test the device operation. During the design phase, the planned turnaround interval should be considered to determine whether on-line testing is needed to demonstrate the required SIF performance. Follow-up testing of SIS equipment may be considered at intervals shorter than the complete proof test to improve the SIF performance. Factors that impact the frequency of these tests include:

- process severity for sensors and final elements

- accuracy of measurements required for safety
- need for positive isolation of streams by valve action
- mechanical wear and tear on equipment
- desire for longer test interval between complete proof tests

Test intervals should be documented in the facility's maintenance management system. The proof test interval can be determined using a combination of good engineering practice, manufacturer recommendations, operating history, insurance requirements, industry standards, operational constraints and the risk reduction requirements. It is always permissible to test more frequently that what is specified in the SRS. Since operational issues can affect the test window, meeting the exact test interval may be difficult at times. The MI plan should define the allowable test interval variation, including management approvals for test deferral (refer to 6.5.4 for more guidance on deferrals and approvals).

NOTE Test intervals may be impacted by unplanned repairs or replacement. If a proof test is performed and documented, consideration may be given to resetting the next test date, recognizing that the proof test interval documented in the SRS may not be exceeded.

When establishing a proof test interval basis, it is necessary to first consider how long unit operations are expected to continue between outages required to conduct off-line testing. Regulatory authorities may also require testing at intervals shorter than the planned outage schedule. These situations can have a considerable impact on the SIS design, as it may be necessary to include the ability to perform on-line testing or may require more complex architectures to achieve the needed risk reduction with a long proof test interval. Once the access and maintenance constraints are understood, the design must provide equipment in an architecture that is sufficient to achieve the required risk reduction with the specified proof test interval.

The MI plan should consider the useful life of the selected SIS equipment. The SIL verification calculations (refer to ISA-TR84.00.02) are based on the estimated dangerous failure rate during the equipment's useful life. When equipment is operated beyond its useful life, the dangerous failure rate begins to increase over time, leading the SIL verification calculation to become increasingly optimistic. Consequently, it is important to monitor the SIS at a frequency sufficient to detect when the failure rate begins to increase over time, so that the actual performance is maintained comparable to the design assumptions. Monitoring the SIS performance is required by ANSI/ISA-84.00.01-2004, 5.2.5.3. User approval as discussed in ISA-TR84.00.04 Annex L relies on prior use information to determine whether equipment is fit for service, whether in a new installation or in an existing one. The approval process acknowledges that once the equipment is installed the in-service performance may indicate the need to modify the design, specification, installation, or mechanical integrity plan to bring the SIS performance into alignment with expectations; it may also indicate the need to remove equipment from service.

With regards to useful life, there are two important considerations: 1) understanding what component/parts limit the overall equipment useful life and establishing a mechanical integrity plan to deal with those components/parts within a suitable timely basis and 2) monitoring the equipment to identify when it has reached wear-out. In many cases, consumable parts or individual parts with a known life dictate the useful life of SIS equipment. The user approval process (see ISA-TR84.00.04 Annex L) should include identifying what limits the useful life of the SIS equipment, so that consideration can be given as to whether it is feasible and cost effective to replace the consumable parts to extend the useful life or to control the conditions that accelerate degradation. Inspection or proof test intervals should not exceed the known useful life and consideration should be given to decreasing the intervals as the end of useful life approaches. To maintain the required risk reduction and to allow the desired proof test interval, it may be necessary to design the system to allow on-line replacement of the weaker parts.

The user is cautioned however that there are some instruments that exhibit a clear break between pass and fail. For instance, a capacitor in a transmitter has a specific life dependent on its materials of construction and operating environment. When it is sufficiently degraded, the instrument will not be able to perform its function(s). In the illustrated example, the user should consider the capacitor and the remaining equipment components. In most cases, a MI program designed around the equipment produces the most effective solution from both a performance and cost perspective. In the case of equipment like transmitters and solenoid valves, repair is generally not cost effective, so replacement is often performed.

6.5.3 Ensuring safe work practices

Incidents involving testing have been caused by many different factors including:

- inadequate test coordination with Operations
- inadequate return to service procedure
- inadequate communication and coordination with adjacent Operations and Maintenance who were unaware of test being conducted and the impact of testing on their situation
- SIS equipment failure
- improper bypassing
- poor test facility design
- misunderstood or incomplete test procedures
- lack of personnel competency and training

Common incidents as a result of testing include:

- beginning a test without satisfying the pre-test conditions
- attempting to start-up when a test is still in progress
- violations of lock-out/tag-out
- leaving SIS equipment bypassed (trip point, relay, timer, or valve) long-term in error
- working on the wrong device (e.g. SIF relies on redundant sensors – meant to test A, but tested B instead)
- leaving a transmitter with a simulated signal or point in manual source mode
- leaving analyzers in zero or span

To prevent these incidents from occurring, MI planning should ensure that inspection/proof test and bypass procedures are clearly documented and that personnel are adequately trained to perform their required tasks. These incidents are further reduced through job safety analysis and human reliability studies. Human factors should be considered during test facility design and procedure documentation, such as requiring that test conditions be satisfied before a test facility is enabled or that cross-checks be performed to ensure that SIS equipment is fully operational after test.

Complete testing may require the process equipment to be on-line. Safe operation must be ensured through work practices and procedure execution. Depending on site procedures, safe work practices may be covered under permitting requirements or may be addressed in the test procedures. Where permits are required, they should be listed in the procedure. Prior to any testing, a review of the tests to be conducted and the procedures for performing these tests should be carried out by persons from Instrument/Electrical Maintenance, Operations, and Technical who are familiar with the process and the SIF. This review should reinforce validating the SIF or SIS equipment against the pass-fail criteria, documenting as-found/as-left, recording and reporting failure and recognizing common cause failure.

6.5.4 Deferrals and approvals

MI programs and the designs that support them should be developed so that the potential need to extend inspection or proof testing is an exceptional event, not a matter of routine. Deferrals need to be handled using the management of change process that includes a technical review to ensure the company's risk criteria is not being violated. In the event that it is, then temporary compensating measures should be put into place until the protection is returned to the "as good as new" condition.

The most common MI deferrals are requests to delay inspections, proof tests, or repair. Common reasons for deferral are as follows:

- The equipment that the SIF is protecting is out of service. The SIF must be tested prior to the equipment being returned to service.
- A turnaround is scheduled shortly after the scheduled test of the SIF. The intent is to perform the test during the turnaround.
- Spare parts or other required resources are not currently available.
- The equipment cannot be accessed or repaired on-line.

Deferrals can be addressed by implementing a deferral procedure or through plant MOC. Annex J – Deferral considerations and example procedures provides an example of a deferral procedure. The purpose of the deferral procedure or approval process is to ensure that the risk associated with the deferral is understood and that any additional risk caused by the deferral is properly addressed. Management should be made aware of the risks involved with delay of SIS inspection, test, and repair and approve deferments on a case-by-case basis.

Probability of failure of an SIF increases as a function of time. The longer the proof test interval, the higher the average probability of failure on demand (PFDavg), potentially resulting in the SIS not achieving the risk reduction defined in the SRS. Deferring on-line or off-line tests such that the test interval is greater than the specified interval may negatively degrade the SIF performance. The approval process should examine the impact of the deferral on the SIF integrity prior to approving the deferral. Justification should consider historical performance, such as inspection, work order and proof test records, the integrity of planned compensating measures, and the SRS. The SIL verification calculation should be reviewed to determine whether the deferral will compromise the overall SIF performance.

Deferrals must be approved and authorized by competent personnel who are accountable for safe operation, understand the equipment operation, the risk the SIF is designed to reduce, and the equipment reliability history. Typically, Operations, Maintenance, and Technical representatives are involved in the approval processes. In some cases, there may be different levels of required review and approval dependent on the SIF complexity, the SIL, the potential event consequence severity that the SIF is protecting against, and the planned deferral length. An example of this is shown in Table 2.

Table 2 — Example of temporary test or inspection deferral authorization

In compliance	Unit supervisor manager	Site manager	Operating group V.P. and process safety
Less than or equal to 30 days beyond test or inspection due date	31 to 60 days beyond test or inspection due date	61 to 90 days beyond test or inspection due date	> 90 days beyond test or inspection due date.

6.5.5 Proof test strategy

Each SIF in the SIS should be identified, including its inputs, outputs, and the required logic to be performed using the inputs and outputs. A test procedure should define how each piece of SIS equipment or segment is tested. All equipment necessary for performing testing should be identified and verified suitable for tests to be performed. This includes calibration equipment with traceable performance. If any equipment is shared by multiple SIF, the proof test strategy should take this into account to guard against unnecessary testing, e.g., block valve shared among several independent SIF.

6.5.5.1 Off-line testing

The most common test of an SIF is the off-line manual proof test. This test is performed while the process being protected is not in operation thus allowing all features of the SIS equipment, SIF segment, or SIF to be validated. The primary purpose of this testing is to detect dangerous unrevealed faults that exist in the SIF. When the SIF is properly designed and maintained, this testing should rarely find faults. There are, however, multiple ways that tests can be performed. This subclause will describe techniques and procedures that are known to be effective in carrying out the proof test.

Off-line end-to-end testing of the complete SIS should be performed prior to placing the SIS in service. This is described as validation in ANSI/ISA-84.00.01-2004 and demonstrates that the SIS operates according to the SRS.

NOTE After the initial validation has been performed, subsequent tests that demonstrate the operation of the SIS equipment or SIF segments are referred to as a proof test.

SIF proof testing should be performed at intervals determined by one or more of the following criteria:

- the test interval specified in the SRS
- the test interval recommended by the equipment manufacturer
- when changes are made to logic, impacting the function of the SIF
- when the process or equipment is taken out of service for scheduled maintenance activities that require work involving SIS equipment
- company policy requiring complete SIF testing on a predefined schedule
- after extended down time of the SIS (see deferrals clause)

6.5.5.2 On-line testing

On-line testing may be necessary where the normal operating cycle of the process between scheduled shutdowns is greater than the test interval defined in the SRS. Maintaining the required SIF integrity requires that this test interval be maintained. Therefore, the testing of some SIF will require executing on-line testing.

Before performing an on-line test, it is important to ensure the process has stable operating conditions. Stable operating conditions include no major rate changes, emergency situations, process upsets, etc. On-line testing may require bypassing of the equipment to be tested. In some cases the risk of being in bypass may require presence of a field operator as the compensating measure. This will introduce stress on those performing the testing as well as any operators providing the protection. It is therefore imperative that on-line testing be performed under closely controlled and monitored conditions using procedures that have been technically reviewed and previously executed off-line. On-line testing should not be started unless it can be worked step by step to completion with no anticipated interruptions. Once the inputs or outputs are bypassed, a dedicated operator should monitor the process continuously in case there is a process demand, requiring shutdown. Once the manual bypass valves are opened or closed, a dedicated field operator should be available to close or open the block valves quickly if a process

demand occurs. During the on-line test, the operator should be capable of manually tripping the SIF via a manual shutdown switch, which initiates the SIF final elements in the event a trip is required. All personnel involved in on-line testing of SIS equipment should be aware of the procedures to follow in case a process demand occurs while the testing is in progress.

6.5.5.3 Effect of incomplete testing

An effective test will detect all hidden dangerous failures and degraded conditions. The SIF can then be restored to full operation. When effective testing occurs on schedule, the risk reduction is maintained at the desired level. As shown in Figure 5, the SIF probability of failure increases as a function of time. With complete testing at the required proof test interval, the PFDavg will continue to provide a level of performance assumed in the SIL verification.

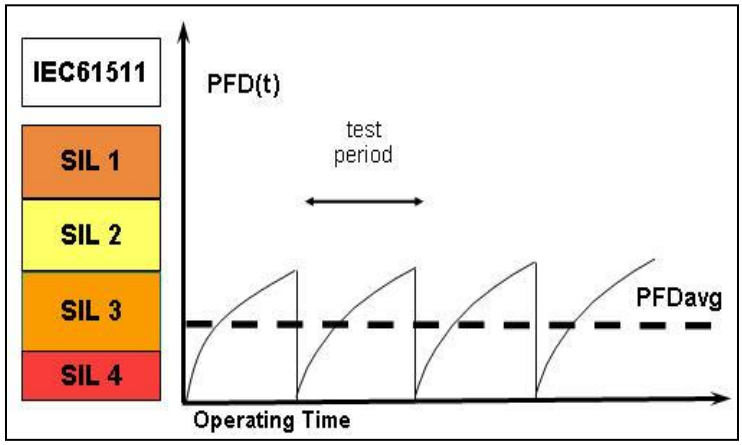


Figure 5 — Change in PFD(t) as a function of time and test interval

If the testing is not done effectively, some hidden dangerous failures will not be detected.

Figure 6 illustrates how the PFDavg will increase over time during the life of the equipment.

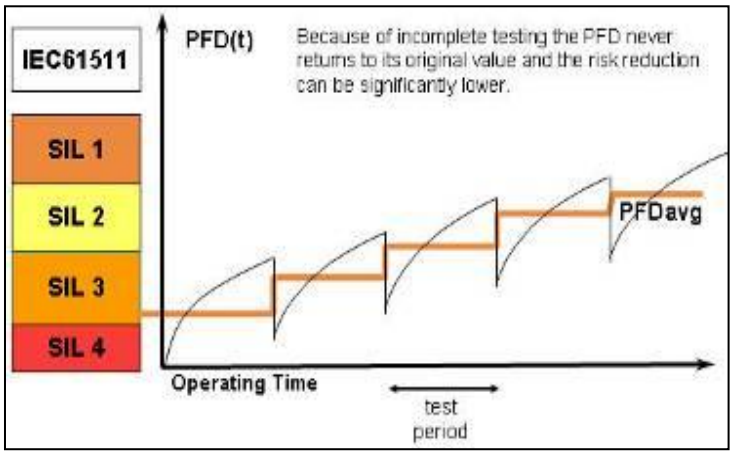


Figure 6 — Increase of PFD(t) over time due to partial testing

If testing is not completed effectively as scheduled, the SIS performance will inevitably deteriorate. If tests are also ineffective and durations between tests are increased, the PFDavg will increase as shown in Figure 7. It becomes more likely that the risk reduction needed to maintain the tolerable risk will not be provided by the SIS.

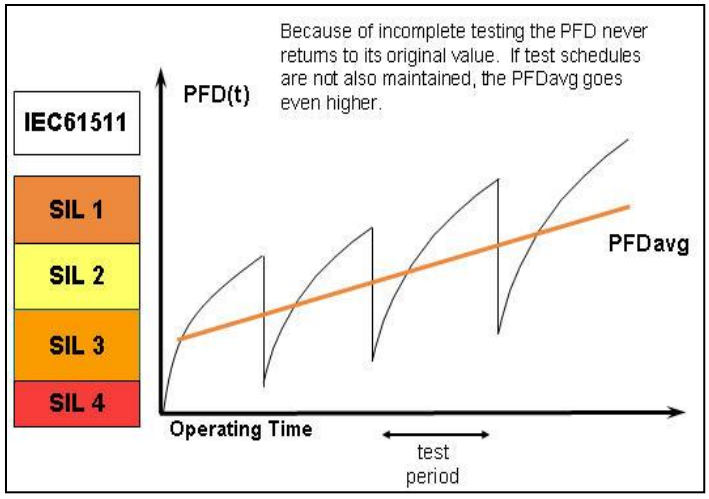


Figure 7 — Increase of PFD(t) over time due to incomplete testing

6.5.5.4 Relationship of diagnostics to proof testing

Diagnostics help to reduce the number of undetected failures that can occur by alerting the operating and maintenance personnel that repairs need to be made. In SIF, these diagnostics should vote to initiate the safety action unless redundancy is provided to ensure the required SIL is maintained. Diagnostics are used to identify specific failure modes of equipment. Diagnostics are not a replacement for proof testing. When diagnostics detect degraded or complete failure, repair or replacement occurs such that the equipment is returned to the “as good as new” condition. Unlike a proof test, the diagnostics do not inspect for incipient conditions. Although diagnostics are never a full replacement for routine inspections or proof tests, their benefits may allow greater time intervals between complete proof tests while ensuring the required risk reduction is provided.

6.5.5.5 Proof testing by demand

Trips related to process demands or manually initiated shutdowns can be treated as proof tests if adequate verification is performed and documentation similar to a proof test is created after the trip. To be considered a proof test, the following should occur:

- confirmation the demand was not caused due to failure of the component to be tested
- proper documentation
- visual inspection of equipment being tested
- confirmation of expected action of the equipment being tested
- confirmation of functional requirements of the equipment being tested
- pre-demand and post-demand status

Since the test will be reactive and unexpected, a robust system designed to track the trip and document the cause should be in place in order to take credit for the demand as a test. The required data for proper documentation also needs to be created, stored and retained. If the data is gathered manually, resources (electronic and or personnel) will be necessary during the process interruption and this should be taken into account during trip response and start-up activity planning. Before start-up, the affected SIS equipment should be visually inspected, along with any auxiliary systems, to the same rigor of a planned proof test. Automated methods of gathering the data are generally preferable because personnel are usually focused on returning the process to a normal /safe operating state after an SIF demand. Detailed analysis of the data can be performed at a later time by qualified personnel once start-up is complete.

Implementation of a system to take credit for a demand may not be appropriate for all applications based upon the test interval and testing strategy of SIF at a location. For example, if an SIF proof test interval was every three years and coincided with the plant shutdown / turnaround schedule, there would be little benefit for taking credit for a proof test of the final element if the trip occurred one year into the cycle. It may be more beneficial to design the SIF's test interval through diagnostics and a robust architecture to meet or exceed the available testing duration opportunity rather than developing a comprehensive system that can take credit for demand trips. On the other hand, if the testing strategy consisted of small segments that could be tested independently of a larger system or were needed to operate during the planned turnaround, the benefit could be greater. An example would be an individual oil well or a cooling / heating system for a vessel with inventory.

Typically, demand tests are focused on final elements, since sensor and logic solver tests can be performed on-line. However, this does not limit the potential for demonstrating a complete proof test of SIF after a demand. The most important aspect is that the demand test generates data and documentation equivalent to a planned proof test for the demand to be considered a proof test (i.e., functional requirements incorporated into the equipment proof test and associated pass/fail criteria should be demonstrated and appropriate evidence gathered during the demand).

Using the data gathered, the final element can be documented that it passed or failed the functional requirements. It is important to note that a final control element may be a part of multiple SIF and so the data should be compared to its most stringent functional requirements. Failure to pass a functional requirement should be viewed as a failed test and the proper procedures followed to restore the functionality of the device.

6.6 Planning and performing bypasses

An SIF is considered bypassed when the output is intentionally prevented from acting to achieve or maintain a safe state of the process. A bypass can occur if the signal is forced, terminal wiring is jumpered, trip settings are such that the trip will not occur, valve is clamped, or physical/logical bypasses are initiated. Start-up bypasses are sometimes required during plant start-up due to the required SIF functionality, e.g., low flow cut-off for a pump. They are sometimes necessary to allow maintenance or testing to be performed while the process is still operational, reducing downtime required for testing thus improving process reliability. However, bypassing SIF often means that the process equipment is less protected and more vulnerable to a hazardous event should a process demand occur.

Bypasses increase the potential for systematic errors. SIF in bypass are not available to operate when a process demand occurs, so bypass periods should be tracked and minimized. The use of bypasses should be reviewed and approved under a MOC process that involves procedures, administrative control, and access security provisions. Bypasses are considered acceptable, as long as their use is controlled and the risk is properly managed.

When bypasses are initiated, the bypass may result in impairment of the function or in its disablement. If the SIF is not fault tolerant, the bypass of a single device results in complete loss, or disablement, of the SIF. If the SIF is fault tolerant, a single device in bypass does not impair the SIF, but it often reduces the SIL of the SIF. For this reason, an analysis of the increased risk during bypassing should be performed so that compensating measures can be identified to address any increased risk.

If the bypass is implemented while the process is on-line, there is generally increased risk. A bypass permit system is generally used to satisfy MOC requirements and to provide traceable and auditable MOC documentation (See Annex K - Example bypass approval procedures). An assessment should be performed to identify the conditions under which the risk can be safely managed and the compensating measures that provide risk reduction equivalent to the degree of system impairment. The bypass period should be limited to what is necessary to test or repair SIS equipment.

The operator should be informed, by alarm or by procedure, when any part of an SIS is bypassed. Some companies choose to send notifications to Operations supervision as well. Bypass alarms should “ring back” functionality, where alarms are periodically repeated after shift change to ensure acknowledgement that the alarm is in bypass. Compensating measures necessary to maintain safe operation when bypasses are active should be clearly identified and documented in operating procedures.

Proof tests usually require bypassing SIS equipment. Bypass safe work practice requires the documentation of the installation and removal of each bypass. Test procedures often include the bypass permit requirements. Test procedures should specify for each bypass the approval and confirmation of:

- the activation of each bypass, force or override
- the use of each bypass, such as approval to install, tracking bypass period, maximum bypass time
- the removal of each bypass, force, or override

6.7 Defining pass/fail criteria

It is repeatedly stated in this technical report that the mechanical integrity plan seeks to maintain equipment in the “as good as new” condition, but what does that mean? Essentially, the installed equipment must function in the operating environment as intended and support the risk reduction necessary to meet the process hazards analysis requirements. The equipment is not “as good as new” when the mechanical integrity records show increasing failure or wear out. Each piece of equipment has failure modes that can be detected by observation, diagnostics or tests. These failure modes can result in degraded conditions or complete failure of the equipment. Pass/fail criteria determine when the failure mode results in the equipment not being capable of operating as needed.

MI records document the acceptability of equipment operation. The as-found condition provides evidence of the equipment operation at the initiation of the MI activities. If the as-found condition meets the pass/fail criteria, the equipment is operating as intended and the equipment is said to “pass” the inspection or test. Well defined pass/fail criteria ensures that the as-left condition supports equipment that can be considered “as good as new” when returned to service. As an example, the specified as-left tolerance for an instrument may be tighter than the pass/fail criteria applied to the as-found reading, to allow for expected drift during the operating cycle. The expectation is that as-left condition will support operation within specification until the next scheduled proof test.

6.7.1 Identifying failure modes

Failure mode is defined as the observed manner of failure. Generally this observation involves determining that some function of the equipment has been lost or that a degraded condition exists. It is most convenient to think of a failure mode as a loss of a particular function provided by the equipment. Most equipment have multiple functions, therefore most equipment have several failure modes. With respect to SIF, these failure modes may be considered safe, i.e. causes the process to be placed in a safe state, or dangerous, i.e. fails to operate when there is a process demand. Whether a specific failure mode is safe or dangerous is highly dependent upon the process and the SIS design. For instance a transmitter does not know whether high or low flow represents a hazardous condition. If the failure results in a high output on a low trip or low output on a high trip, the failure is dangerous. Conversely, if the failure results in a high output on a high trip or low output on a low trip, the failure is safe. Even with a switch contact, safe and dangerous take on different meanings for energize-to-trip and de-energize-to-trip. Where increased ventilation or fire water pumps are required, the switch failing open is dangerous.

Once the failure modes for a specific application have been determined, improvements to both safety and reliability can be gained if diagnostics coupled with appropriate architectures are properly employed. Diagnostics help to reduce the number of undetected failures that can occur by alerting the operating and maintenance personnel that repairs need to be made. It should be recognized that diagnostics are themselves acting as protection for the equipment and may also be prone to undetected failures. This propensity is dependent upon the particular diagnostic. Any time that diagnostics are being used to enhance the SIS performance, they need to be addressed and considered in the overall MI program.

An example of a complete listing of failure modes for a remote actuated valve is included in Table 3.

Table 3 — Remote actuated valve failure modes

Description	
Complete failures • Fail to closed position • Fail to open position • Fail to close on demand • Fail to open on demand • Frozen position • Valve rupture • Seal/Packing blowout **Partial Failures** • Reduced capacity • Seat leakage • External leak • External leak - Body/Bonnet • External Leak - Packing/Seal • Fugitive emission • Controlled variable high • Controlled variable low • Fail to hold position • Unstable control (hunting) • Responds too quickly • Responds too slowly • Excessive noise	**Incipient Conditions** • 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

(Excerpted from CCPS PERD Remote Actuated Valve Taxonomy)

6.7.2 Defining “as good as new”

Once facilities are commissioned and placed into operation, equipment and systems begin to wear out due to a variety of mechanisms. Like other facility equipment, SIS equipment is maintained under the MI program. For SIS, a rigorous MI program, with the subsequent reliability data collection and analysis, is necessary to ensure that the equipment is maintained in the “as good as new” condition and meets the design functionality defined in the SRS. MI procedures define the inspection, preventive maintenance and proof test activities necessary to assure the equipment integrity and to determine when equipment requires replacement or upgrade. As reliability data is captured and analyzed, inspection, preventive maintenance and proof test procedure intervals may be adjusted. Inspection and preventive maintenance should be sufficient to ensure equipment is not run to failure and to identify potential failures and to prevent dangerous failure.

6.7.3 Detecting wear out

When wear out occurs, the SIS may not provide the expected level of protection. The lifecycle assumes that equipment will be maintained in a manner that assures it remains in its useful life

where the failures occur on a random basis. Wear out can be identified by monitoring equipment at a frequency that is sufficient to detect an increase in failures over time. When the number of reported equipment failures trends upward, wear-out is a likely cause. An increased failure rate would indicate that action should be taken to repair or replace the ageing equipment; otherwise other means of protection should be implemented to address potential risk gaps. The mean time between work orders or the frequency of diagnostic alarms can also be examined. A short mean time between work orders or high diagnostic alarm rate would indicate wear out or some other failure mechanism that requires further investigation and resolution.

6.7.4 Defining as-found/as-left

Most MI personnel recognize the need to document the results of the proof tests as they move through the testing process. What is sometimes overlooked is to document the as-found/as-left conditions. The as-found condition is the initial state of the equipment prior to any corrective action or preventive maintenance activity. The as-left condition is the final state of the SIS equipment after MI activities have been completed.

As-found information is critical to understanding the actual degradation or failure rate of the equipment. For a successful test, it documents that the SIS equipment successfully achieved design intent. As a general rule, if hardware must be repaired or replaced, or settings/configuration must be changed, record the original state or value before making the change. When the as-found condition does not meet the design intent, corrective action should be taken and previous MI history should be reviewed to see if the problem has occurred previously. If so, a root cause analysis should be conducted so that changes to the design or MI plan can be identified to reduce the likelihood of re-occurrence.

The as-left condition should indicate that the equipment is in its “as good as new” condition and ready to return to service. Documenting the as-left information serves several purposes. It formally records the state that the SIS equipment was left in after testing. When the SIS equipment is being returned to service, this documentation provides a good crosscheck against the as-found information to verify that SIS equipment is operating as required.

Examples of typical forms used to document “as-found/as-left” are included in Annexes E through H.

6.7.5 MI documentation

As part of the MI program within process safety management, regulatory agencies require as-found/as-left conditions to be documented as part of any inspection or test in accordance with written procedures. The following information generally represents the minimum information required for SIF and systems:

- date of inspection or test
- name of the person who performed the inspection or test
- serial number or other identifier of the equipment on which the inspection or test was performed
- description of the inspection or test performed
- inspection / test results prior to any maintenance activity being performed whatsoever
- documentation of work performed (if any)
- test result following any maintenance activity

While required by regulatory agencies, the intent of this documentation from a lifecycle perspective is as follows:

- provide information for measuring and tracking performance (refer to ISA-TR84.00.03, 5.6)

- support prior use analysis of installed equipment (refer to ISA-TR84.00.04-1 Annex L)
- support estimation of the equipment failure rate and probability of failure on demand (refer to ISA-TR84.00.02)
- identify systematic/common cause problems that should be minimized through management system activities or taken into account in the SIL verification calculation (refer to ISA-TR84.00.02)

6.8 Developing validation plan and procedures

Process Control, Operations, Design Engineering, and Maintenance personnel are involved in developing the validation plan and procedures. SIF validation (sometimes referred to as a Site Acceptance Test “SAT”) is intended to demonstrate through inspection and functional testing that the SIF meets all aspects of the SRS as installed before starting any operation of the process equipment for production purposes. Validation provides proof that the SIS, including those utilities and diagnostics required for the system or function to perform as required meets the SRS intent, is installed in accordance with construction, installation and detailed engineering requirements, and is ready for process equipment start-up. It is generally witnessed by process control and production (or manufacturing) representatives. Although validation is often considered an inherent part of the project implementation and construction phases, this activity also provides an opportunity for facility personnel to become familiar with the operation of SIS equipment and its actions prior to the facility commencing full operation.

SIF validation can only be performed after all mechanical, electrical, instrument, SIS and supporting utilities have been installed. Validation or functional test of the SIF is performed by simulating the process and watching for the proper response of the logic solver and field equipment. The validation is a “whole loop” test using the actual field sensors, logic solvers and final elements (e.g., pressure transmitters, block valves, pumps, air supplies, etc.). It is normally performed once unless there is a fundamental change to the process design or significant modification of the SIS.

Validation completion establishes the date from which individual SIS equipment or segment proof tests are scheduled. Validation records provide the baseline for subsequent revalidations or proof tests. As such, strict adherence to the testing protocols with appropriate supervision and signature approval to confirm complete and ready to operate. Any deviations need to be managed according to a validation plan.

6.8.1 Validation plan development

A successful SIF validation is a culmination of many related steps throughout a project process. A validation plan ensures these steps are completed as required. The validation plan should identify the related steps and step execution timing, outlining the required resources, the expected level of involvement of each participant, the protocol to be followed during the inspection or test, the order in which the SIS or SIF segments are to be tested, and the scope of each test. The plan should also define how and to whom failures should be reported, as well as how they will be resolved. Annex L – Example validation plan provides an example of a validation plan.

To support any validation plan development, it is necessary to have the safety requirement specification and detailed design information, including but not limited to:

- instrument specification sheets,
- logic flow diagrams or Boolean drawings for application program testing,
- cause and effect matrices and loop drawings for maintenance troubleshooting, and
- SIF I/O and set point list.

This information should be consistent and accurate, and one set of documentation should be considered as master for validation execution.

It is also necessary to have inspection procedures, test procedures and pass fail criteria documented for each activity. Annexes E through I give specific examples for each activity.

When planning site validation, it is essential that the discrete activities do not undo previous work. A test should not be negated by subsequent alterations due to construction, commissioning or other activities that follow completion of the test. Field clean-up of deficiencies found during the commissioning / loop check phase should be repaired prior to start of validation. This reduces the potential for unforeseen delays during the validation execution.

6.9 Developing Factory Acceptance Test (FAT), commissioning, and Site Acceptance Test (SAT) procedures

Engineering, Construction, and Maintenance personnel have significant roles and responsibilities in executing the FAT, commissioning the SIS, and conducting validation (SAT). These activities should be conducted in a logical and organized manner to minimize the probability of human error or equipment damage and to ensure rigorous testing and validation is completed.

6.9.1 Factory Acceptance Test

An FAT is not required by IEC 61511-1 Clause 13, which is the only informative clause in Part 1. The FAT may be conducted for any portion of an SIF or on the entire SIS and it may rely on simulated inputs uses switches and analog dials or simulation software. The user may elect to only perform the Site Acceptance Test. In general, FATs are conducted on vendor-packaged systems, hardwired panels, and PE logic solvers. An FAT is routinely performed for programmable electronic (PE) systems, where it may involve an integrated test of the SIS logic solver and the BPCS. The FAT verifies the ability of the BPCS to communicate with the SIS logic solver, its communication security, and its ability to meet the SRS. Additionally, PE hardware, firmware, and application program may be tested before installation and commissioning in the field.

An FAT is a test performed in a controlled setting, usually at the manufacturer, integrator, or engineering contractor location. The FAT is a series of tests performed by the system supplier, as required by the customer, to ensure the system meets design specifications and was built with the required integrity. The FAT verifies that the supplier is providing SIS equipment that function according to the SRS, the application program specification where applicable, and other contracted documents. During the FAT, the owner/operator is generally an observer.

Some manufacturers and users may wish to break the FAT into phases or distinct tests performed at different times. Some typical FAT phases are:

1) Hardware Factory Acceptance Test (HWFAT) is the test of SIS equipment, panels, I/O, power supplies, panel grounding and related equipment at the supplier's facility to ensure that the SIS equipment has been installed and wired according to specification and that there are no faulty devices. Also fault injection testing on the hardware can be performed at this time to ensure proper operation with respect to redundancy and safe failure modes. Depending on system architecture and capabilities, the final software configuration may or may not need to be configured in the logic solver. The advantage of doing this type of test is for systems that are capable of testing the hardware and software independently of each other. The hardware can be tested earlier in the project lifecycle and delivered to the field earlier to potentially shorten the construction schedule. This concept is not unique to SIS and can also pertain to the BPCS.
2) Application Program Factory Acceptance Test (APFAT) is the formal testing of the configuration in the SIS to ensure that it conforms to the SRS, cause and effect or logic narrative. Trips, resets, alarms, bypasses as well as graphics and all modes of operation are

tested. Fault injection testing, voter degradation and other items described in the SRS are tested. This may be done using physical devices to simulate field I/O or software simulation techniques depending on the capabilities of the system. The advantage of this type of test is that it allows for the application program configuration to be independent of the project hardware and can typically be later in the project lifecycle allowing for more complete definition. This concept is not unique to SIS and can also pertain to the BPCS.

3) Integrated Factory Acceptance Test (IFAT) is the formal testing of the SIS and BPCS simultaneously so that combined actions result in the desired safe automation of the process facility. This test may or may not require all or part of the SIS and BPCS hardware to be present depending on system(s) capability. A SIS may have secondary non-safety actions or trips performed in the BPCS to aid Operations in restarting the unit after a trip. For example a typical action maybe putting a control loop in manual and moving the control valve to the safe state upon the trip of an SIF. Another example would be ensuring the BPCS cannot move its control valve when the SIS has final control of the device. This test is performed prior to the configuration being installed in the field. The advantage of this type of testing is to expedite field commissioning by minimizing configuration errors.

The above FAT phases are typically conducted wherever there are more resources available to rigorously test and correct operational issues if needed. Performing the work at the factory generally provides an economic benefit to the project in terms of scheduling and less rework in the field, which is more costly. The four (4) main objectives of the FAT are stated in Table 4. Each objective is further divided into specific goals that should be considered in developing the FAT procedure.

Table 4 — FAT objectives and associated goals

OBJECTIVES	GOALS			
	Goal-1	Goal-2	Goal-3	Goal-4
(1) Supplier site hardware and system checkout sometimes referred to as the HWFAT	Verify supplier tests were completed. Test and verify all SIS equipment/ components before field installation. Establish a basis in case problems/ defects show up in field.	Minimize product defects and manufacturing errors.	Reduce start-up and commissioning time.	Ensure system will perform its safety shutdown functions on demand. Reduce start-up and commissioning time.
(2) SIS configuration checkout sometimes referred to as the SWFAT	Test and verify all design and SIS configuration work before field start-up/commissioning.	Ensure that Engineering Support and Operations personnel agree that the SIS configuration meets the application requirements.	Reduce start-up and commissioning time.	Reduce start-up and commissioning time.
(3) "Open" SIS sometimes referred to as the IFAT	Prove that there are no compatibility issues with the integration of the SIS with non-SIS supplier-specific hardware or application programs.	Test the performance of the SIS and all non-SIS supplier-specific hardware and application programs in their control environment.	Test and verify all SIS equipment/ components before field installation. Establish a basis in case problems/ defects show up in field	
(4) Training	Train operating and support personnel before field installation.	Training key operating personnel before start-up and commissioning.	Reduce start-up and commissioning time.	

The tests listed below can be a specific sub-set of the supplier's standard tests. These tests are not intended to eliminate any of the supplier's standard tests, but to specifically highlight typical tests conducted as part of an FAT.

- inventory the hardware items in the system, point out any discrepancies at the start of staging, and find out when these items will arrive. The FAT should only be conducted if a fully functional system can be tested. Verify all the items purchased function properly including each type of I/O card, HMI equipment, and other items such as printers. After the FAT is successfully completed and accepted, the owner/operator periodically performs hardware and application program testing.
- physically inspect the hardware. Inventory and system layout must be checked based on the specification. The I/O wiring and layout should be checked. The HMI and related system hardware integration should also be inspected.
- validate communications through the various levels of the SIS to the HMI. The following need to be checked for integrity:
  - internal logic solver communication
  - I/O module to logic solver communication
  - intra-module communication network
  - logic solver network to HMI network server communications

  - HMI network communications (such as Ethernet)
  - printers
  - modems
- when a historian is included in the scope, communication to historical data logger needs to be confirmed, as well as proper communication with redundancy failure for any of the above communication protocols that are implemented with redundancy.
- proper operation of power supplies should be validated as well as the distribution wiring. The following needs to be checked for integrity:
  - module power supply
  - I/O power supply
  - proper I/O card failure
  - proper control card failure
  - logic solver battery power backup
  - I/O module redundancy
  - SIS grounding integrity
- for an instrumented system that has segregated safety layers, it is necessary to inspect, test out, and verify that module power and I/O power are installed in accordance with the requirements as documented in the equipment safety manual.
- for I/O power supply that does not have a built-in system alarm on loss of power, confirm external signal wiring (e.g., as 24 VDC discrete input or voltage input) into the control system and verify the alarm.
- perform an SIS hardware and operating system software check versus SRS to the extent necessary to prove correct functionality. I/O channels need to be tested with proper simulation panels and equipment. The I/O test needs to be conducted with signal generators and original termination units in place.
- special attention needs to be given to observing and recording events or discrepancies in the area of system reliability and designed redundancy functions. If any system component failure does not generate automatic-failure-reporting to the operator, it needs to be recorded and resolved with the assistance from the supplier. If proper "fail-over" to the backup component does not occur automatically within a designed redundancy, a discrepancy report with proper punch listing needs to be documented for a root-cause analysis and final resolution.
- proper operation of the HMI and Engineering Work Station (EWS) needs to be confirmed. The EWS is defined as the main configuration station that has application program & I/O configuration capability. Occasionally, the EWS also has HMI console capability.
- Site Integration Test (SIT) is the formal testing of the ability of the SIS and BPCS to be able to properly communicate with each other once those systems have been installed in the field. It also can include any third party systems that need to interface with the BPCS.

6.9.2 Installation and commissioning

After the SIS equipment is delivered to the site and has been installed, it needs to undergo the appropriate inspection and commissioning processes before validation (or Site Acceptance Test) can be completed. Figure 8 provides an illustration of the conceptual work process.

Typically, physical inspection is the first task to be performed once an instrument is turned over from construction. Physical inspections need to be documented to provide evidence of what was checked and whether the device passed or failed. It is recommended that field inspection reports be filled out for every piece of instrumentation. Failed equipment needs to be repaired or replaced before proceeding to commissioning. Physical inspections need to be performed prior to

commissioning as improper physical installation may require removal or alteration of the instrument and therefore would require “re-commissioning” the instrument. In some cases, physical inspections may be performed on skidded equipment while still at the supplier's site if appropriate. Physical inspections done at supplier sites should be spot checked once permanently installed at site to ensure no damage was done during transportation.

Commissioning is intended to ensure the wiring is landed on the proper termination point and to verify the overall integrity of the loop from field device, through I/O modules, logic solver, and to the HMI operator console displays as well as the final elements. Commissioning activities include:

- all hardware properly installed according to manufacturer's requirements
- check of all installed hardware according to system drawings
- proper installation of computers/workstations
- check of all diagnostic systems statistics
- routing of cables and wires verified for proper AC/DC segregation
- ensuring all cables and wires are properly supported
- ensuring all cable connectors are secure and relieved of stress
- ensure wiring is landed on the proper termination and verify overall wiring loop integrity for all field instrumentation
- verify proper crimping and perform a tightness check
- verify proper instrument range by use of a calibration check (field check)
- verify proper labeling and identification as SIS equipment
- verify engineering units, tag name, and diagnostics, etc. of each instrument according to specification
- verify SIS input range is in agreement with field instrumentation and specification
- verify and confirm proper operation of the instruments, sensors and final elements according to supplier and specifications
- verify proper installation of air supplies
- verify proper grounding by visual inspection and perform grounding test
- verify proper freeze protection
- verification that HMI system network topology is installed according to design drawings
- verification of security settings for field and SIS devices (e.g., password protection or jumpers)

The emergency back-up power (e.g., uninterruptible power supply (UPS), battery banks, auxiliary generation, transfer switch, etc.) should be fully tested to provide:

- adequate bumpless power to all appropriate devices
- prevent loss of critical data parameter
- retain SIS application program
- provide adequate time for the operating personnel to place the facility in a safe mode in case of extended power interruptions

UPS circuit labeling should be checked for correctness as to not place any undue load from non-critical devices being plugged into UPS outlets.

Backup generator systems should be tested to work in conjunction with the UPS system to provide adequate power coverage.

All backup power systems should be verified to provide appropriate alarms and diagnostics. The interfaces between the SIS and the back-up power systems needs to be functionality checked to the greatest extent possible. Functionality tests should be initiated at the back-up power system while observing proper operation of the SIS. It is not acceptable to lift interface wires. The goal is to test the system as a whole to the greatest extent possible.

The piping and instrumentation diagrams (P&ID's) or cable/instrument schedules can be used as a record of equipment checked. Proper documentation of commissioning should be stored on a loop-by-loop basis and become a permanent record at the site.

6.9.3 Validation completion (Site Acceptance Test)

Validation can be completed once the SIS equipment installation, inspection and commissioning is confirmed. Validation is sometimes referred to as the Site Acceptance Test (SAT). Validation demonstrates that all installed SIS equipment fully meets the SRS. In executing validation, emphasis should be on completing the functional testing of each SIF to demonstrate its operation according to the SRS, not on correcting deficiencies. It is expected that most, if not all, deficiencies have been identified during earlier verification activities, such as the FAT, field equipment installation, inspection, commissioning and loop checks. If these earlier verification activities are thoroughly performed, validation should progress smoothly and on schedule.

When the scope of functional testing of each SIF is determined for inclusion in the Validation, consideration should be given to logical testing already performed during the FAT. Each SIF should be proven to be functional regardless of the FAT, however extensive testing of all possible combinations of voting conditions that can activate a SIF may not be necessary as part of the Validation if there is good documentation in place that records the testing results of the relevant logical configurations during the FAT **AND** effective MOC of the logic solver configuration can be demonstrated from the time that the FAT was completed.

The overall project plan should include the SIS design and construction activities impacting on-site validation requirements. These activities include:

- Factory Acceptance Test
- SIS equipment installation and commissioning

Various aspects of the SIS should be tested and confirmed as a part of validation, including but not limited to the following:

- set points and ranges,
- status of sensors and final elements,
- operator interface,
- diagnostic indications, such as out of bounds, deviation, or not in commanded state,
- indication of any automated logic changes, such as voting degradation or fault handling,
- indication of where the process is in its sequence, if applicable,
- indication that an SIF has taken action,
- indication of SIF bypass,
- operation of manual shutdown facilities,
- operation of resets,
- indication of SIS support system loss,
- failure of environmental conditioning equipment, which supports the SIS,

- response time, and
- criticality requirements, such as valve shutoff tightness and closure speed.

All auxiliary systems associated with the SIS need to be checked with the appropriate rigor and thoroughness. Examples of auxiliary systems are:

- controls or control systems external to the main SIS
- Foreign Device Interfaces between the SIS and an external party
- stand alone historian data collecting devices
- billing systems either internal to the logic solver or external systems
- callout systems for unmanned plants
- remote access
- remote control

The interfaces between the SIS and the auxiliary systems must be proof tested to the greatest extent possible. Proof tests should be initiated at the auxiliary system while observing proper operation of auxiliary system and the SIS inputs and responses. It is not acceptable to lift interface wires. The goal is to test the system as a whole to the greatest extent possible.

Testing should be performed to ensure design intent of the auxiliary system failure modes and the failure modes of the interface signals to the SIS. Normally these auxiliary systems and interfaces are designed fail safe. Testing for fail safe functionality may include loss of power, loss of instrument air, loss of communications, loss of interface wiring, etc.

The outcome of a successful validation provides an auditable documentation trail, which proves that the designed and constructed SIS operates according to the SRS and equipment specification. Discrepancies identified during validation should be corrected and tracked to completion. Documentation should incorporate signoff sheets identifying the personnel who conducted tests or served as verifiers for various work activities.

When the SIS is approved for service, site safety, permitting, and facility management of change procedures for in-service systems will apply. Validation approval indicates that necessary parties agree that the SIS operates as required in the operating environment and is ready for the process unit startup. Documentation should include a formal notice of turnover to the site management.

Note that completion of the SIS validation does not approve the SIS for handover to Operations on its own. A Stage 3 Functional Safety Assessment and a Pre-Startup Safety Review are required to be completed prior to handover.

Table 5 — Validation roles and responsibilities

The following roles and responsibilities relating to SIS validation are listed as a recommendation for its completion.

SIS Specialist/Engineer	
Responsibility	**Qualifications**
Overall responsibility for planning and executing the SIS validation and ensuring that it is completed with appropriate documented results.	Sufficient experience and training in working on SIS related projects/equipment. Possesses a detailed understanding of ANSI/ISA-84.00.01-2004 (IEC 61511 MOD).
Construction or Maintenance Supervision/Technician	
Responsibility	**Qualifications**
Represent the owner of the SIS in confirming that all validation activities are effectively carried out.	Sufficient experience and training in working on SIS related projects/equipment. Possesses a working understanding of ANSI/ISA-84.00.01-2004 (IEC 61511 MOD).
Independent Reviewer	
Responsibility	**Qualifications**
Performing a peer review along with the SIS engineer to make a general judgment that the validation plan is appropriate, and that evidence of completion that is provided is sufficient.	Sufficient experience and training in working in a related job role (Instrumentation, Process, and Process Safety Management). Possesses an awareness of ANSI/ISA-84.00.01-2004 (IEC 61511 MOD). Independent of the project team and should have had no involvement in its execution.
Management Team Representative	
Responsibility	**Qualifications**
Approval of the individuals that will be performing the above three roles as they relate to this specific project. This approval is to confirm that these individuals have sufficient experience and professional standing in order to undertake these responsibilities.	Sufficient experience in the industry. Possesses a basic awareness of ANSI/ISA-84.00.01-2004 (IEC 61511 MOD).

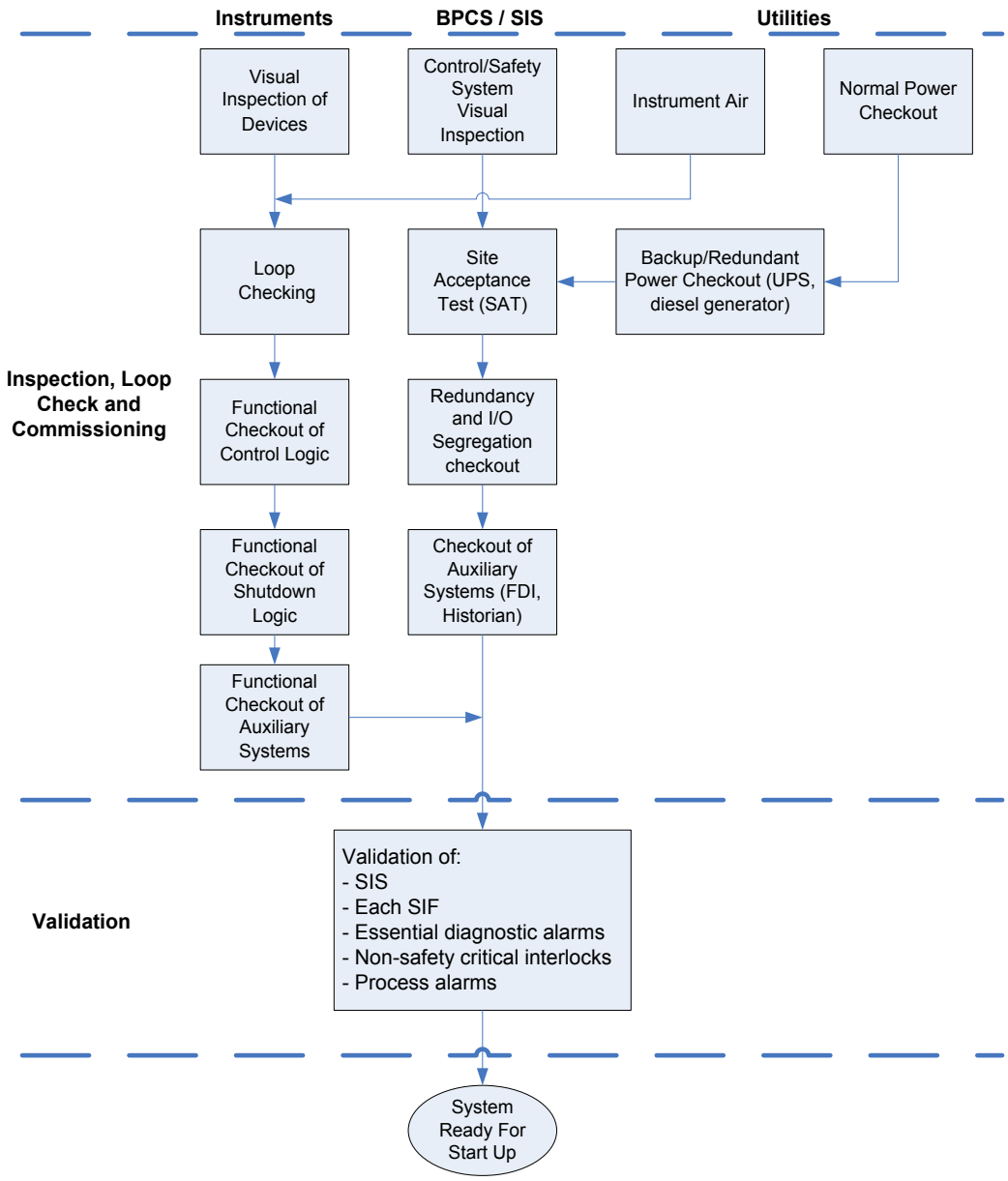


Figure 8 — Validation flowchart

Functional Safety Assessment Stage 3 Prior to Start Up

7 References

Health and Safety Executive, Findings from Voluntary Reporting of Loss of Containment Incidents 2004/2005, Hazardous Installations Directorate, Chemical Industries Division, St Anne's House, Bootle, UK, 2005.

ANSI/FCI 70-2-2006, Control Valve Seat Leakage.

ANSI/ISA-84.00.01-2004 (IEC 61511 Modified), Functional Safety: Safety Instrumented Systems for the Process Industry Sector, www.isa.org.

API 598, Valve Inspection and Testing, Ninth Edition, American Petroleum Institute, 2009 Edition.

CCPS – Process Equipment Reliability Database (PERD), American Institute of Chemical Engineers, Center for Chemical Process Safety.

IEC 60534-4, Industrial Process Control Valves Part 4: Inspection and Routine Testing.

ANSI/ISA-84.91.01-2012, Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry, Research Triangle Park, NC. www.isa.org

ISA-TR84.00.02-2002, Parts 1-5, Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Package, www.isa.org.

ISA-TR84.00.03-2002, Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS), www.isa.org

ISA-TR84.00.04-2011, Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Modified), Research Triangle Park, NC (2006). www.isa.org

NAMUR Ne43 Standardization of the Signal Level for the Breakdown Information of Digital Transmitters.

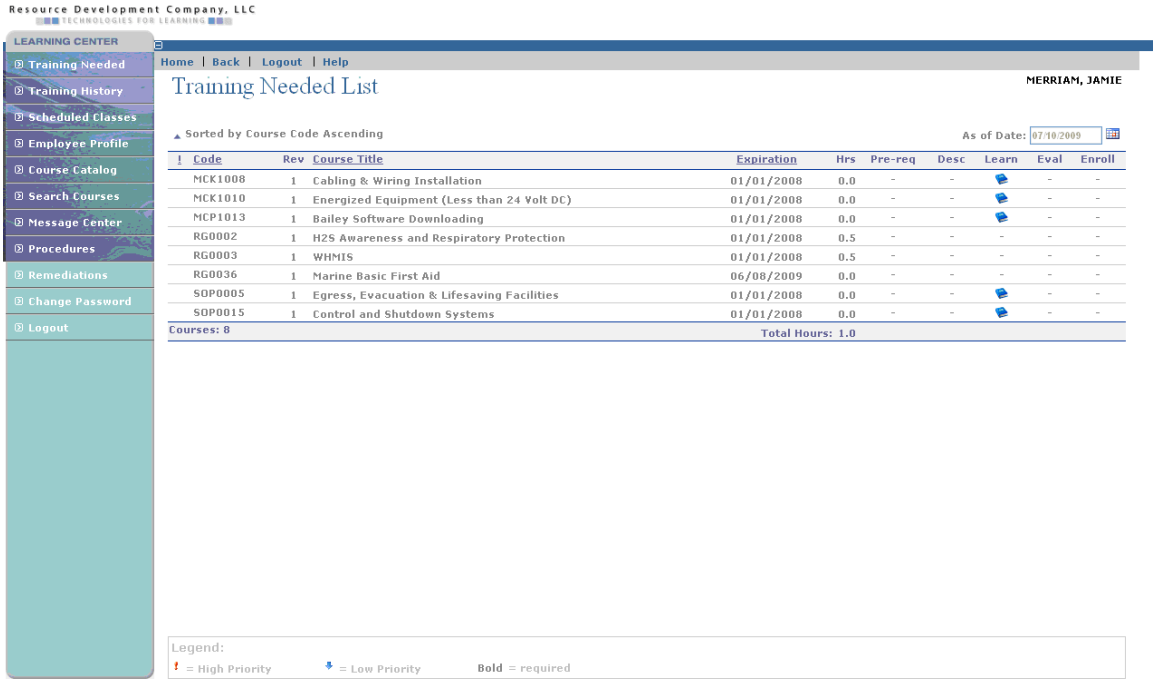
NFPA 86, Ovens and Furnaces, National Fire Protection Association, 2003 Edition.

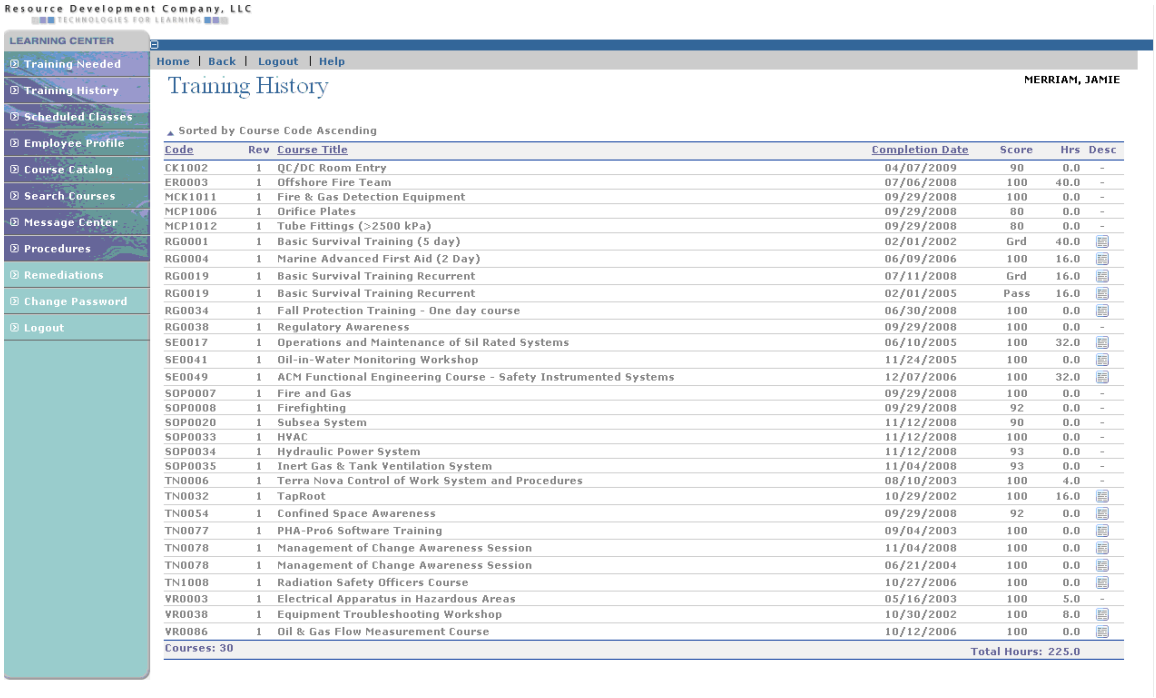
NFPA 70e, Standard for Electrical Safety in The Workplace, National Fire Protection Association, 2012 Edition.

Annex A — Example training documentation

SIS related training should be part of an individual's comprehensive training plan and should be tracked through an operating facilities training documentation and management system as shown in Figure A.1 below. The first document shows how one company documents the training in an electronic database to track the training of each individual. The second example shows a checklist used for performing and documenting the training. The checklist identifies the training required and as the trainee completes the training a trainer will sign off that the tasks have been completed.

Form A.1





Resource Development Company, LLC
TECHNOLOGIES FOR LEARNING

LEARNING CENTER

- Training Needed
- Training History
- Scheduled Classes
- Employee Profile
- Course Catalog
- Search Courses
- Message Center
- Procedures
- Remediations
- Change Password
- Logout

Home | Back | Logout | Help

Training History

MERRIAM, JAMIE

Sorted by Course Code Ascending

Code	Rev	Course Title	Completion Date	Score	Hrs	Desc
CK1002	1	QC/DC Room Entry	04/07/2009	90	0.0	-
ER0003	1	Offshore Fire Team	07/06/2008	100	40.0	-
MCK1011	1	Fire & Gas Detection Equipment	09/29/2008	100	0.0	-
MCP1006	1	Orifice Plates	09/29/2008	80	0.0	-
MCP1012	1	Tube Fittings (>2500 kPa)	09/29/2008	80	0.0	-
RG0001	1	Basic Survival Training (5 day)	02/01/2002	Grd	40.0	
RG0004	1	Marine Advanced First Aid (2 Day)	06/09/2006	100	16.0	
RG0019	1	Basic Survival Training Recurrent	07/11/2008	Grd	16.0	
RG0019	1	Basic Survival Training Recurrent	02/01/2005	Pass	16.0	
RG0034	1	Fall Protection Training - One day course	06/30/2008	100	0.0	
RG0038	1	Regulatory Awareness	09/29/2008	100	0.0	-
SE0017	1	Operations and Maintenance of Sil Rated Systems	06/10/2005	100	32.0	
SE0041	1	Oil-in-Water Monitoring Workshop	11/24/2005	100	0.0	
SE0049	1	ACM Functional Engineering Course - Safety Instrumented Systems	12/07/2006	100	32.0	
SOP0007	1	Fire and Gas	09/29/2008	100	0.0	-
SOP0008	1	Firefighting	09/29/2008	92	0.0	-
SOP0020	1	Subsea System	11/12/2008	90	0.0	-
SOP0033	1	HVAC	11/12/2008	100	0.0	-
SOP0034	1	Hydraulic Power System	11/12/2008	93	0.0	-
SOP0035	1	Inert Gas & Tank Ventilation System	11/04/2008	93	0.0	-
TN0006	1	Terra Nova Control of Work System and Procedures	08/10/2003	100	4.0	-
TN0032	1	TapRoot	10/29/2002	100	16.0	
TN0054	1	Confined Space Awareness	09/29/2008	92	0.0	
TN0077	1	PHA-Pro6 Software Training	09/04/2003	100	0.0	
TN0078	1	Management of Change Awareness Session	11/04/2008	100	0.0	
TN0078	1	Management of Change Awareness Session	06/21/2004	100	0.0	
TN1008	1	Radiation Safety Officers Course	10/27/2006	100	0.0	
YR0003	1	Electrical Apparatus in Hazardous Areas	05/16/2003	100	5.0	-
YR0038	1	Equipment Troubleshooting Workshop	10/30/2002	100	8.0	
YR0086	1	Oil & Gas Flow Measurement Course	10/12/2006	100	0.0	

Courses: 30 Total Hours: 225.0

Form A.2 — Training documentation and process

The following NOTES apply to all tasks.

1. Circling perform or simulate [P, S] must indicate method of accomplishment for each skills demonstration. Skill demonstrations that are provided with a [P] only must be performed.

2. Initiating of task certifies the person for INDEPENDENT operation.

3. Person initiating the successful completion of the knowledge requirements must be a qualified craft technician, supervisor or other knowledgeable personnel.

TASK #	TASK STATEMENT	REFERENCE	(P/S)	INIT
TASK 1	**DRAW** the following instrument symbols : a) Pneumatic signal lines b) Electrical/electronic signal lines c) Control room mounted instrument/field mounted instrument		P/S	
TASK 2	**DRAW** a closed loop flow control system naming the components and showing proper symbols for each component		P/S	
TASK 3	**CALIBRATE** a pneumatic controller that has proportional plus reset action		P/S	
TASK 4	**CALIBRATE** a magnetic flow transmitter		P/S	
TASK 5	**CALIBRATE/ADJUST/REPAIR** a Varec		P/S	
TASK 6	**CALIBRATE/ADJUST/REPAIR** an interface level		P/S	
TASK 7	**CALIBRATE/ADJUST/REPAIR** a level transmitter loop		P/S	
TASK 8	**CALIBRATE** a **SMART** transmitter		P/S	
TASK 9	**PERFORM** the following to the SIS PLC system: **EXPLAIN** the purpose **STATE** the inputs and outputs of the SIS PLC system • Using the PLC operating instructions, ACCESS data in PLC to determine the source of a problem • **IDENTIFY and REPLACE** failed board • **COPY** error codes and fault details to diskette **PERFORM** functional checkout		P/S	
TASK 10	**CALIBRATE** the following transmitters: • Differential pressure • Pressure		P/S	
TASK 11	**PERFORM** an SIS bypass		P/S	
TASK 12	**COMPLETE** bypass authorization form • **EXPLAIN** the different level for bypass approvals • **STATE** location of an active SIS bypass form • **STATE** the location of a completed (inactive) bypass form • Using corporate SIS document as a reference, **STATE** the acceptable reasons for bypassing an SIS		P/S	

TASK 13	**PERFORM the following SIS valve performance tests** TIMING TEST BUBBLE TEST FUNCTIONAL TEST (what is the content of this test?) EXPLAIN the purpose of each of the above test STATE the location of the test sheets Using a test sheet, EXPLAIN the performance parameters for the respective test		P/S	

1st Attempt ☐ **2nd Attempt** ☐ **3rd Attempt** ☐

_____ / _____

Evaluator **Date**

Trainee has successfully completed all performance evaluation requirements, and is approved to perform this task INDEPENDENTLY.

_____ / _____

Trainee **Date**

Annex B — Example demand logs

A demand occurs when a process deviation results in the need for the SIS to take action to achieve or maintain a safe state. Demands should be recorded and tracked so that their frequency can be compared to the assumptions in the process hazards analysis. Repeated demands often indicate a reliability problem with SIS or operating procedures. Repeated demands should be investigated and actions taken to reduce the frequency where possible. This annex provides examples of demand logs. Users may develop other log sheets or reports incorporating similar information or use other forms of documentation to record and track demands.

Form B.1 — Demand log

Facility _____
Plant _____
SIF ID # (e.g., loop number or description) _____
Demand start date: _____ Start time: _____
Demand end date: _____ End time: _____
SIS type involved: (Circle applicable type)
Shutdown – Go to (1)
Permissive – Go to (2)
Auto-Start – Go to (3)

1) Shutdown info							
Did shutdown function?	Yes	No	(Circle one)				
Did process variable reach or exceed setpoint?				Yes	No	(Circle one)	
Comments:							
2) Permissive info							
Did permissive function correctly?	Yes	No	(Circle one)				
If no, circle one of the following: Permissive failed to prevent unsafe state Permissive spuriously initiated action							
Comments:							
3) Auto-start info							
Was system supposed to start?	Yes	No		(Circle one)			
Did system start?	Yes	No		(Circle one)			
Did system start on first attempt?	Yes	No	N/A	(Circle one)			
Did system start within defined time criteria?				Yes	No	N/A	(Circle one)
Comments:							

Form B.2 — Demand log

Distribution list:
SIS Specialist:
Operations Manager:

Operator	Date and Time of Event	Instrument Loop Number(s)	Service	Process Area Sub-Area	Batch No	Initiating Event	Comments

Example

Operator	Date and Time of Event	Instrument Loop Number(s)	Service	Process Area Sub-Area	Batch No	Initiating Event	Comments
John Doe	8/21/2007 14:08	206LSLL and 207LSLL	Boiler #1 Steam Drum Low Level Switches	Power House Boiler #1	N/A	While swapping boiler #1 to boiler #2 operator lined up the wrong blowdown valve which dropped the level in boiler #1 causing trip	See Data Historian and SOE Log for 8/21/2007

Form B.3 — Trip investigation report

Distribution list:
SIS Specialist:
Operations Manager:

SIF tag number or loop ID:	Plant ID:
SIF description: (If there is a documented SRS provide document reference)	
☐ Process demand ☐ Spurious trip (Was there a process excursion or was it a spurious SIF failure?)	Date/Time:
Classification: _____Safety _____Environmental _____ Asset Protection	
Trip caused by: Check all that apply ☐ Process upset ☐ Wind ☐ Control failure ☐ Ground movement ☐ Operator error ☐ Loss of containment detection ☐ Equipment failure ☐ Fire ☐ Lightning ☐ Explosion (What caused the process to shutdown or to be interrupted?)	
Did all of the SIS equipment operate as designed? ☐ yes ☐ no If no, fill out a failure report for any equipment that did not function properly.	
Plant restart Date/Time	
Estimate cost of the trip based on business interruption or lost production: Estimate equipment damage costs:	
If trip was due to failed equipment, has a failure report been completed? ☐ yes ☐ no	
Considering the impact of the trip, are there any recommendations to prevent future occurrence?	
Information used in analysis: (Attach DCS trends, alarm journals, first out, sequence of events logs, manufacturer failure reports)	
Comments:	
Assessment led by: Date: (Process Automation/Control System Engineer)	

The form shows how the individual demand reports in B.1 through B.3 can be summarized for reporting to the management team.

Form B.4 — SIF demand report

This form to be maintained by the Process Automation/Control System Engineer or SIS Specialist					
Report time period			**From:**		**To:**
SIF ID#	Number of trips	Actual demands (process issue)	Spurious events (reliability issue)	Remarks	

Annex C — Example failure reports

A failure has occurred when equipment is not able to perform its required function. Failures should be recorded and tracked so that their frequency can be compared to the assumptions in the process hazards analysis and SIL Verification calculation. Repeated failure is a leading indicator of inadequate mechanical integrity and should be investigated so that action can be taken to reduce the frequency of reoccurrence where possible. This annex provides examples of failure reporting forms. Users may develop other failure reports incorporating similar information or use other forms of documentation to record and track failure.

Form C.1 — Failure investigation report form

SIF ID #:	Plant ID:
SIF description: (If there is a documented SRS provide document reference)	
Manufacturer:	Software Rev # (Firmware/application program, where relevant)
Model number:	When Installed?
Failure was detected by: ☐ Operator ☐ Diagnostic alarm ☐ Inspection ☐ Proof test ☐ Near miss / incident (If detected by incident, this report may accompany the near miss/incident report)	
Classification: _____Safety _____Environmental _____ Asset protection	
How did the equipment fail? ☐ Failed to operate according to specification ☐ Operated without cause	
Where was the failure? (check all that apply) ☐ Part failure ☐ Installation ☐ Electrical connection ☐ Process connection ☐ Program error ☐ Human error ☐ Utility (e.g., power supply, communication) ☐ Design error ☐ Other (describe) _____	
Describe what failed? (Examples: Plugged process connection, over-temperature, short, power supply went bad, electronics failed)	
Was the failure corrected through ☐ repair ☐ replacement ☐ modification ☐ program fix	
Was the repair/replacement “like for like”? ☐ yes ☐ no Was the replaced equipment on the Approved Equipment List? ☐ yes ☐ no	
Will the failed equipment be subjected to manufacturer/outside shop failure analysis? (If so, forward report to Maintenance Manager and SIS Specialist)	
Are there similar installations in this process unit, which should be examined for similar failure?	
Comments: (Detail any additional monitoring or precautions required?)	
Assessment led by: Date: SIS Specialist/Engineer or equivalent	

1 **Form C.2 — Transmitter failure report**

Plant ID:	**Loop ID:**	**Tag #:**
Test date:	**Who tested:**	**Test procedure #:**
Previous test date:	**Previous failure report #:**	
What was the effect of the failure: ☐ Failed to operate according to specification ☐ Operated without cause		
What caused the failure: ☐ Sensor ☐ Process connection ☐ Electrical connection ☐ Electrical contact ☐ Power supply ☐ Impulse line plugged ☐ Root valve/manifold closed ☐ Configuration ☐ Other (describe)		
Comments:		
Assessment led by: _____Date:_____ SIS Specialist/Engineer or equivalent		

2

3 **Form C.3 — Valve failure report**

Plant ID:	**Loop ID:**	**Tag #:**
Failure date:	**Identified by:**	**Test procedure #:**
Previous test date:	**Previous failure report #:**	
What was the effect of the failure: ☐ Failed to operate according to specification ☐ Operated without cause		
What parts contributed to the failure: ☐ Actuator ☐ Seat ☐ Airset/Air supply ☐ Solenoid valve ☐ Spring ☐ Pneumatic connection/tubing ☐ Body/Bonnet ☐ Gasket ☐ Pneumatic accessory (e.g. booster, quick vent, etc.) ☐ Guide ☐ Packing ☐ Power supply ☐ Shaft ☐ Position switch ☐ Electrical connection		
Comments:		
Assessment led by: _____Date:_____ SIS Specialist/Engineer or equivalent		

4

Annex D — Effective procedure writing, verification and implementation

A comprehensive MI program is only useful if personnel understand the intent of the program and have the means and capability to execute its procedures as written. Procedure documentation is more than just the act of putting words on paper, it involves the systematic review of the steps required to execute a job task, including the examination of human factors and ergonomics. Procedures should be in place prior to the start-up of the process equipment and should be written with the intended audience in mind. Consideration should be given to the level of technical knowledge expected of the reader.

Procedures should provide instructions, practices, and guidelines used for SIS equipment inspection, preventive maintenance, and testing. Procedures should be in place before process equipment is placed in service, updated before any change is implemented, and kept current throughout the SIS life. An internal practice should provide overall requirements for procedure scope and content. Each SIS should have a set of procedures covering the MI requirements unique to that specific SIS and its SIF. Separate work processes are often used for on-line versus off-line maintenance.

Inspection and test procedures should be available and should describe the work tasks in a step-by-step manner with clear pass/fail criteria. As with other procedures, responsible personnel or departments, the required permits and notifications, the required test equipment and tools, and any appropriate hazard or safety warnings should be identified. Procedures should provide the work process steps necessary to successfully complete equipment commissioning and validation. Validation should be performed whether repair is done on-site or by the manufacturer.

Test procedures should describe any related functions, such as SIS alarms, bypass switches, manual shutdown buttons, and resets. Procedures may be modularized as desired with procedures written for individual pieces of SIS equipment, SIF subsystems, each SIF, a set of SIF, or the entire SIS. Procedures should be comprehensive and clearly convey the work expectations and requirements. Maintenance records should be signed and dated by the person(s) conducting the work.

Those assigned responsibility for conducting work according to a test procedure should be sufficiently competent to understand and implement the procedure as written. The procedures should include an inspection of the physical installation to provide visual confirmation that equipment is in satisfactory condition. Preventive maintenance activities should also be described.

SIS equipment should be periodically proof tested to demonstrate and document that the equipment is operating according to the SRS and equipment specification. Proof tests can be performed on-line or off-line. On-line test procedures should be carefully planned, documented, and validated, because minor mistakes during on-line testing can potentially lead to process upsets or spurious trips. Off-line testing is inherently safer, but given the current trend of increasing run time between process facility turnarounds, it is becoming increasingly difficult to determine the “as good as new” equipment status without some on-line testing.

When automated diagnostics detect a fault, the SIF is configured to initiate 1) an automatic shutdown, 2) a safety alarm, or 3) a fault alarm. The required configuration is defined in the SRS and is determined by the equipment choice, subsystem fault tolerance against dangerous failure, the nature of the failure (e.g., dangerous failure versus safe), and the availability of compensating measures. Continued operation requires compensating measures to ensure safe operation during the allowable repair time (refer to ISA-TR84.00.04 Annex P). When applicable, operating procedures should provide restrictions on the maintenance activities, e.g., prohibited during certain operating modes.

Test procedures should cover in detail how maintenance is performed safely while the process equipment is operating. A key parameter for on-line repair is the allowable repair time

established in the design and operating basis. The allowable repair time provides the maximum time that the equipment can be out of service prior to initiating management of change activity. The management of change review is performed to determine whether the compensating measures are sufficient for the extended period, additional measures are required, or manual shutdown executed. The review should also address the priority status for the repair activity.

A specific written test procedure should be available for each SIF. The procedures should be of sufficient detail to allow personnel who are not intimately familiar with the SIF to perform the appropriate testing. These should include where appropriate the following:

- list of SIF included in the SIS
- equipment description and location for each safety function
- functional requirements for each safety function
- inspection procedures to be followed
- calibration and testing methods to be followed
- frequency of calibration, testing, inspections, and maintenance activities
- specify acceptable performance limits (± 2% of full range if no limits specified)
- specify sequence of testing if required
- specify who should perform test
- specify state of process when test is performed
- if the SIF is mirrored in the BPCS, test should show that SIF actuated final control device
- verification of operational state of SIF after test complete
- test of internal and external diagnostics (WDT, etc.)
- verify auxiliary service components are operational (fans, filters, batteries, UPS, etc.)
- define a means of ensuring testing is performed and documented

All test procedures should have system being tested, page numbers, and revision date on each page of procedure. The responsible role/person for maintaining each procedure should be identified in the procedure. The electronic file path or hard copy library location of test procedures corresponding to the device to be tested should appropriately loaded in the maintenance management system.

All drawings used to describe SIF should be referenced including P&IDs, loop drawings, logic sheets, etc.

Procedures should focus on the ways in which the core attributes, namely independence, integrity, functionality, reliability, auditability, access security, and management of change, are maintained to the suitable level of rigor. Well written procedures help eliminate systematic failures by providing instructions, improving communication, reducing training time, and improving work consistency.

The test procedures are considered a controlled document just like the process operating procedures. Any deviations from the documented test procedure should be reviewed to make sure the change will lead to a failure of the SIF.

A thorough understanding of the intended SIS functionality is critical to ensuring that the SIS is operated and maintained to meet the required performance. Consideration should be given to potential language barriers to effective learning. If multiple languages are spoken, safety and emergency information should be communicated in other languages as necessary to ensure personnel understand work process requirements and expectations. If personnel do not

understand how the SIS equipment is expected to operate, a procedure change, variance, or deviation may seem acceptable, yet yield an undesirable outcome.

Personnel should be trained on facility procedures, such as safe work practices, evacuation and response procedures, access permit requirements, and management of change. Personnel should receive specific training related to their assigned responsibility. Personnel training should be verified as complete during the pre-start-up safety review for any new or modified SIS. New personnel should complete training on the SIS operation prior to taking responsibility for the process equipment.

Once an SIS is operational, knowledge and skills should be maintained through an on-going training program. For best results, facility training should emphasize the fundamental criticality of SIS operation. Means for evaluating the training program effectiveness should be implemented. Training should be revised to resolve deficiencies. Knowledge and skills based testing can be used to validate training effectiveness, as necessary. When knowledge and skills do not match expectations, consideration should be given to improving training content, depth, or frequency to obtain the desired level of competence. Training records should be maintained.

Training should familiarize maintenance personnel with the hazardous events the SIS protects against and the expected SIS operation. Personnel assigned responsibility to perform maintenance and testing on the SIS equipment require the knowledge and experience necessary to perform the procedures correctly. Training should ensure that maintenance personnel understand what permits and notifications are required to work on or to bypass SIS equipment. Training should cover task expectations, such as documentation, reporting, and failure investigation.

D.1 Format

The procedure format is often determined by the equipment to be tested, the testing equipment employed and the capabilities of the technician performing the test procedure. All procedures should be written with their intended audience in mind and with an appreciation for the specific technical knowledge of the reader. The procedures should be clear and concise, with minimum complexity. Procedures should provide information in different formats, such as text, graphics, and flowcharts, to accommodate different learning styles. Where multiple languages are spoken, consideration should be given to developing procedures and training materials in each language to ensure critical information is not lost in translation.

Task lists, checklists, hierarchical outlines, or task analysis can be used to create procedures, which are easy to understand and use. Task analysis offers a more rigorous organization than other methods. It often uses a three or four column format delineating major steps, providing detailed work tasks, caution notes and comments.

The choice of technique is highly related to the complexity of the procedure. Task lists are generally restricted to very simple work instructions, requiring few steps and decisions. Longer instructions should be written in checklists or in hierarchical (i.e., outline) format to break the work process into smaller logical steps that are generally executed in series to obtain the specified result. For example, a series of maintenance steps for a transmitter would include activities such as checking the transmitter range, verifying the deviation alarms, and validating the trip set point. Each step has specified pass-fail criteria, which is evaluated and recorded.

When many decisions are required, graphical techniques for presenting the steps of the procedure, such as flow charts, should be considered. Flow charts break down the procedures into small logical steps and provide an effective means to illustrate decision blocks where the answer choice, e.g., a “yes or no,” affects the action to be taken.

Regardless of the format chosen, the goal is to ensure that safe and reliable operation is achieved through the detection and correction of failures. The SIS procedures should be written

with sufficient detail to achieve the performance specified in the SRS. Just as the core attributes affect the SRS, they are also significant to effective procedure development.

D.2 Test scope

The test scope should identify for the technician what the procedure intends to test, the status of the process during the test, and what is not tested using this procedure. In some cases there may be several test procedures for a specific component or SIF.

- the hazardous event(s) for which the SIF provides protection
- the hazardous event(s) classification or SIL target
- the testing and inspection interval
- the identification of the equipment on which the inspection or test was performed (e.g., loop number, equipment number, SIF identification, test procedure reference for a set of SIF)
- the settings and tolerance or acceptable performance limits (e.g., pass/fail criteria) for the SIS equipment
- the pretest conditions required to safely run the test, including the state of the process (normal operating conditions, shutdown, on-line, off-line, lock-out, etc.)
- for on-line tests with a process hazard present, the procedure must give specific instructions on what to do if the SIF fails and specify limits on when to abort the test
- the proper step-by-step sequence in which to run the test
- the procedure validates each channel of the SIF, including
  - each channel of the SIF independently trips each final element as designed
  - each SIF independently trips each final element as designed
  - each logic solver independently trips each final element as designed. If BPCS is used in the SIF, it should be tested in the procedure.
- the name(s) of the qualified individuals performing the test, and their responsibilities
- reference drawings and documents
- test equipment required
- removal of equipment used for the test
- verification that equipment and final control element is returned to normal operation. Verification that each sensor and final control element is returned to pre-test operation.
- permits required
- manufacturing authorization of the procedure

D.3 Related reference data, drawings, documentation, procedures

The technician may need additional information not contained in the test procedure in order to properly carry out the test such as calibration procedures, lock out procedures, line breaking procedures, inspection procedures, schematic diagrams, and P&ID. Providing references to the technician will ensure the test procedure will be properly carried out and reduce the time required to perform the tests. This is especially important during turnarounds where many test procedures may need to be completed in a short period of time.

D.4 Personnel safety considerations

Personnel may be exposed to the process while performing the test procedure or have to enter an area which would put the operator at risk. In order for the technician to perform the work safely, they need to be informed of the hazards they may incur, such as exposure to hazardous

substances, electrocution, flammables, radiation, gravity, and ergonomic considerations and the potential consequences of failure to follow the procedure or of exposure.

D.5 Planning

Performing testing on a process can be costly and potentially result in a loss of production. It is important to document in the planning section of the procedure the testing equipment, PPE, test gases, scaffolding, and any other equipment needed to perform the test. In addition, the plan should include information on what to do if the test fails. Remember that if the test is performed on-line, you do not have an unlimited amount of time to complete the test. Locating the spare parts for the SIF before the shutdown can save a lot of precious time when SIS equipment fails the test and needs to be replaced. To aid the technician in planning it is recommended to have notification of required test issued via the maintenance management system 30 to 60 days from the actual required test date.

D.6 Notification (Operations, Facility, etc.)

What the technician does in the process can affect many others in the process and even potentially the community if the work is not coordinated with the proper plant personnel. Before the technician starts work, a permit to work should be obtained from the appropriate person in order to make sure it is safe to perform the work. In addition the technician may need to get a breaking into process permit or a lockout permit in order to perform the procedure safely. The notification section of the procedure should identify the permits required to perform the work safely.

D.7 Operating procedure requirements

Figure D.1 provides an example of a simplified work process, illustrating the typical interrelationship between operational and maintenance activities. The content and depth of the information communicated to various personnel should be based on the intended role of the individual in managing risk and performing the MI activity.

Process Engineering and Operations are primarily responsible for defining the content of SIS operating procedures. These procedures should cover SIS specific information and should explain to the operator the correct use of bypasses and resets, the required response to SIS alarms and trips, when to execute a manual shutdown, and provisions for operation with detected faults. These procedures, along with analogous ones developed by Maintenance/Reliability Engineering for maintenance activities, make up the backbone of the operating basis for the process equipment.

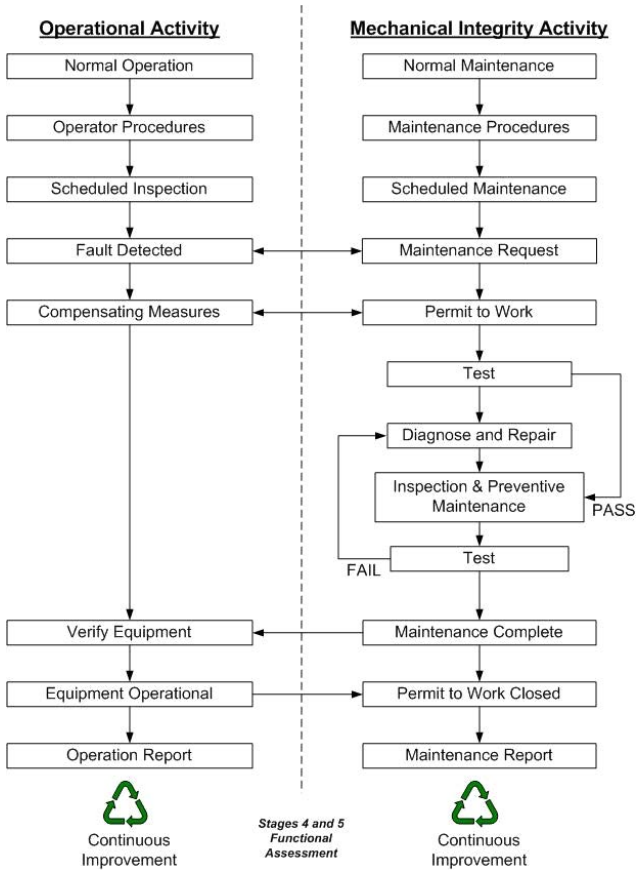


Figure D.1 — Simplified operation and maintenance work process

D.8 Procedure verification

Maintenance procedures should be analyzed using a suitable, standardized method to determine the coverage comprehensiveness of the test procedure, ensure adequate test coverage for all dangerous failure modes, and ensure the potential for systematic (human) errors have been considered in the procedure. These methods may vary depending upon the complexity of the task and may include failure mode and effects analysis (FMEA), job step analysis, task analysis, or equivalent. While a test should be comprehensive, if it is too difficult or complex, there is a greater likelihood the test will not be completed properly.

D.9 Procedure analysis

Each procedure should define the individuals, departments, or job functions responsible for the development, approval, upkeep, distribution, and revision management of the procedures themselves. Work procedures are most successful when they are broken down into steps or tasks intended to achieve specific results.

If the intended audience does not understand them or feels that they are too complex, the procedures will not be followed. In an operating and maintenance environment, people often tend to follow the path of least resistance and, if they perceive a difficult path, they may find an easier, though not necessarily correct, or safe, one.

Table D.1 provides a listing of people, situations, and system related errors. Slips, such as omissions and lapses, are common, yet critical errors. Incorrect equipment assembly, installation, and repair are common maintenance errors.

Table D.1 — People, situations, and system related errors

People-oriented errors
Slips (lapses, omissions, execution errors)
Capture error
Identification error
Impossible tasks
Input or misperception errors
Lack of knowledge
Over-motivation or under under-motivation
Reasoning error
Task mismatches
Situation-oriented errors
Environmental
Stress
Timing
System-oriented errors
Errors by others
Procedural
Violations
Human errors in system design
Mistakes
Specification errors
Communication breakdown
Lack of competency
Functional errors
Common errors in instrument design

D.10 Continuous improvement

Personnel should contribute their experience and knowledge to the continuous improvement of procedures and practices. Cooperation of multiple parties is necessary to ensure that the SIS requirements match the capability of personnel. Procedures used in combination with training and regular performance feedback achieve predictable work results. The procedure should be reviewed after completion by a planner and any deviations should be reviewed to determine whether the procedure should be updated. Any modifications to the procedure should follow the MOC procedures at the site.

D.11 Modification

SIS procedures should be under revision control. Procedures should be periodically reviewed to ensure that the procedures are up-to-date and reflect current work tasks and expectations. Changes to SIS procedures, whether technical or editorial, should be reviewed and approved.

This page intentionally left blank.

Annex E — Example inspection items and forms

The following are recommended inspection items that should be covered by an inspection program as part of an overall mechanical integrity plan. The bullet lists are not exhaustive and do not include everything that should be covered by the inspection program for particular equipment or SIS.

Inspection is typically not a singular activity, but something that is done as part of other duties and in some cases only under specific circumstances. Some items can be addressed by simple visual inspection, where personnel perform a unit walkthrough and look for discrepancies, e.g., tagging or labeling. These inspections do not require tools and may be performed by plant operators or maintenance technicians. Other items can be intrusive, requiring “hands-on” inspection and would likely be performed only by maintenance personnel under controlled conditions, e.g., pulling wire to determine whether it is loose. These latter items are often verified during commissioning or proof testing when equipment is off-line or in bypass. Some inspections require specialized resources, tools and equipment access. For example, examining the physical condition, application program, and diagnostic status of a logic solver requires a skilled control system technician and access to the engineering station and logic solver. Another example requiring specialized tools would be the use of radiography to detect a plugged process connection. Any person trained in the use of the radiography equipment could perform the inspection, but it is likely that it would only be performed on connections where process pluggage has been identified as a concern.

The recommended inspection items are not intended to be turned into a single checklist, since these items may be performed at different frequencies depending on manufacturer recommendations, the type of inspection being performed, the expected equipment degradation rates, specific characteristics of the process, and SIS management of change history. Some of these items may be inspected frequently as in the case of visual inspections, while others may only be performed infrequently as in the case of “hands-on” inspections.

Generally, an inspection checklist or form is used to support thorough inspection. An example checklist is provided in Table E.1. This checklist applies to multiple equipment types and is not intended for use as is. Typically, a user will have a generic template with typical inspection items and then modify the template to address the specific application and device technology, subject to a particular inspection. Specific checklists are used to ensure consistency in the inspection scope and record quality. Training should ensure that inspectors understand the importance of verifying the overall fitness of the equipment in service and of reporting any discrepancies with the equipment regardless of the checklist items.

E.1 General field inspection items

On the field side, the focus is on the physical aspects of the installation, such as wiring, status of any punch list items remaining from the commissioning effort, and adherence to construction specifications. Field inspections should verify:

- tags and labeling
- painting, where applicable
- conduit seals
- covers
- wiring
- grounding systems
- support systems (e.g., communications, power supplies, and instrument air)
- installation materials (e.g., gaskets, grounding rings)

- installation (e.g., bolts, insulation, process connections, supports, tracing, purges, bug screens,)
- installation quality (e.g., no signs of physical disturbances, such as absence of moisture/debris/corrosion, excessive vibration or steam impingement)
- barriers (e.g., bollards protecting equipment from physical impact or covers on emergency push buttons)
- warning signs (e.g., radiation or high voltage hazard)

Each component of an SIF should be in good condition with no visible physical defects, which could impact the performance or reliability of the system. All parts of the SIF should be inspected for damage, deterioration, missing parts, or other physical damage and for incipient conditions such as water ingress. The physical examination should include:

- all input devices to the SIS such as transmitters, switches, thermocouples
- all output devices such as solenoid valves, control valves, motor controllers
- system wiring with particular attention to terminations, junction boxes, conduit
- SIS logic solver - electromechanical relays, PLC, etc.

E.2 Sensors

In addition to the items covered in E.1, the following inspection criteria apply to field sensors:

- instruments clearly identified as part of SIF
- process connections in good condition with respect to leaks, insulation, corrosion, etc.
- root valves in correct position
- instruments installed per design standards and manufacturer guidelines
- configuration per design
- heat tracing functional and insulation in good condition
- conduit connections and covers in good condition and properly supported
- cabling in good condition and correct length for thermal expansion
- cabling drip loops in place and functional with drainage to a proper location
- drains and seals, if required, in place and functional
- process tubing lines properly supported and sloped

E.3 Final elements

In addition to the items covered in E-1, the following inspection criteria apply to the final elements:

- final elements clearly identified as part of SIF
- configuration per design (e.g., valve fails open or closed)
- heat tracing functional and insulation in good condition
- bug screens in place and functional
- tubing for air supply and connections to positioner or top works in good condition
- solenoids properly mounted with tubing and electrical connections in good condition
- valve piping gaskets in good condition (e.g., no cracks or leaks)
- valve stem in good condition

- top works in good condition (e.g., no cracks or leaks at gaskets)
- valve installation supports in good condition
- no corrosion build-up around valve stem
- motor control circuits in good condition
- variable speed drive mounting is secure
- electrical wiring terminals (at each end) are properly tightened
- no sign of overheating has occurred at each terminal
- no corrosion, burnt spots, overheating, de-formation, or discoloration on contacts
- instrument pressure gauges in good condition
- any auxiliary equipment, such as signal converters and positioners, in good condition
- any other conditions which might hinder proper operation of the valve

E.4 Logic solvers

The following inspection items apply to logic solvers:

- diagnostic checks
  - diagnostic alarms configured per specification and properly prioritized
  - proper operation of all communication buses
  - power to redundant power supplies and proper operation
  - proper logic solver scan order to ensure proper process safety time
  - operating records indicate that solid state outputs are not generating “off” leakage current above rated value
- physical checks
  - components clearly identified as part of SIF
  - absence of moisture
  - status condition lights are functional and normal (e.g., fault, communication, power, fusing)
  - ventilation or cooling is functional
  - absence of dust or other foreign material (e.g., filters)
  - closure hardware installed per design standards
  - check that access security (e.g., doors locked) is in place
- logical checks
  - configuration per design (e.g., absence of forces and bypasses, scan rate)
  - manufacturer recommendations (e.g., bug fixes, recalls)

E.5 Wiring connections

The following inspection items apply to wiring connections:

- wiring, terminals or junction boxes clearly identified as part of SIF
- wiring connections in junction boxes, scramble boxes, or other terminations are tight
- wiring and cable segregation, as required, is in place
- fire proofing per design

- seals where required should be checked
- conduit covers should be in place
- conduit drains should be in place and working properly
- cabinet doors are closed, water tight, and properly labeled

E.6 Power and grounding/bonding

Proper grounding includes many separate grounding entities in a process facility. Some examples include DCS, PLC, highway, static, substation, neutral, single point, motor, raceway, control room, instrument transformer, building, faraday effect (framing), lightning cone of protection, surge protection, safety, noise (e.g., shielding), ungrounded, ground tripod, lightning rods, ground rods, ground noise, computer flooring, footing ground rods, isolated, ground plane, UPS, isolation transformer, computer, ground resistance, etc. For this technical report, discussion of grounding is focused on the SIS, but the reader is cautioned that improper grounding and poor maintenance of the grounding systems is one of the leading causes for process unreliability.

Power and grounding connections and insulation should be verified to ensure no degradation. Visual inspection is typically performed during on-line operation, while more rigorous physical inspection is executed off-line. The following inspection criteria apply:

- all power and grounding / bonding installed per documented design
- all power and grounding / bonding connections securely fastened
- no evidence of corrosion or fouling on any power or grounding / bonding connections
- no evidence of sliced, cracked or otherwise degraded power and grounding / bonding insulation
- no evidence of charring or heat build-up
- power operating within acceptance range

Form E.1 — Generic field sensor checklist

Instrument number: _____
Test number: _____

Materials of construction:

☐ OK ☐Not OK	No obvious signs of corrosion in area with the process
☐ OK ☐Not OK	Model number of installed instrument matches instrument calibration records

Protection from the environment:

☐ OK ☐Not OK ☐ NA	Protection from mechanical damage (can instrument be used as a step, etc.)
☐ OK ☐Not OK ☐ NA	Protection from weather (freezing, rain, snow, ice, etc.)
☐ OK ☐Not OK ☐ NA	Protection from insects, birds, etc. (vents clear, etc.)
☐ OK ☐Not OK ☐ NA	Protection from corrosive leaks of adjacent process (signs of external corrosion on instrument)

Proper installation of impulse lines:

☐ OK ☐Not OK ☐ NA	Sloped correctly (down for liquids, up for gases)
☐ OK ☐Not OK ☐ NA	Materials of construction correct (no obvious signs of corrosion)

Proper installation of instrument:

☐ OK ☐Not OK ☐ NA	Orientation of instrument
☐ OK ☐Not OK ☐ NA	Field zeroed after shop calibration (if required)
☐ OK ☐Not OK ☐ NA	Primary elements not worn or eroded (orifice plates, vortex shedder bar, etc.)
☐ OK ☐Not OK ☐ NA	Breather drain fitting installed
☐ OK ☐Not OK ☐ NA	Low point conduit drain installed
☐ OK ☐Not OK ☐ NA	Conduit in good shape
☐ OK ☐Not OK ☐ NA	Proper static grounding applied

Process concerns:

☐ OK ☐Not OK ☐ NA	Impulse lines not plugged
☐ OK ☐Not OK ☐ NA	Purges working properly
☐ OK ☐Not OK ☐ NA	No corrosion present
☐ OK ☐Not OK ☐ NA	Thermowell fouling

Equipment identification:

☐ OK ☐Not OK ☐ NA	Green "Safety Interlock" tag installed
☐ OK ☐Not OK ☐ NA	Clearly labeled with instrument number
☐ OK ☐Not OK ☐ NA	Up-to-date calibration sticker

Comments/Observations:_____

Inspected by:_____

Inspection date:_____

This page intentionally left blank.

Annex F — Example calibration forms

This Annex provides an example of a calibration record. Users may develop other calibration records incorporating similar information or use other forms of documentation to record and track calibration.

Form F.1 — Instrument calibration record

TAG NUMBER:			**DATE:**	/ /	
UNIT:			**SYSTEM:**		
TRANS DAMPENING:		**Seconds**	**TRANSMITTER**	**Analog** ☐	**SqRt.** ☐
VERIFIED AGAINST GOVERNING DOCUMENT ☐			**AS-FOUND:**	**Digital** ☐	**Linear** ☐

Transmitter Calibration Data				**SERIAL NUMBER:**		
Zero and Span	Process Range	Units	Transmitter Input	Units	Transmitter Output	Units
Lower Limit						
Upper Limit						

Transmitter Calibration Record								
Transmitter Input:		**Transmitter Output:**						
Percent of Span	**Actual Input**	**Desired Output**	**Output As-found**	**% Error As-found**	**After Calibration**	**% Error After Cal.**	**Output As-left**	**% Error As-left**
0%								
25%								
50%								
75%								
100%								

Actual output - Desired output			
Percent error = (Actual output - Desired output)/(Upper output limit - Lower output limit) X 100%			
Maximum allowable % error:			The maximum allowable % error is listed in the instrument maintenance SOP.
Maximum % error as-found:			
Calibration required:	☐ Yes	☐ No	Calibration is required if the maximum % error as-found is greater than the maximum allowable % error.
Maximum % error after calibration:			Corrective action (repair or replacement is required if the maximum % error after calibration is greater than the maximum allowable % error.
Corrective action required:	☐ **Yes**	☐ **No**	
Corrective action taken: (If required)			

Switch Settings:		Serial Number:			
Tag Number	**Switch Setting**	**Signal As-found**	**Signal As-left**	**Deadband**	**Comments**

Switch Settings:		Serial Number:			
Tag Number	**Switch Setting**	**Signal As-found**	**Signal As-left**	**Deadband**	**Comments**

Calibration Equipment Used:		
Instrument Shop I.D. Number	**Calibration Due Date**	**Comments**
IS	/ /	
IS	/ /	
IS	/ /	
IS	/ /	

REMARKS: _____

TRANSMITTER
- ☐ DIGITAL
- ☐ ANALOG
- ☐ PROPERLY COLOR CODED

AS-LEFT:
- ☐ PMI PERFORMED

- ☐ DOWNSCALE B/O
- ☐ UPSCALE B/O
- ☐ SQUARE ROOT
- ☐ LINEAR

- ☐ SS TAG ATTACHED

TECHNICIAN: _____ DATE: _____/ /_____

Annex G — Preventive maintenance

Preventive maintenance is a proactive activity that maintains the equipment in the “as good as new” condition. When the equipment is in this condition, it is operating within its useful life period. Preventive maintenance reduces the frequency of equipment failure through periodic restoration of the equipment condition. It involves many different activities that occur based on fixed schedules and based on predicted degradation. It includes performing maintenance to extend the equipment life such as changing an air filter and replacing disposable parts such as changing batteries. Common preventive maintenance tasks include timely:

- battery replacement
- process connection cleaning
- periodic replacement of eroded components based on historical erosion rates (e.g., flow tubes, thermowells, or orifice plates)
- rebuilding valves
  - seat
  - actuator
  - packing
- gasket replacement
- instrument air filter / separator cleaning/change-out
- lubrication
- electrical contact replacement

Appropriate preventive maintenance tasks may be identified from sources such as manufacturer’s literature, brainstorming, operating experience, maintenance experience, and best practices. Important considerations in establishing a rigorous MI program include:

- integrating preventive maintenance efforts with other plant tasks resulting in a cost effective efficient multi-tasking maintenance program.
- availability of the competent and trained personnel to perform the desired maintenance.
- availability of correct materials and tools to utilize in the desired maintenance.
- availability of correct instructions and related planning to utilize in the desired maintenance.
- availability of MI and reliability processes to identify chronic failure issues (e.g., possible improper selection of equipment/materials).

G.1 Identification of preventive maintenance tasks

Understanding causes and mechanisms of equipment failures provides the insight as to how the path to failure may be measured. It also helps to establish appropriate predetermined levels of degradation that mandate action is taken within some prescribed time period.

An initial source of needed preventive maintenance tasks can be found in the manufacturer’s safety manual and equipment maintenance manual. This will need to be supplemented with the tasks required due to the impact of the process and environmental conditions, which may accelerate the degradation or wear beyond manufacturer expectations. Failure Modes and Effects Analysis (FMEA) and Reliability Centered Maintenance (RCM) are analytical methods that can be used to identify preventive maintenance tasks that sustain the SIS equipment’s integrity and reliability.

Failure investigation, such as Root Cause Analysis, can potentially identify weaknesses in the maintenance program which should be corrected. This approach helps facilitate an overall

reliability centered maintenance program that additionally would measure and analyze equipment performance, looking to maintain expected performance as well as to identify opportunities to improve reliability.

G.2 Criticality

Some maintenance tasks are performed to extend the life of the equipment, such as replacing the electrolyte in an analyzer's cell, or improving the reliability of the equipment. Other tasks are critical to ensuring the integrity and reliability of the SIF on a routine basis, such as replacing instrument air filters to reduce the likelihood of failing or rebuilding shutoff valves on a periodic basis. While all of these activities are important to the operation of the process, tasks associated with maintaining the performance of the SIS need to be managed using the typical lifecycle management systems such as MOC, action tracking, failure response, and documentation.

G.3 Timing

The frequency of maintenance tasks are affected by the following:

- shutdown schedule
- on-line vs. off-line tasks
- unexpected as found condition during preventive maintenance
- manufacturer's recommendations
- good engineering practices and expert judgment
- system architecture (e.g. level of fault tolerance)
- PFD targets
- incident investigation results
- testing interval constraints and requirements
- number of operations
- hours of operation experience

In some cases optimizing all of the factors to satisfy performance expectations can be a challenge, especially the shutdown schedule. The SIS design may need to include provisions for performing preventive maintenance on-line. During a turnaround, preventive maintenance tasks may need to be performed in conjunction with inspection and testing tasks. The order of these tasks and whether they can be performed at the same time should be discussed and scheduled. When production units do not run continuously, the preventive maintenance tasks may by based on how long the equipment is operating or may need to be scheduled just prior to startup of the unit.

As part of the continuous improvement part of the lifecycle, the timing of the activities need to be reviewed to determine if the performance of the maintenance program meets the assumptions of the SIL Verification. Maintenance records and incident investigations can provide insight into whether the MI plan is achieving its goals. Where the equipment performance does not meet the required performance, the task may need to be performed more frequently or modified to improve performance. Where the performance of the equipment cannot be improved by modifying the timing or task, other equipment may need to be selected.

Once a schedule basis is established, changes should be reviewed to ensure that the change does not impact the SIS equipment integrity. When the task cannot be performed within a defined acceptable grace period, the user has several options using management of change. This may include permanent changes to the schedule if justified or implementing alternative

temporary means of risk reduction. Annex J provides additional guidance for dealing with potential deferral situations.

G.3.1 Fixed schedule

Fixed schedules are often used to address parts that predictably wear out, gum up, foul, corrode, etc. Inspection checklists, such as those listed in Annex E, can supplement scheduled preventive maintenance by identifying corrosion and wear and to determine what parts need to be replaced. When a part is found to be out of tolerance, the part is repaired/ replaced to bring the equipment back to an “as good as new” condition.

Some of the advantages of conducting preventive maintenance on a fixed schedule include:

- allows maintenance effort to serve as a training tool
- improved process uptime and fewer process upsets
- planned maintenance resulting in a safe plant floor environment
- planned maintenance resulting in shorter downtime
- sustain warranty protection
- reduced spares inventory

G.3.2 Predictive maintenance schedule

Predictive, or condition-based, maintenance represents a means to detect equipment degradation, allowing repair to occur prior to a complete failure. It is only appropriate when there is a method in place that allows measurement of degraded performance so that a predetermined intervention point can be defined. For example, inspection or proof testing checklists can be used to identify when replaceable parts are wearing out, so the replacement of the part can be scheduled so that it is replaced prior to the equipment failure.

For predictive maintenance, the timing is linked to an inspection, test or diagnostics to determine the timing. The MI plan should define the response required once a deficiency has been identified and when the task becomes overdue. The response to an overdue task will need to consider how fast the equipment is degrading. The response is generally more critical than scheduled maintenance since degradation has already been identified and documented either through inspection activities or automated diagnostics that alert personnel when there is a need for intervention.

For example a 2oo3 voting level sensors where two sensors are DP level and one radar level, comparison diagnostics can be used to identify the onset of excessive drift or allowing identification of impulse line pluggage. Instead of cleaning the impulse lines on a weekly basis the lines could be cleaned based on the diagnostics results.

Advantages of predictive maintenance include:

- improved process uptime and fewer spurious shutdowns, especially when used in conjunction with fault tolerant systems
- availability of information to support troubleshooting
- providing an alert to the appropriate personnel, giving them some time to optimize the performance of critical maintenance activities
- integration with other mechanical integrity efforts resulting in a cost effective efficient multi-tasking maintenance program
- automated documentation of specifically defined degraded conditions to support proven in use

- extended life as degraded conditions are repaired prior to more complete failures
- analysis of actual equipment “wear-out” versus estimated “wear-out” performance allowing MI plan upgrade
- controlled analysis of replaced equipment for evidence of unexpected application limitations or potential unsafe failures
- optimized spares inventory

G.4 Documentation

Preventive maintenance should be documented and include step-by-step instructions as needed to ensure the task is being performed consistently and properly. The procedure should include:

- procedure for performing the task
- who is qualified to perform the task
- pass / fail criteria
- as-found condition
- listing of parts replaced
- other work performed in response to as-found condition
- as-left condition
- name of person(s) performing task

Where the as-found is outside the expected condition, the current condition should be documented for that piece of equipment. The deviation from expected performance should be investigated to determine if the frequency of the maintenance activity is adequate or if potential changes should be considered. Options include development of additional scheduled maintenance activities, redesign of the device in question or implementation of predictive maintenance via diagnostics.

Annex H — Example proof test template and procedures

The proof test template (Table G.1) and technology test procedures contained in this technical report are examples of how some user companies develop proof test procedures. The user is reminded that the proof test template and the device tests contained in this technical report are examples illustrating how some user companies develop and implement proof test procedures. It should not be interpreted that these are recommendations or requirements for proof testing any specific technology. Users should consider their application and SIF requirements, as well as manufacturer's recommendations, when writing proof test procedures. The user is cautioned to clearly understand all facility design and operational constraints prior to developing and executing proof test procedures.

Table H.1 — Proof test procedure template

Generic Procedure	
Scope	**This generic procedure is meant to provide a basis to develop plant specific and technology specific proof test procedures. It DOES NOT take into account specific concerns regarding safety, process control disturbances, etc. that may be related to a particular plant or process. While there are some points in the procedure where notice is given that safety, control of the process, etc. should be considered, it is the responsibility of the person using this document, and modifying it for a specific plant and technology, to take these process concerns into account. Steps that lead the user to check specific known hazards should be added to this procedure by plant representatives who understand the process, and who thus know what kinds of items should be addressed.** This document explains the basic rules of the test procedures and provides directions for the development of plant specific procedures and or new procedures. *(Define the task along with explaining when to apply and why it must be done a specific way. Also, describe how it affects product or service quality)*
General Plant and SIF Information	Facility code number: _____ Plant code number: _____ Safety Instrumented Function (SIF) identification number: _____ Protective system type (circle applicable type) • Alarm • Shutdown interlock • Permissive interlock • Auto-Start interlock Protective circuit description: (Reference applicable interlock table or master alarm summary as appropriate) _____

Continued on next page