Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

*Setting the Standard for Automation™*

TECHNICAL REPORT

**ISA-TR84.00.03-2019**

# Automation Asset Integrity of Safety Instrumented Systems (SIS)

**Approved 14 August 2019**

ISA-TR84.00.03-2019
Automation Asset Integrity of Safety Instrumented Systems (SIS)

ISBN: 978-1-64331-072-5



ISA
67 T.W. 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-TR84.00.03-2019.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 T.W. 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.**

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of nonprofit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following served as leaders and voting members of ISA84 in the development of this technical report, which was prepared by ISA84 Working Group 3.

| NAME | AFFILIATION |
|---|---|
| Murli Balsubramanian, WG3 Chair | ExxonMobil |
| Angela Summers, WG3 Editor | SIS-TECH Solutions |
| Rahul Bhojani, ISA84 Co-Chair | BP |
| Paul Gruhn, ISA84 Co-Chair | aeSolutions |
| Nicholas Sands, ISA84 Co-Mgr Director | DuPont |
| Dennis Zetterberg, ISA84 Co-Mgr Director | Chevron |
| Richard Dunn, ISA84 Vice Chair | DuPont |
| Nagappan Muthiah, ISA84 Secretary | Phillips 66 |
| Tadaaki Ando | Yokogawa |
| David Bennett | Worley |
| David Blackburn | Phillips 66 |
| Harry Cheddie | Cteris |
| Raju Chittilapilly | ONGC |
| KV Gandhi | KBR |
| Luis Garcia | Siemens |
| Ian Gibson | Consultant |
| William Goble | exida |
| James Harris | UOP |
| Farshad Hendi | Schneider Electric |
| Janardhanan Kallambettu | Bechtel |
| Palaniappan Kannan | Petroleum Development of Oman |
| Len Laskowski | Emerson |
| Donald Lyons | Valero |
| Edward Marszal | Kenexis |
| Marcelo Mollicone | SYM PCS |
| Ramon Morillo | Marathon Petroleum |
| Scott Mourier | Dow Chemical |
| Donatus Ogwude | Creative Systems International |
| Bhagyashree Pataskar | Covestro |

| | |
|---|---|
| Richard Roberts | Consultant |
| Michael Scott | aeSolutions |
| Peter Skipp | Rockwell Automation |
| William Vogtmann | Enterprise Products Partners |
| Arthur Woltman | Consultant |

This technical report was approved for publication by the ISA Standards and Practices Board on 14 August 2019.

| NAME | AFFILIATION |
|---|---|
| C. Monchinski, Vice President | Automated Control Concepts Inc |
| D. Bartusiak | ExxonMobil Research & Engineering |
| D. Brandl | BR&L Consulting |
| P. Brett | Honeywell Inc |
| E. Cosman | OIT Concepts, LLC |
| D. Dunn | T.F. Hudgins, Inc. - Allied Reliability Group |
| J. Federlein | Federlein & Assoc LLC |
| B. Fitzpatrick | Wood PLC |
| J-P Hauet | Hauet.Com |
| D. Lee | Emerson Automation Solutions |
| G. Lehmann | AECOM |
| T. McAvinew | Consultant |
| V. Mezzano | Fluor Corporation |
| G. Nasby | City of Guelph Water Services |
| M. Nixon | Emerson Process Management |
| D. Reed | Rockwell Automation |
| N. Sands | DuPont Company |
| H. Sasajima | Fieldcomm Group Inc. Asia-Pacific |
| H. Storey | Herman Storey Consulting |
| I. Verhappen | Industrial Automation Networks |
| D. Visnich | Burns & McDonnell |
| W. Weidman | Consultant |
| J. Weiss | Applied Control Solutions LLC |
| M. Wilkins | Yokogawa UK Ltd |
| D. Zetterberg | Chevron Energy Technology Company |

This page intentionally left blank.

# Contents

## Figures

## Tables

# FOREWORD

ANSI/ISA-61511-1-2018 gives requirements for specification, design, installation, operation and maintenance, modification, and decommissioning, so that a safety instrumented system (SIS) 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-61511-1-2018 Figure 7 and described in ANSI/ISA-61511-1-2018 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 SIS lifecycle. Figure 7 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-61511-1 in 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 automation asset integrity (AAI) 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 AAI requirements for any given SIL. Once a SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured AAI program as described in ISA-TR84.00.03.

**ISA-TR84.00.03 – Automation Asset 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 AAI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective AAI program that demonstrates through traceable and auditable documentation that the SIS and its equipment are maintained in compliance with the safety requirements specification. The technical report addresses the identification of personnel roles and responsibilities when establishing an AAI plan, important considerations in establishing an effective AAI program, and detailed examples to illustrate user work processes used to support various activities of the AAI program. Data and information collected as part of the AAI 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-61511**—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-61511. 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, and fault tolerance – 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 AAI program, which is discussed in ISA-TR84.00.03.

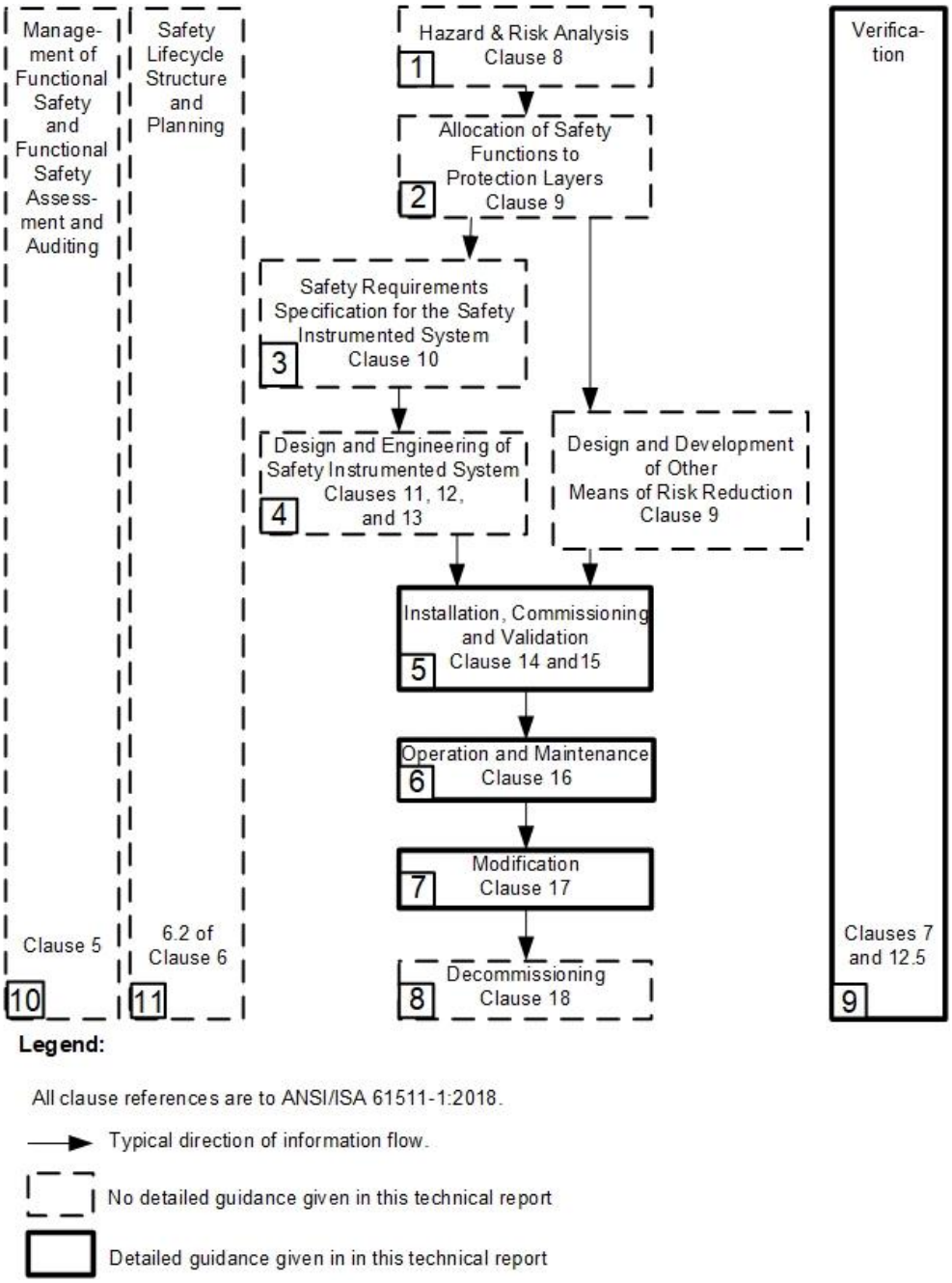



**Figure 1 – SIS safety lifecycle phases (modified ANSI/ISA-61511-1 Figure 7)**

**Table 1 – SIS safety lifecycle overview (modified ANSI/ISA-61511-1 Table 2)**

| Safety lifecycle phase or activity | | Objectives | ANSI/ISA-61511-1-2018 Requirements Clause | ISA84 Technical Report Reference |
|---|---|---|---|---|
| Figure 7 box number | Title | | | |
| 1 | H&RA | 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 SIF, the associated SIL | 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 SIF 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 SIF and their associated safety integrity | 11, 12 | ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q<br>ISA-TR84.00.02 |
| **5** | **SIS installation commissioning and validation** | **To integrate and test the SIS**<br>**To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and their associated safety integrity** | **14, 15** | **ISA-TR84.00.03** |
| **6** | **SIS operation and maintenance** | **To ensure that the functional safety of the SIS is maintained during operation and maintenance** | **16** | **ISA-TR84.00.03** |

| Safety lifecycle phase or activity | | Objectives | ANSI/ISA-61511-1-2018 Requirements Clause | ISA84 Technical Report Reference |
|---|---|---|---|---|
| Figure 7 box number | Title | | | |
| **7** | **SIS modification** | **To make corrections, enhancements, or adaptations to the SIS, ensuring that the required SIL 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 remains 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, 12.5** | **ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02** |
| 10 | SIS FSA | 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 |
| 11 | Safety lifecycle structure and planning | To establish how the lifecycle steps are accomplished | 6.2 | ISA-TR84.00.04 Annex C |

## 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), it is referred to as a safety instrumented function (SIF). The risk reduction required from the SIF is related to one of four discrete safety integrity levels (SILs). The SIS, which executes one or more SIF, is designed and managed according to ANSI/ISA-61511, which establishes requirements necessary to claim a specified SIL.

A critical aspect of maintaining the SIL is the monitoring and management of the automation asset integrity (AAI) of the SIS equipment. Automation failures are often viewed in the process hazardous analysis as binary—either the equipment fails dangerously, allowing a hazardous event to propagate, or fails spuriously, causing a SIS to initiate its SIF. Today's automation practices generally include diagnostics or other monitoring to identify degradation or "misoperation," allowing equipment to be repaired or replaced prior to a functional failure. This technical report is an informative document providing guidance on establishing an effective AAI program that demonstrates through traceable and auditable documentation that the SIS and its equipment is inspected, tested, and maintained in a manner that ensures safe operation of the process.

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

The AAI 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 thorough proof testing are needed for all SIS equipment whether existing or new. While the frequency of these activities may vary due to the required SIL, the intent and purpose of inspection and proof testing are not affected by the SIL.* This technical report provides detailed guidance and examples to support user-specific work processes as part of an overall AAI program.

This technical report provides guidance and examples on the following subjects:

- transferring project documentation;
- selecting the maintenance strategy;
- developing AAI maintenance procedures;
- collecting and retaining maintenance documentation;
- defining personnel roles and responsibilities;
- ensuring maintenance personnel skills and training;
- planning for verification and validation;
- developing a verification and validation plan;
- developing factory acceptance test, loop commissioning, site acceptance test procedures;
- defining a management system and performance metrics;
- implementing configuration management and management of change;
- performing an audit to determine AAI program compliance.

This technical report refers to other ISA publications. This technical report does not repeat or replicate the content of these publications. References are provided when it is felt that the reader should pay particular attention to the publication's more detailed guidance and requirements. For this technical report, the following are considered foundational publications:

- ISA-TR91.00.02-2003, *Criticality Classification Guideline for Instrumentation*
- ISA-TR108.1-2015, *Intelligent Device Management Part 1: Concepts and Terminology*
- ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*
- ISA-RP105.00.01-2017, *Management of a Calibration Program for Industrial Automation and Control Systems*
- ISA-TR96.05.01-2017, *Partial Stroke Testing of Automated Valves*

## 2 Audience

The successful design and management of any SIS is dependent on many departments within an operating facility. Likewise, an effective AAI program is a fundamental element of the SIS lifecycle, with many departments having responsibility. The target audience includes all personnel who have roles and responsibilities that impact the success of the AAI program. Organizations can allocate these roles and responsibilities in different ways depending on site-specific issues, such as the automation complexity or novelty, number of SIFs, technologies used, organizational structure, and resources, and many others. As an example of a larger organization, these roles and responsibilities can be allocated as follows:

- Engineering manager : Ensures that engineering work processes are in place to determine the required rigor of the AAI 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 fulfil 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, and bypassing are adequately addressed in the design phase to deliver necessary functionality across the operations lifecycle, including the 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.
- Process safety 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 competent personnel reviewing and approving proposed changes to the SIS.
- 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 AAI activities, including a training program for operations personnel to maintain qualifications, to take place in a planned manner. Ensures the process is available for SIS testing as per the schedule or evaluates risk and mitigation steps needed if test and inspections are not conducted as scheduled (Refer to 5.2.4) 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. It ensures that competent and trained personnel receive the appropriate level of

support and are available to carry out the identified activities and that SIS installations are maintained, inspected, tested, and operated in accordance with ANSI/ISA-61511.

- Instrument/SIS specialist/engineer: Works with both engineering and maintenance personnel to develop and maintain the SIS equipment list and to define the AAI requirements necessary to ensure the integrity of a SIS throughout its lifecycle. Ensures that SISs are appropriately installed, inspected, tested, and validated to demonstrate correct functionality and performance prior to handover to operations.
- Instrument/reliability specialist/engineer: Advises the instrument/SIS specialist/engineer on appropriate testing and reliability techniques. Applies the management system and ensures that testing activities are performed effectively with appropriate supporting documentation, including procedures and test records. To address any deficiency/failure in a timely and effective manner, including investigation of the root cause in order to reduce the likelihood of reoccurrence. Facilitates data capture and analysis in support of ongoing demonstration of SIS reliability and continuous improvement.
- Maintenance (and construction) supervisor: Understands the importance of SIS AAI and provides the necessary resources to ensure that all identified AAI activities are completed in a planned manner.
- Maintenance (and construction) technician: Understands the purpose and function of the SIS, the importance of preventive maintenance, inspection, and testing plans, and how to complete the required documentation to support data collection.
- Testing personnel: Appreciate the concepts of SIS AAI and the rigor required in the identification and reporting of SIS failures.
- Training coordinators: Ensure that training of all roles impacting or impacted by SIS across the plant operating lifecycle occurs in a timely manner.

It is expected that individuals who are assigned the above roles possess an understanding of the requirements of ANSI/ISA-61511 appropriate to their level of responsibility and technical expectation.

# 3 Definitions of terms and acronyms

## 3.1 Terms and definitions

This clause does not repeat all of the definitions included in ANSI/ISA-61511-1-2018 Clause 3. The definitions for MTTR, MRT, and MPRT are replicated because these terms were added to the latest edition and are used within this technical report. The remaining definitions were developed for this technical report and its sister technical reports, ISA-TR84.00.02 and ISA-TR84.00.04.

### 3.1.1
**application program factory acceptance test (APFAT)**
formal testing of the configuration and the application program to ensure that the configuration and the application program have been developed properly and perform according to the safety requirements specification

NOTE 1 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 SWFAT. Refer to the clause on FAT.

### 3.1.2
**as good as new**
equipment condition in the absence of faults and incipient conditions

NOTE 1 to entry: “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 low compared to the claimed performance and the failure rate expected during the useful life is unchanged.

NOTE 2 to entry: When a device is returned to its “as good as new condition,” the expectation is that the as-left condition will support equipment operation according to the safety requirements specification.

**3.1.3**
**automation asset integrity**
management system assuring automation equipment is inspected, maintained, tested, and operated in a safe and reliable manner consistent with its risk reduction allocation. With regard to SIS, the AAI program collects data on the installed performance of the SIS equipment to demonstrate that the equipment meets the safety requirements specification.

**3.1.4**
**complete failure**
the equipment is unable to operate per the safety requirements specification

NOTE 1 to entry: The failure can be further classified as safe or dangerous depending on the application and desired operation.

**3.1.5**
**degraded condition**
the equipment has a partial loss of function, but is still able to operate per the safety requirements specification

NOTE 1 to entry: A degraded condition is a deviation from “as good as new.”

NOTE 2 to entry: Degraded condition also includes any time a portion of the SIF is bypassed but is still able to perform its function automatically. For example, when one sensor out of three in a 2oo3 voting block is bypassed for testing or maintenance, the other two sensors are still able to activate the SIF.

**3.1.6**
**failure cause**
the circumstances during design, manufacture, or use that led to failure

**3.1.7**
**failure mechanism**
the physical, chemical, or other process, or combination of processes, that has led to failure

**3.1.8**
**failure to activate**
occurs when the SIS does not respond to a process deviation, manual activation, or proof test

**3.1.9**
**fit for service**
capable of continuing operation within equipment specification until the next opportunity to test or perform maintenance

**3.1.10**
**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 ensure that the SIS equipment has been installed and wired properly

**3.1.11**
**integrated factory acceptance test (IFAT)**
formal testing of SIS and BPCS simultaneously, including the interfaces between them, to ensure that the combined actions result in the desired safe automation of the process

**3.1.12**
**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

**3.1.13**
**integrity**
ability of the SIS to perform the required SIF as and when required

**3.1.14**
**maximum permitted repair time (MPRT)**
maximum duration allowed to repair a fault after it has been detected

NOTE 1 to entry: The mean repair time (MRT) may be used as MPRT, but the MPRT may be defined without regards to the MRT:

- An MPRT smaller than the MRT can be chosen to decrease the probability of hazardous event.
- An MPRT greater than the MRT can be chosen if the probability of hazardous event can be relaxed.

NOTE 2 to entry: When an MPRT has been defined it can be used in place of the MRT for calculating the probability of random hardware failures.

**3.1.15**
**mean repair time (MRT)**
expected overall repair time

NOTE 1 to entry: MRT encompasses the times (b), (c), and d) of MTTR.

**3.1.16**
**mean time between failure (MTBF)**
for a repairable device, mean time to failure + the mean time to restoration

**3.1.17**
**mean time to failure (MTTF)**
the average time before equipment's first failure

**3.1.18**
**mean time to restoration (MTTR)**
expected time to achieve restoration

NOTE 1 to entry: MTTR encompasses

- the time to detect the failure (a),
- the time spent before starting the repair (b),
- the effective time to repair (c), and
- the time before the component is put back into operation (d).

NOTE 2 to entry: 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).

**3.1.19**
**obsolescence**
equipment becomes outdated, no longer supported

**3.1.20**
**out of service**
any time period when the SIS equipment is unavailable during an operating mode where the hazardous event can occur

**3.1.21**
**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

**3.1.22**
**pass/fail criteria**
preestablished criteria that define the acceptability of equipment operation relative to the SRS and equipment specification

**3.1.23**
**proof test coverage**

expressed as the percentage of failures that can be detected by the proof test

**3.1.24**
**reliability**
ability of a system or device to perform its specified function under stated conditions for a specified period of time

**3.1.25**
**site integration test (SIT)**
formal testing of the ability of the SIS and BPCS to properly communicate with each other and execute their functions once those systems have been installed in the field, including any third-party systems that need to interface with the BPCS or SIS

**3.1.26**
**useful life**
the portion of equipment's life where the random failure rate can be considered constant

**3.1.27**
**wear-out**
the time when equipment's failure rate begins to increase due to various failure mechanisms

### 3.2 Abbreviations/Acronyms

Abbreviations which are new and not previously documented in ANSI/ISA-61511 are indicated with (*)

| | |
|---|---|
| AAI* | Automation asset integrity |
| 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 workstation |
| FAT | Factory acceptance test |
| FMEA* | Failure mode and effects analysis |
| FSA | Functional safety assessment |
| 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 |
| MOC | Management of change |
| MPRT | Maximum permitted repair time |
| MRT | Mean repair time |
| MTBF* | Mean time between failure |
| MTTF* | Mean time to failure |
| MTTR | ANSI/ISA-61511-1-2018 changed mean time to repair to mean time to restoration |
| MTTR | Mean time to restoration |
| MTTRes | Acronym changed to MTTR |
| 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 |
| PFH | Average frequency of failure |
| 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 |
| 2oo2 | two-out-of-two |
| 2oo3 | two-out-of-three |

## 4 AAI planning considerations

For safety instrumented systems (SISs), planning is covered in ANSI/ISA-61511-1 Clauses 5, 6, 7, 13, 14, 15, 16, and 17. Automation asset integrity (AAI) planning involves establishing the management system and the maintenance requirements (e.g., preventive maintenance, inspection, 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 related. Fundamentally, all equipment is covered by AAI, but only a subset of the equipment is rigorously managed according to ANSI/ISA-61511. Classification is performed and documented during the process hazards analysis as discussed in the standard ANSI/ISA-84.91.01. The AAI program should cover all equipment required to support the safety instrumented function (SIF) integrity and reliability, including sensors, logic solvers, final elements, utilities, communications, and diagnostic equipment.

The facility safety and operating expertise should be considered when designing the SIS, because technical proficiency affects the AAI program, which must be capable of supporting the SIS functional and integrity requirements defined in the safety requirements specification (SRS).

Once a SIS is designed and implemented, its independence, integrity, functionality, and reliability become inherent attributes of the installation. These attributes are proven through periodic AAI 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-61511 lifecycle includes setting the requirements for procedure development and personnel training needed to support AAI program effectiveness. Examples of the types of activities include

- documentation handover 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,
- performing preventive maintenance,
- minimum required inspection practices to maintain equipment AAI,
- minimum required proof testing effectiveness to ensure correct operation of equipment,
- managing SIS degradation and failure conditions identified during plant operation, inspection, diagnostics, 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 requirements and limitations for operating environment conditions,
- 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 AAI 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 functional requirements of the SRS before 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. A FAT allows rigorous testing of the equipment in a controlled environment without the time pressure that often occurs during the site acceptance test (SAT). ANSI/ISA-61511 contains requirements for executing the FAT. 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 equipment (e.g., air supplies, power supplies, climate controls, 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 that the installed SIS operates as specified.

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 on a fixed schedule is conducted to replace wearable or short-life parts to extend the useful life of the equipment. Inspection and proof testing are required to demonstrate that the SIS equipment is operating as specified and to identify deviations from acceptable operation, so they can be corrected through predictive or reactive maintenance. Test records provide documented proof that the SIS equipment is capable of supporting the claimed performance. All SIS equipment should be tested, including field sensors, final control elements, logic solvers, human-machine interfaces (HMI), communication links with other systems, interconnecting wiring and terminations, the user

application program, and any required ancillary equipment, such as power, instrument air, or climate controls.

It is also essential to consider the expected useful life when defining the AAI plan for the equipment. As the equipment approaches wear out, the failure rate assumptions used to determine the testing schedule can become invalid. Continuing to use the equipment indefinitely is equivalent to adopting a reactive maintenance strategy. Initially, the AAI plans may adopt a replacement (rebuild/refurbishment) interval based on the manufacturer's recommendations. However, as the facility collects the necessary body of prior use data to support the claimed performance for the existing SIS, the demonstrated performance can be taken into consideration to extend or reduce the replacement interval.

Many processes have operating cycles that are longer than the test interval necessary to theoretically achieve the safety integrity level (SIL). Therefore, the ability to perform testing while the process remains in operation (i.e., on-line) is often desirable. The requirements of ANSI/ISA-61511 can be met using off-line testing with the process in 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-61511.***

Effective AAI planning ensures that the maintenance strategy is consistent with maintaining the SIS integrity. The SIS AAI plan should be a component of the facility's overall AAI 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. AAI planning includes the development of procedures on how to plan, perform, and document the following:

- preventive maintenance;
- diagnostics monitoring;
- inspections;
- calibrations;
- proof tests;
- spare parts management;
- repairs;
- reliability data capture and analysis;
- loop check/commissioning procedures;
- validation procedures;
- feedback to ensure continuous improvement.

There are several considerations that go into developing a holistic AAI program that ensures proper scheduling and completion of preventive maintenance, inspections, proof tests, and reliability improvement tasks. Each of these considerations is discussed in more detail in later clauses:

- identification of the equipment and systems to be covered by SIS AAI;
- determination of the maintenance strategy to be used for each type of equipment;
- development of AAI procedures;
- 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 AAI program compliance.

### 4.1 Transferring project documentation to maintenance

The design documentation should be transferred to the organization responsible for the facility's maintenance and records system, so that this documentation is available to maintenance personnel. Examples of the types of information needed for the AAI program are:

- 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 equipment should also be identified in the maintenance management system to ensure calibration certifications are performed as required.
- location description (e.g., T-630 discharge);
- SIS instrumentation data sheet number;
- 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 of SIS equipment;
- SIF identification number;
- voting architecture and existing comparison (e.g. external diagnostics);
- device diagnostic software (if applicable) and firmware version;
- wiring details;
- date installed;
- calibration, tolerance, and configuration values (e.g., span, filtering, square root extraction, fail-direction on detected fault, leak tightness);
- preventive maintenance intervals and procedures;
- inspection/proof test intervals and procedures;

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

  NOTE Ancillary equipment can be a major contributor of common cause to equipment failure across a site.

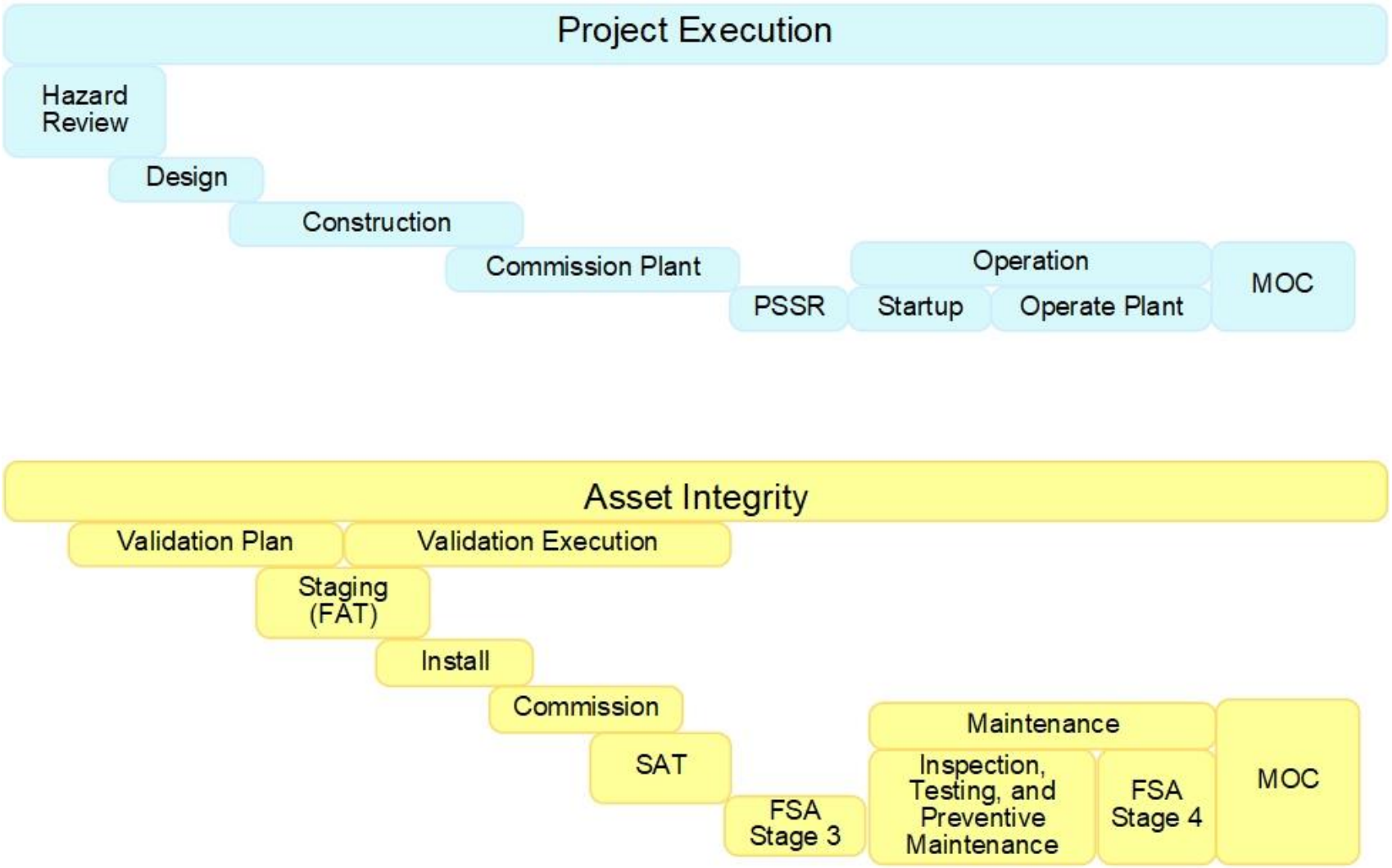



**Figure 2 – Automation asset integrity across the lifecycle**

The figure shows conceptually where the AAI program and its specific activities fit into an overall project and subsequent plant operation. FSA Stages 3 and 4 involve a review of the maintenance records and findings.

### 4.2 Selecting the maintenance strategy

The AAI plan ensures that the facility maintenance strategy is in agreement with the intent of the SIS AAI program—that the equipment is maintained in the “as good as new” condition through its lifecycle. As shown in Figure 3, there are three basic maintenance strategies employed within the process industry, depending on the type of equipment:

- Preventive maintenance: Maintenance is performed proactively to detect and correct incipient faults and degraded conditions prior to complete failure of one or more specified device functions. The intent of this strategy is to avoid significant loss of function from known degradation mechanisms and the resulting need for reactive maintenance.
  - Preventive maintenance is performed on a fixed schedule, e.g., annual change out of air supply filters on automated valves.
  - Preventive maintenance can also be referred to as planned preventive maintenance (PPM), “proactive maintenance,” or “fixed schedule maintenance.”
- Predictive maintenance, also known as “condition-based maintenance”: Applicable maintenance is initiated based on monitoring the condition of the equipment or particular equipment components through diagnostics, scheduled tests and inspections, and performance observation. For example, operations might observe that the valve response to the control signal is sluggish, indicating that an air filter change out might be required. The intent of this strategy is to detect and correct degradation prior to complete functional failure of the device.
- Reactive maintenance, also known as “run to failure” or “corrective maintenance”: No preventive nor predictive maintenance is performed. Repair or replacement is initiated based on detecting complete functional failure of the device. This detection may be the result of a failure upon demand, a failure discovered during testing, spurious process impact, or a complete failure detected through diagnostics.

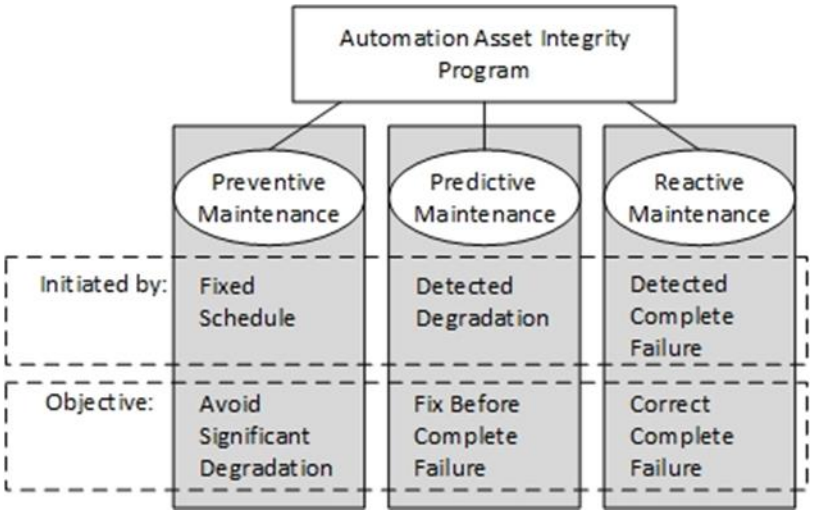



**Figure 3 – Automation asset integrity program activities**

Though a viable strategy for some general equipment populations, reactive maintenance strategies for SIS equipment should consider the effect on the SIS performance. Use of reactive maintenance strategies on subsystems with hardware fault tolerance and high diagnostic coverage may be acceptable, whereas these strategies may not be appropriate for subsystems with no hardware fault tolerance or diagnostics. A reactive maintenance approach significantly increases the likelihood of the SIS failing to operate as required when required.

Preventive and predictive maintenance strategies ensure equipment is not run to failure for slower degradation mechanisms or to allow timely reaction to detected faults as appropriate. Unexpectedly frequent occurrences of complete failure should be promptly investigated, and action taken to minimize reoccurrence. In cases where there is insufficient prior use data accumulated to provide confidence in the reliability parameters used to determine preventive and predictive maintenance intervals, fault-tolerant architectures should be strongly considered to avoid unintended run-to-failure performance. In all cases, the device installation design should conform to the maintenance strategies deemed necessary for the application. Some inputs that influence the development of the AAI strategy or installation design for a device include

- device failure modes,
- bypass strategies,
- repair strategies, and
- deferral practices.

### 4.2.1 Device failure modes

Once facilities are commissioned and placed into operation, equipment and systems begin to degrade due to a variety of mechanisms. For SIS, a rigorous AAI 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. 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 no longer “as good as new” when the automation asset integrity records show increasing failure or wear out.

Determining which type of maintenance inspection, testing, diagnostics, or component replacement activities are reasonable to include in the strategy for a given device requires understanding how the device fails. Certain degradation mechanisms can happen so rapidly that even on-line diagnostics with a high scan rate will be insufficient to respond to the degradation before full functionality is lost, whereas others are so slow that even the relatively long proof test intervals will be sufficient to identify them. Refer to Table G.1 for further details.

Failure mode is defined as the observed manner of failure. 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. 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. Automation equipment can be used to execute different types of functions in various applications, so the impact of a particular failure mode is unique to the application. 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.

> As an example of the above, a transmitter can be used to measure flow in a process where high and/or low flow can cause hazardous conditions. If the failure results in a high output, the low trip will fail. If it results in a low output, the high trip will fail; the failure is dangerous in either direction. 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 deenergize-to-trip. Where ventilation fan output or flow from fire water pumps are required during a demand, the fan or pump motors must remain energized to perform the safety function. In such a design, a loss of the electrical supply to the motor would be dangerous.

Once the impact of each failure mode has been determined for a specific application, 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 AAI program.

As an example for a final element, Table 2 contains a list of failures and failure modes for a remote actuated valve.

**Table 2 – Remote actuated valve failure modes**

(Excerpted from CCPS PERD Remote Actuated Valve Taxonomy)

| **Complete failures** | **Incipient Conditions** |
|---|---|
| • Fail to closed position<br>• Fail to open position<br>• Fail to close on demand<br>• Fail to open on demand<br>• Frozen position<br>• Valve rupture<br>• Seal/packing blowout<br><br>**Partial Failures**(1)<br>• Reduced capacity<br>• Seat leakage<br>• External leak<br>• External leak – Body/Bonnet<br>• External Leak – Packing/Seal<br>• Fugitive emission<br>• Controlled variable high<br>• Controlled variable low<br>• Fail to hold position<br>• Unstable control (hunting)<br>• Responds too quickly<br>• Responds too slowly<br>• Excessive noise | • Body cracked<br>• Body eroded<br>• Body corroded<br>• Body material wrong<br>• Guide fouled<br>• Guide galled<br>• Guide corroded<br>• Guide worn<br>• Stem fouled<br>• Stem galled<br>• Stem corroded<br>• Stem bent<br>• Stem worn<br>• Seat fouled<br>• Seat cut<br>• Seat eroded<br>• Seat corroded<br>• Seat excessive wear<br>• Seat (soft) embedded debris<br>• Seat (soft) overheat evidence<br>• Seat loading mechanism dysfunctional<br>• Spring cracked<br>• Spring corroded<br>• Spring fatigued<br>• Spring rubbing<br>• Excessive vibration |

(1) This technical report refers to partial failures as degraded conditions, because it requires an analysis of the particular SIF to know whether these conditions are considered a functional failure.

### 4.2.2 Bypass strategies

A 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 by various means, such as the signal is forced; the terminal wiring is jumpered; the trip settings are changed such that the trip will not occur; the valve is clamped; or the valve is physically bypassed, blocked in, or bypassed using software. 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.

Bypassing of devices can be reviewed and approved using a bypass permit process or the site management of change (MOC) process. The bypass permit process is typically used when the anticipated bypass period is within the mean time to restoration (MTTR) specified in the SRS. The permit process generally involves review of the current process operational status, implementation of compensating measures, approval by management, and communication to operations. A more detailed MOC process should be initiated when the bypass period is expected to exceed the MTTR.

Bypasses are sometimes required during plant startup due to the required SIF functionality, e.g., low flow cutoff for a pump. Bypasses are often necessary to allow maintenance or testing to be performed while the process is still operational, reducing downtime required for testing and 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 can be considered acceptable, as long as their use is controlled, and the risk is properly managed. For this reason, an analysis of the increased risk during bypassing should be performed. This analysis should 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. Whether or not a compensating measure exists to manage the risk and the expected duration of bypass needed for the AAI maintenance can influence the type of AAI strategy chosen for a particular application.

Bypasses increase the potential for systematic errors. SIFs inadvertently left in bypass are not available to operate when a process demand occurs, so bypass periods should be tracked and minimized. The use of any bypass should be covered by procedures, administrative controls, access security provisions, and confirmation of return to service, as appropriate.

### 4.2.3 Repair strategies

Repair work is performed to correct revealed faults in a timely manner. Typical preventive and predictive strategies for SIS AAI assume that the correction of degradations will be done as soon as it can be scheduled and safely executed and certainly before full functional failure would be anticipated. Repairs executed per reactive strategies, or when a functional failure is found during preventive or predictive maintenance, are expected to be completed within the maximum restoration time indicated in the specification.

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

a) Sensor: Exercise sensor input and verify that alarms, diagnostics, and trip set points are correct. Use the applicable section of the SIF test procedure, and complete the required documentation for the equipment checked.

b) Final element: Exercise all outputs that actuate final control elements, and observe output actions. Verify that 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.

c) 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 a test of the affected hardware, application program, or configuration to ensure proper operation, and complete the required documentation.

### 4.2.4 Deferral practices

AAI strategies and the designs that support them should be developed so that the potential need to defer preventive, predictive, or reactive maintenance is an exceptional event, not a matter of routine. Deferrals can be handled using the management of change (MOC) process or by approved procedure. Deferrals should undergo technical review to ensure the company's risk criteria is being met. In the event that the company's risk criteria would not be met, then temporary compensating measures should be put into place until the protection is returned to the "as good as new" condition.

The most common AAI 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 before the equipment is 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 preapproved procedure or through plant MOC at the time that the deferral is needed. “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 delaying SIS inspection, test, and repair, and approve deferments on a case-by-case basis.

Probability of failure of a SIF increases as a function of time. The longer the proof test interval, the higher the probability of failure, 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, increases the probability that the SIS equipment fails to operate as required when required. 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 would increase the process safety risk unacceptably. However, the strongest basis for the extension is not the calculation, but rather it is the confidence that the SIF equipment is in good enough condition to continue to provide the necessary risk reduction. If the actual SIF performance does not support extending the test interval, compensating measures should be considered to address the deferral risk.

Industry best practice is that deferrals be approved and authorized by competent personnel who are accountable for safe operation. This competence includes understanding 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, the AAI strategy may indicate 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 3.

**Table 3 – 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. |

### 4.3 Developing AAI maintenance procedures

The effectiveness of the SIS AAI strategy will depend on having written procedures for the AAI maintenance activities.

Technical content of the AAI maintenance procedures should include clear instructions regarding

- pass/fail criteria for failure modes,
- end of useful life criteria,

- human factors for AAI maintenance activities,
- safe use of bypasses,
- response to degradation and faults,
- analysis of as-found/as-left data, and
- failure investigation.

### 4.3.1 Pass/fail criteria

Clear pass/fail criteria should be established for each of the failure modes, particularly those that are deemed dangerous for the application the device is in. Pass/fail criteria determine when the failure mode results in the equipment not being capable of operating as needed. For all maintenance strategies, the pass/fail criteria are derived from the functional requirements in the SRS. Failure modes and pass/fail criteria are established for each piece of equipment, and the maintenance procedures should be written so that parallel paths within the SIS are individually tested.

Well-defined pass/fail criteria ensure 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 the as-left condition will support operation within specification until the next scheduled proof test.

### 4.3.2 End of useful life criteria

AAI procedures defining the preventive maintenance, diagnostics monitoring, inspection, and proof test activities should contain clear criteria for determining when equipment requires replacement or rebuild. As reliability data is captured and analyzed, preventive and predictive maintenance intervals may be adjusted. AAI records document the acceptability of equipment operation. The as-found condition provides evidence of the equipment operation at the initiation of the AAI 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. See 5.2.5 for additional guidance on useful life management.

### 4.3.3 Human factors for AAI maintenance activities

Incidents have been caused by many different systematic errors involving AAI maintenance activities, including:

- inadequate access;
- incorrect or missing labeling;
- poor lighting;
- lack of documentation, such as specifications, narratives, and manufacturer’s manuals;
- documentation is not as built;
- inadequate test coordination with operations;
- inadequate return-to-service procedure;
- inadequate communication and coordination with adjacent operations and maintenance personnel who were unaware of the test being conducted and the effect of testing on their situation;
- improperly installed SIS equipment;
- improper bypassing;
- poor test facility design;
- misunderstood or incomplete test procedures;

- lack of personnel competency and training.

Specific procedural errors that commonly occur during SIS maintenance include:

- beginning a test without satisfying the pretest conditions;
- attempting to start up when a test is still in progress;
- violations of lockout/tagout;
- not documenting that a physical bypass is being put in place;
- leaving physical jumpers in place;
- 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, AAI procedures should be clearly documented and personnel 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 testing.

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.

### 4.3.4 Procedures for safe bypassing

Some AAI preventive and reactive maintenance strategies may require bypassing SIS equipment. 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”). Bypass safe work practice requires documentation of the installation and removal of each bypass. For each bypass, test procedures should specify 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

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

#### 4.3.5 Responding to degradation and faults

As faults are found and corrected during execution of an AAI maintenance procedure, 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.

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. Negative findings should be communicated to the site reliability engineer. A return-to-service procedure should be followed to ensure that operations confirms that the equipment is functioning as expected and that any bypasses have been removed.

#### 4.3.6 Analysis of as-found/as-left data

Procedures also need to be developed for periodic analysis of the data captured during execution of AAI maintenance activities against the specified performance requirements or design assumptions. The performance analysis procedures should ensure that repeat maintenance offenders, such as repeat work orders to address performance issues, are investigated and action taken to minimize failure. These actions may include changing the AAI plan, such as shortening the test interval, or even reevaluating the design, specification, or installation.

### 4.4 Collecting and retaining lifecycle documentation

As part of the AAI 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 needed 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, 5.10);
- 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).

Some documentation management system considerations that can have a significant impact on the sustainability of the AAI program are:

- addressing the multidisciplinary aspect of AAI documentation development;
- collection of as-found/as-left data;
- AAI document retention

### 4.4.1 Multidisciplinary AAI documentation development

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 use and maintain the various documents described within the technical report. The AAI 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, and the role(s) or person(s) who will maintain the master documents as evergreen. The AAI 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.

### 4.4.2 Collection of as-found/as-left data

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

As-found information is critical to understanding the actual degradation or failure rate of the equipment for different failure modes. For a successful test, as-found information 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 any troubleshooting or corrective action. For example, a valve that did not move upon the initial request to do so has a “failed stuck” as-found condition, even if the valve subsequently moves after repeated stroking attempts. When the as-found condition does not meet the design intent, corrective action should be taken, and previous AAI 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 AAI plan can be identified to reduce the likelihood of reoccurrence.

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 cross-check 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.

### 4.4.3 AAI document retention

All operating facilities should comply with their respective corporate records retention guidelines and policies. The records may be maintained electronically or as hard copies in on-site or off-site storage. AAI records are needed for tracking and trending equipment failure, and retention

intervals should be selected to support this activity. These records are also typically reviewed whenever a functional safety assessment (see ISA-TR84.00.04, Annex D), prior use assessment (see ISA-TR84.00.04, Annex L, L.6) or audit (see ISA-TR84.00.04, Annex E) is performed. Regulatory authorities may establish the minimum retention period for AAI records. For example, OSHA PSM requires that records 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.

### 4.5 Defining personnel roles and responsibilities

AAI planning also ensures that personnel understand their roles and responsibilities in supporting the maintenance strategy. Maintenance/reliability personnel have a significant role in AAI 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 AAI 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 engineers 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 AAI 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.

### 4.6 Ensuring maintenance personnel skills and training

This subclause specifically addresses the skills and training necessary for maintenance personnel who support SIS AAI. Maintenance training includes maintenance management that directs and funds the maintenance activities, the instrumentation technicians, the electricians, and the mechanics. Maintenance personnel need to understand 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 vocational schools offer programs covering different technical skills, such as PLC configuration or field instrumentation. There are many resources available to a user who is developing a training program, for example: ISA Certified Control Systems Technician Program and ISA-67.14.01-2000, *Qualifications and Certification of Instrumentation and Control Technicians in Nuclear Facilities*.

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

- use of safety-approved equipment for repair or replacement;

- use of approved and standardized equipment, such as calibration equipment;
- permitting;
- bypassing;
- preventive maintenance activities;
- instrument diagnostics interpretation and response;
- inspection and testing;
- understanding pass-fail criteria;
- documenting as-found/as-left;
- recording and reporting failure;
- recognizing common-cause failure;
- management of change, including configuration management;
- 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.

### 4.7 Planning for verification and validation

Prior to maintaining automation devices in “as good as new” condition, the devices must be installed and configured correctly to begin with. Systematic errors that occur after the approved design of the instrumented safeguards can result in a well-maintained system that nevertheless will fail to perform. Verification and validation are the lifecycle activities used to ensure that these systematic errors are identified and corrected before the hazards are present.

Process control, operations, design engineering, and maintenance personnel are involved in developing the verification and validation plan and procedures. SIF verification activities (such as the factory acceptance test [FAT] and loop commissioning checks) are intended to demonstrate that a portion of the SIS construction and installation work have been completed to the extent appropriate for that phase of the project. 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 startup. Validation tests should also include specified operating conditions and requirements of any other ancillary equipment (e.g., climate control). 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 auxiliary equipment have been installed. The validation or functional test of the SIF is performed by using interfaces to the field sensors to simulate the process deviation that activates that SIF 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). 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 is essential to confirm that validation is complete and the facility is ready to operate. Any deviations need to be managed according to a validation plan.

### 4.8 Developing a verification and validation plan

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;
- logic narratives;
- requirements specified for ancillary equipment;
- cause and effect matrices and loop drawings for maintenance troubleshooting;
- SIF I/O and set point list.

This information should be consistent and accurate, and one set of documentation should be considered as the 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. For this reason, the plan should ensure that all the verification procedures are scheduled to be completed before validation. To avoid unnecessary delays in startup, verification activities can, and should, be completed as soon as the documents, devices, or systems being verified are available. Sufficient time in the schedule should be allowed to ensure deficiencies found during the commissioning/loop check phase or other verification activities have been repaired prior to the start of validation. This reduces the potential for unforeseen delays during the validation execution.

### 4.9 Developing factory acceptance test (FAT), loop 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. Testing should cover all functional requirements to ensure that the SIS operates consistently with the SRS. Test protocols should guarantee the required detailed aspects to prevent any challenge and also should include a scoring list for executing/witnessing all safety-related testing activities that may negatively affect the results and final approval of the overall test.

#### 4.9.1 Factory acceptance test

When a FAT is identified in the planning stage of the lifecycle, ANSI/ISA-61511 defines the requirements for performing the FAT. The FAT may be conducted for any portion of a SIF or on the entire SIS. The logic solver FAT can be conducted with simulated inputs, physical switches, analog dials, or simulation software. In general, FATs are conducted on vendor-packaged systems, hardwired panels, and PE logic solvers. Vendor-packaged systems can include valve and actuator assemblies, burner management systems, and high integrity protective systems. A FAT is routinely performed for programmable electronic (PE) systems, where it may involve an integrated test of the SIS logic solver and the basic process control system (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.

A 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 functions 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:

a) 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.

b) 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.

c) 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 nonsafety actions or trips performed in the BPCS to aid operations in restarting the unit after a trip. For example, a typical action might be putting a control loop in manual and moving the control valve to the safe state upon the trip of a 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,<br>sometimes referred to as the HWFAT<br><br>(specific hardware version test) | Verify supplier tests were completed and met effectiveness requirements.<br>Test and verify all SIS equipment/ components before field installation.<br>Establish a basis in case problems/ defects show up in field. | Minimize product defects and manufacturing errors. | Reduce startup and commissioning time. | Ensure system will perform its safety shutdown functions on demand.<br><br>Reduce startup and commissioning time. |
| (2) SIS configuration and application program checkout,<br>sometimes referred to as the SWFAT<br><br>(specific application program version test) | Effectively test and verify all design, SIS configuration and application program work before field startup/ commissioning. | Test and verify applicable functional aspects of risk reduction requirements. | Assure that engineering support and operations personnel agree that the SIS configuration meets the application requirements. | Reduce startup and commissioning time. |
| (3) “Open” SIS<br>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 startup and commissioning. | Reduce startup and commissioning time. | |

The tests listed below can be a specific subset 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 minimum tests conducted as part of a 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 that 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 the 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.
- When an asset management system is included in the scope, communication to the asset management system and its interfaces needs to be confirmed.
- 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 an I/O power supply that does not have a back-up system for loss of power, confirm external signal wiring (e.g., as 24 VDC discrete input or voltage input) into the control system and verify the loop power.
- Perform a 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 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 workstation (EWS) needs to be confirmed. The EWS is defined as the main configuration station that has application program and I/O configuration capability. Occasionally, the EWS also has HMI-console capability.

- The site integration test (SIT) is the formal testing of the ability of the SIS and BPCS 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.

### 4.9.2 Loop 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 the site acceptance test) can be completed. Table 4 provides an illustration of the conceptual work process.

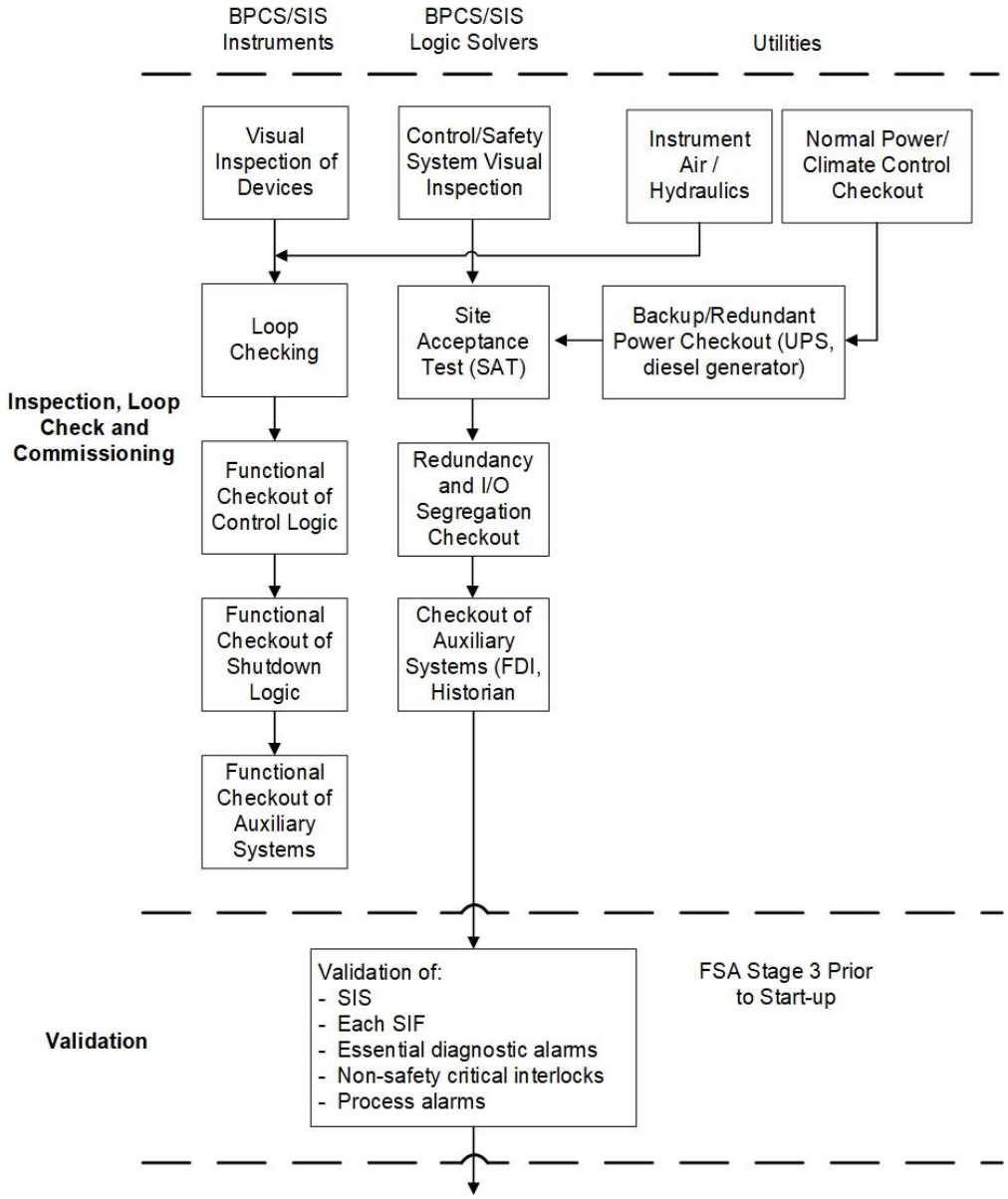



**Figure 4 – Validation flowchart**

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 “recommissioning” the instrument. In some cases, physical inspections may be performed on skidded equipment while still at the supplier’s site if appropriate. Equipment should be physically inspected after installation to ensure no damage was done during transportation or installation.

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

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

The emergency backup power (e.g., uninterruptible power supply [UPS], battery banks, auxiliary generation, transfer switch) 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 so there is not any undue load from noncritical 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 for appropriate fault response and diagnostics. The interfaces between the SIS and the backup power systems need to be checked for functionality to the greatest extent possible. Functionality tests should be initiated at the backup 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&IDs) 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.

### 4.9.3 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 sufficient, precise, and approved 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. When the scope of the SAT is reduced based upon the successful completion of a robust FAT, care must be taken to track application program revisions between the FAT and validation completion. Logic changes made after the FAT should be tested on site.

The validation procedure must still prove that the SIS as installed in the operating environment performs all the requirements of each SRS. For example, a SIF with a standard fail-safe 2oo3 (e.g., A/B/C) sensor architecture, in which detected sensor failure or a manual bypass of the sensor would also count as a vote to trip, would have 27 unique combinations for triggering the safe action. To verify the application program has been configured correctly, a robust FAT would test all 27 combinations. If the detailed documentation of the FAT confirmed the architecture was correctly configured in the application program and there was proof that the application program in the installed SIS was identical to the one tested in the FAT, the procedure for the SAT might consider reducing the trip function testing to the combinations necessary to prove that each type of trip functionality worked as specified. Care would be taken to ensure that the combinations in total would include a trip vote, a detected failure vote, and a bypassed signal vote from each of the sensors. The FAT would still need to include tests of any specified manual trip, full function bypass, or any other feature that would be dependent upon the correct interaction between the field hardware, the application program, and any auxiliary systems.

The overall project plan should include the SIS design and construction activities affecting 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 a SIF has taken action;
- indication of SIF bypass;
- operation of manual shutdown facilities;
- operation of resets;
- indication of SIS ancillary equipment loss;
- failure of environmental conditioning equipment, which supports the SIS;
- response time;
- criticality requirements, such as valve shutoff tightness and closure speed.

All ancillary 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;
- utility equipment (instrument air, instrument power);
- climate controls.

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 sign-off 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.

Completion of the SIS validation does not approve the SIS for handover to operations on its own. A Stage 3 FSA and a pre-startup safety review should be completed prior to handover. Stage 3 FSA is covered in detail in ISA-TR84.00.04, along with the other FSA stages. With respect to the AAI program, FSA 3 verifies test completion, finding resolution and record retention.

**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.<br>Possesses a detailed understanding of ANSI/ISA-61511-2018. |
| **Construction or Maintenance Supervision/Technician** | |
| **Responsibility** | **Qualifications** |
| Representing 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.<br>Possesses a working understanding of ANSI/ISA-61511-2018. |
| **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).<br>Possesses an awareness of ANSI/ISA-61511-2018.<br>Independent of the project team and should have had no involvement in its execution. |
| **Management Team Representative** | |
| **Responsibility** | **Qualifications** |
| Approval of the individuals who 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.<br>Possesses a basic awareness of ANSI/ISA-61511-2018. |

## 4.10 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 an SRS where SIF functional and AAI requirements were specified. The SIL verification calculations made assumptions about the failure modes and failure rates of the SIS equipment. Assumptions made for failure modes and failure rates imply that SIS equipment operate under the specified environmental conditions, e.g., sensor fouling, high humidity, high temperature, polymerization.

A health and safety executive (HSE) study found that 32% of loss-of-containment events in the process sector (excluding refineries) were caused by equipment or process failure, due to inadequate design (28%) and maintenance (30%) (HSE, 2005). Safety equipment performance is limited by the rigor, timeliness, and repeatability of AAI 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.

### 4.10.1 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.

### 4.10.2 Performance metrics

The success of the AAI program is proven by its AAI data, which demonstrates that the SIS can achieve the performance assumed during the process hazards analysis. Significant degradation found during preventive maintenance may reveal the need to change the preventive maintenance frequency. Diagnostics monitoring, inspection, 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 AAI 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. This analysis should include the complete SIS, including the performance of specified auxiliary equipment. Repeated SIS failures indicate that the AAI program is not achieving its intent—to maintain the SIS equipment in the “as good as new” condition.

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 reoccurrence. “Annex B – Example demand logs” provides examples of demand logs and trip reports. “Annex C – Example failure reports” provides examples of device failure reports.

ISA-TR84.00.04 Annex R provides a table of metrics that can be used to track and trend SIS performance. Multiple trending metrics are included in ANSI/ISA-61511, such as

- process demands,
- time in bypass,
- mean time to restoration,
- dangerous failure rate, and
- spurious trip rate.

The data necessary to perform reliability analysis can come from many different tasks, such as inspection, preventive maintenance, tests, and fault response. The most difficult part of instituting reliability improvement is the culture change necessary for data capture and classification, which must be supported by maintenance and operations personnel. Training and positive reinforcement 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.

### 4.11 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. Because 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 operating environment conditions;
- changing the SIS equipment specification;
- changing the manufacturer or model of SIS equipment;
- modifying SIS equipment installation details (e.g., auxiliary equipment configuration);
- changing the SIS alarm or trip set points;
- changing SIS equipment firmware;
- changing the SIS application program;
- modifying the intervals or procedures for SIS preventive maintenance, diagnostics monitoring, inspection, or proof test.

### 4.12 Monitoring performance of a new or modified SIS

The earlier systematic design errors are identified, the less likely there will be process impact. Project planning should include post-startup monitoring of the performance of a new or modified SIS. Monitoring runs for a defined period of time, often dependent on the novelty of the technology used in either the process or SIS. A monitoring period of 90 days to one year is typical. Then, the SIS becomes subject to periodic FSA Stage 4 and management of change with FSA Stage 5. Refer to ISA-TR84.00.04 for more guidance on FSA.

The intent is to monitor for device failures during the initial phase of operation when the failure rates are expected to be highest. Operation records are also monitored closely for device faults, alarm errors, and unnecessary alarm generation from field devices and wiring.

> For example, in the early installation, hidden specification errors can become apparent, such as incorrect trip set points, calibration ranges or process calculations (e.g., orifice plate and meter sizing). Verify that the operating environment is not causing premature failure or degradation of the equipment performance, e.g., deposition in or plugging of the process connections for input devices. Check to ensure that spurious trips are not occurring because normal operation is “too close” to the trip setpoints.

### 4.13 Performing audits to determine AAI program compliance

ISA-TR84.00.04 Annex E provides guidance on developing and implementing an auditing program to ensure ANSI/ISA-61511 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 the 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 three-to-five-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 to specific personnel or departments for correcting deficiencies.

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

## 5 AAI maintenance activity considerations

The automation asset integrity (AAI) program is intended to ensure that safety instrumented system (SIS) equipment is maintained in the “as good as new” condition throughout its installed life. AAI 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 AAI program is required to detect degraded conditions and complete failure so that these 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 AAI program also includes preventive maintenance activities.

When equipment is known to have consumable components (e.g., batteries, catalytic bead sensor), preventive maintenance activities ensure that these components are replaced on a periodic basis. Inspection and automated diagnostics can identify degraded device conditions, triggering maintenance. Preventive maintenance, diagnostics monitoring, and inspection complement periodic proof testing, which is necessary to identify undetected failures prior to a demand being placed upon the safety instrumented function (SIF). Together, AAI activities increase the likelihood that the SIS operates correctly throughout its installed life.

There needs to be a process in the AAI program to address identifying when a device becomes obsolete and what the acceptable replacement would be. When a device in active service becomes obsolete, it does not mean the device needs to be replaced immediately. Reviewing and approving the new device may be performed ahead of the replacement, identifying the device configuration, installation, and documentation requirements. This will minimize the impact to the process when a failure occurs.

Without a sound AAI program incorporating preventive maintenance, appropriate response to diagnostics, periodic inspection, and proof testing, one risks running equipment to dangerous failure. Inspection and proof testing are conducted to

- meet regulatory requirements,
- meet ANSI/ISA-61511 requirements,
- meet equipment manufacturer requirements (e.g., safety manual),
- demonstrate through witnessed test, preventive maintenance records, and predictive maintenance records that the equipment is being maintained in the “as good as new” condition,
- detect and correct unrevealed failures,
- verify that the AAI program and test interval are sufficient to ensure that functional and integrity requirements are met for the equipment life,
- monitor equipment for degradation mechanisms, which may compromise future performance,
- identify when equipment has reached wear out and requires replacement, and
- provide data and information to facilitate the evaluation of AAI program success and to support continuous improvement.

It is essential that equipment be maintained such that it meets the functional and integrity requirements defined in the safety requirements specification (SRS). Inspection and preventive maintenance programs are necessary for achieving the equipment’s assumed performance criteria in the safety integrity level (SIL) verification calculations. The lack of a good AAI program for the SIS devices and associated ancillary equipment (e.g., 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 nonsafety equipment. Understanding how to judge pass/fail criteria and the current condition of the equipment is critical to AAI program success. Before one can define pass/fail criteria, it is necessary to understand the critical failures and failure modes with respect to the required SIF performance. A significant activity within the AAI 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.

AAI 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 as chronological a 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 AAI 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, and random equipment failures. For the overall AAI program to accomplish its mission, the personnel involved need to be sufficiently competent to successfully execute the AAI activities.

This clause provides guidance related to the following AAI maintenance activities:

- planning and performing preventive maintenance;
- planning and performing predictive maintenance;
  - response to diagnosed degradation;
  - planning and performing inspections;
  - planning and performing calibration checks;
  - planning and performing proof tests;
  - managing useful life;
- planning and performing reactive maintenance;
- planning and performing reliability analysis.

### 5.1 Planning and performing preventive maintenance

As described in 4.2, preventive maintenance is performed according to a fixed schedule. Preventive maintenance can 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. Often achieving the manufacturer's indicated useful life for SIS devices is dependent upon performing prescribed preventive maintenance activities. For example, the failure rate of a linkage may be quite different in the case of periodic oiling (i.e., preventive maintenance) versus no oiling (i.e., reactive maintenance).

Inputs to preventive maintenance planning include manufacturer recommendations and past experience with the equipment in similar operating environments. The information on past experience (i.e., prior use data) confirms how 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.

### 5.2 Planning and performing predictive maintenance

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 test activities are often supplemented with other predictive maintenance tasks. As the time interval between periodic proof testing is increased, there is a need to improve the effectiveness of these additional maintenance activities.

As described in 4.2, predictive maintenance is typically performed in response to degradations found during scheduled inspections, from on-line diagnostics, or as a result of operations noticing the impact of the degradation on the process operation. Routine visual inspections can often

uncover incipient faults and degraded conditions, allowing them to be corrected before complete failure occurs.

In addition, today's SISs employ a great deal of diagnostics, which support predictive maintenance based on the observed condition of the equipment. Whether the diagnostics can support sustained device performance is dependent on the correct implementation of device and host configurations, adequate alarm and alert interfaces, fault-tolerant application programs, routine monitoring of diagnostic notifications, timely use of response procedures, and robust administrative control programs.

Whether or not predictive maintenance activities may be used to change the interval or procedure content of proof tests, modify the SIL verification calculation, or change the spurious trip rate estimate is dependent upon a number of factors. Whether the defect can be corrected and the process returned to normal operation without process impact or immediate shutdown is dependent on whether the diagnosed defects

- can be responded to within an adequate time to preserve safety (see ISA-TR84.00.02-2015, 5.3),
- are being monitored at a frequency consistent with the AAI plan, and
- can be corrected through on-line repairs.

### 5.2.1 Response to diagnosed degradation

The diagnostics available for older analog devices was often capable of detecting only complete failure. With the advent of more advanced transmitter technologies and digital communications, detection of some degraded states became possible. This advance in technology created the opportunity to perform predictive maintenance based on automated diagnostics. Using this advanced form of diagnostics to initiate correction of the degradation before complete failure of one or more functions of the device would be included in a predictive maintenance strategy. Whether or not this opportunity will exist for a given installation will depend upon:

- the presence of enough time between detectable degradation and complete failure to allow action—in some cases this can be a matter of seconds or minutes;
- the implementation of effective and alert annunciation systems and response procedures—refer to the ISA-18 series of standards and guidance documents;
- installations that facilitate timely repair or replacement of degraded components;
- resource planning sufficient to support annunciation monitoring and response.

If any of these are not provided, it is unlikely that repair will be proactively addressed before complete failure of the device and the resulting impact on plant operations or upon safety system performance on demand. Annex G provides further information on preventive and predictive maintenance, including the relationship between degradation time and maintenance strategy selections.

### 5.2.2 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 adverse environmental conditions and operating effects such as corrosion, process spills, and leaks. Inspections should be documented, and any corrective action needed should be initiated immediately through site work order processes as discussed in 4.3.5.

As a general practice, a thorough nonintrusive 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. Nonintrusive inspection can be performed while the process is running. Intrusive inspection generally requires that the process be shut down, so that the SIS equipment can be removed from service. 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 is corrosion buildup around the stem of a rising stem valve used to isolate a process stream. The buildup, 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 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.

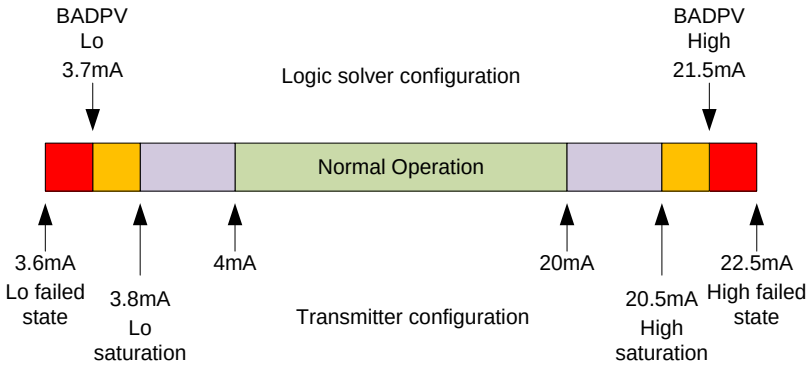
### 5.2.3 Planning and performing calibration checks

All SIS equipment should be calibrated prior to placing the SIF in service. Calibration of modern instruments is typically performed by the manufacturer, and calibration deviation is generally not expected under manufacturing shop floor conditions. However, instrument calibration is affected by the physical and environmental conditions that the instrument experiences over time. In many cases, the only option to a calibration problem is replacement of the instrument. A calibration check is used as part of the predictive maintenance inspection procedure as a way of detecting very early stages of degradation. For older devices, recalibration might need to be performed routinely by the user in the workshop or field. In this case, the calibration may be addressed by the preventive maintenance portion of the AAI plan.

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. Figure 5 depicts a suggested transmitter and logic solver analog input configuration. 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 it in service.

Correct functionality between transmitters and the SIS logic solver is essential to effective SIF operation. Failure to ensure that the transmitter 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.




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

**Figure 5 – Example of transmitter and logic solver analog input configuration**

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

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

Calibration check procedures should be available for each type of SIS equipment (See “Annex F – Example calibration forms”). In general, calibration check 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 restarted. 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 nondiverse process measurements.

Periodically, the calibration equipment is subjected to verification and recertification. When a calibration verification identifies a problem with the accuracy of the calibration equipment, the user should assess the significance of the deviation and determine whether devices calibrated since the last verification need to be rechecked.

### 5.2.4 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 are not a substitute for preventive maintenance and repair. Detailed recording of inspection and test observations is 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, pretrip, and trips). 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 ensure 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 ensure 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. 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 communication 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 consider:

- 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;
- proof test coverage requirements (refer to ISA-TR84.00.02 for more guidance on proof test coverage);
- when applicable, how tests may affect other SIF or operating systems and how to address the impact;
- where applicable, how the SIF or SIS equipment is affected by bypasses;
- required notifications during the 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, including any limitations on how long the bypass may be in place without requiring additional approvals and risk management.

- Do operations have an equivalent process variable to monitor when the SIF process sensor is in bypass?
- Do operations have control of a final element that can be used to shut down the process independently during testing when the output is in bypass?
- Discuss what to do 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 about when to evacuate to a safe location?
- Discuss what to do 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 ensure 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.

#### 5.2.4.1 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 startup. 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 are 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-61511 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, afterward 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 AAI 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 6 illustrates a SIF that has been divided into three overlapping segments for testing. Any project or change affecting 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;
- proof test coverage requirements (refer to ISA-TR84.00.02 for more guidance on proof test coverage);
- procedures that define 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.

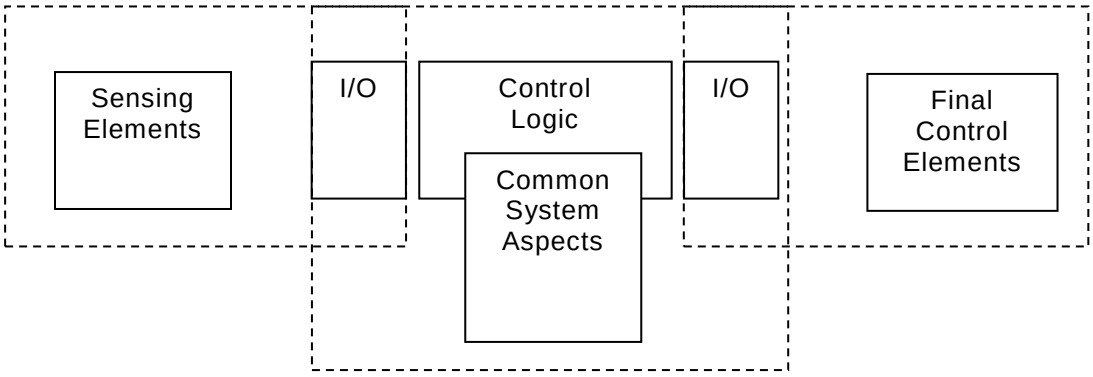



**Figure 6 – Example of SIF segment tests illustrating overlapping segments**

#### 5.2.4.2 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 AAI 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 affect 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 than 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 AAI plan should define the allowable test interval variation, including management approvals for test deferral (refer to 4.2.4 for more guidance on deferrals and approvals).

NOTE Test intervals may be affected by unplanned repairs or replacement. If a proof test is effectively 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 the 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.

It is also necessary to consider the relationship between proof test coverage and useful life when determining the proof test interval. When the proof test coverage provided by the written test procedure is less than 100% of the known dangerous failures, sustaining the average probability of failure on demand (PFD) or the average frequency of failure (PFH) for the duration of the expected useful life may not be possible through fixed schedule maintenance, inspection, and testing alone. Depending on the contribution of the untestable dangerous faults to the overall dangerous failure rate, the accumulation of failure probability from the untestable faults may make it difficult to maintain the target SIL across the full range of the useful life (refer to 5.2.5). The untestable failures can be addressed through refurbishment, such as rebuilding or replacing a limited number of component(s) within the device. Refurbishment is part of preventive maintenance and can be executed based on the device's current condition or on a fixed interval. Refer to 4.3.1 for guidance on establishing pass/fail criteria, including criteria for the detection of wear out.

#### 5.2.4.3 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 effectively tested. The test procedure should cover how redundant elements will be individually tested, and it should ensure all channels in a parallel path are tested. For instance, when process control valves are used as part of a SIF, the test procedure should reinforce that a basic process control system (BPCS) failure (or action) will not prevent the SIF from fulfilling its safety action. If any equipment is shared by multiple SIFs, the proof test strategy

should take this into account to guard against unnecessary testing, e.g., a block valve shared among several independent SIFs.

All equipment necessary for performing testing should be identified and verified suitable for tests to be performed. This includes calibration equipment with traceable performance.

#### 5.2.4.4 Off-line testing

The most common test of a 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-61511 and demonstrates that the SIS operates according to the SRS.

NOTE After the initial validation has been performed, a subsequent test that demonstrates the operation of the SIS equipment or SIF segments is 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 downtime of the SIS (see deferrals clause).

#### 5.2.4.5 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 the equipment to be tested. In some cases, the risk of being in bypass may require the 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.

#### 5.2.4.6 Effect of incomplete proof testing

An effective test will detect all hidden dangerous failures and degraded conditions, so that the equipment 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 7, the SIF probability of failure increases as a function of time, PFD(t), but the PFDavg is constant. With complete testing at the required proof test interval, the SIS will provide a level of performance assumed in the SIL verification.

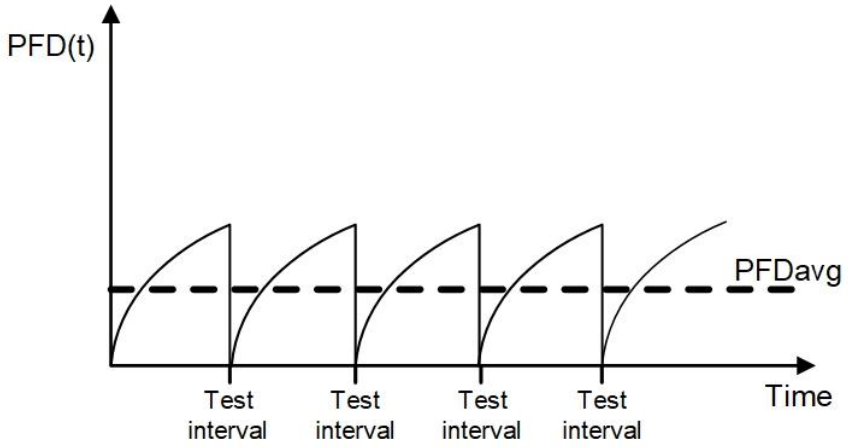



**Figure 7 – Change in PFD(t) as a function of time and test interval**

If the test is incomplete, some hidden dangerous failures will not be detected. Figure 8 illustrates how the PFD(t) increases over time due to the increased probability that an undetected failure could occur. The PFDavg at each test interval increases until the equipment is overhauled to return it to “as good as new” condition.

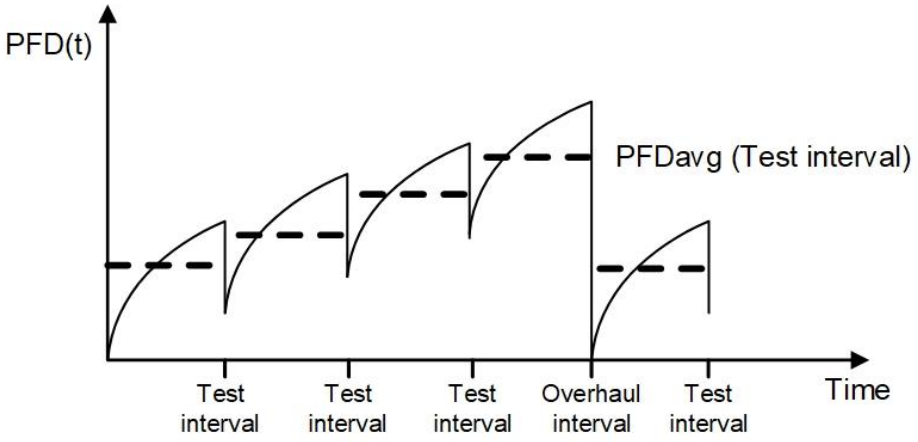



**Figure 8 – Increase of PFD(t) over time due to partial testing**

Figure 9 illustrates the PFDavg calculated based on proof test effectiveness and a defined overhaul interval. The PFDavg is higher than in Figure 7 due to the undetected failures being present until overhaul occurs and the failures are corrected.

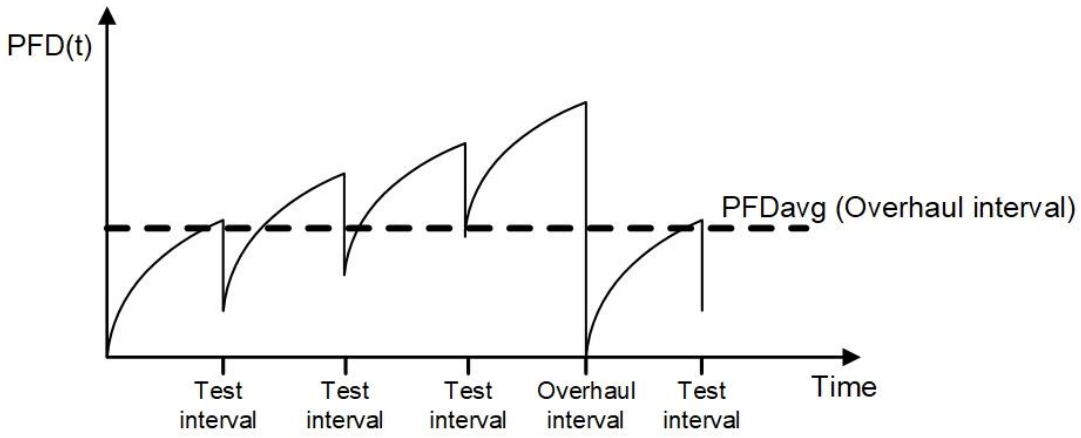



**Figure 9 – Increase of PFD(t) over time due to incomplete testing**

#### 5.2.4.7 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. Device proof testing should include testing of the diagnostic features, where these features are being claimed in the SIL calculations and test interval determination. 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 may or may not detect incipient conditions or the impending end of useful life (e.g., wear out). The reliable detection of incipient failure and wear-out conditions through on-line diagnostics typically requires the use of intelligent devices with diagnostics monitoring. Refer to 5.2 and Annex G for further guidance on diagnostics monitoring as part of predictive maintenance. 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. As noted in 5.2, diagnostics should only be used to extend the proof test interval or modify the proof test content if the following are provided:

- sufficient time to respond to diagnostics within the process safety time;
- appropriate and alert interfaces;
- inclusion of diagnostics configuration, alarm interfaces, and associated SIS application programming in verification and validation testing;
- timely monitoring and written response procedures;
- access restriction for device and host system diagnostic configurations and application programming;
- change management for the diagnostic function, including device configuration, response procedures, and monitoring resources.

#### 5.2.4.8 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 a proof test record compliant with ANSI/ISA-61511 is created after the trip. Trips related to process demands can be treated as proof tests only for the SIF or SIFs that initiated the automatic shutdown. To be considered a proof test, the following should occur:

- confirmation the demand was not caused by 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.

Manually initiated demands can only be considered as a partial proof test when sensors/initiators are not covered by the test. In these cases, only the logic solver and final elements are being tested. To be considered a complete proof test, the following should occur:

- 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;
- immediate testing of sensors/initiators of the related SIFs with its respective off-line testing procedure.

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 startup activity planning. Before startup, the affected SIS equipment should be visually inspected, along with any auxiliary systems, to the same rigor as 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 the trip. Detailed analysis of the data can be performed at a later time by qualified personnel once startup 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 the SIF at a location. For example, if the 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 (see Figure 10). 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.

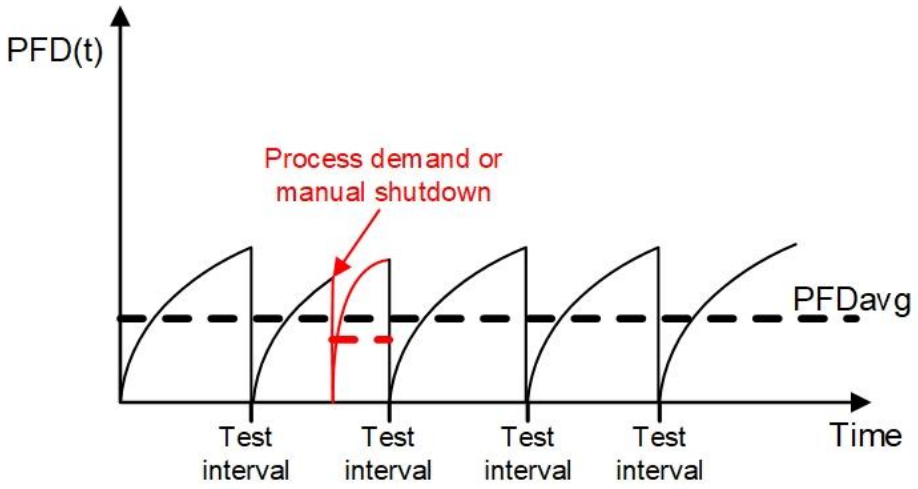



**Figure 10 – Change in PFD(t) as a function of time and process demand**

Typically, demand tests are focused on final elements, because sensor and logic solver tests can be performed on-line. This means that a demand test is not a complete test of the SIF (refer to 5.2.4.6 for more guidance on incomplete testing). However, this does not limit the potential for demonstrating a complete proof test of the 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, it can be documented that the final element passed or failed the functional requirements. It is important to note that a final control element may be a part of multiple SIFs, 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.

#### 5.2.4.9 Proof testing sequenced shutdown

In a sequenced shutdown, one system detects the hazard in a unit (or area) and sends a signal to final elements located in another unit (or area), possibly through one or more additional logic solvers. Compressor stations in pipelines are an example of a process application that may use this protective strategy.

It is recommended to avoid transferring risk between units or plants in this way, even when both units belong to the same organization, as it can create ambiguity regarding management of the safety system. Transferring risk between units can increase the likelihood of systematic errors in conducting the hazards and risk analysis, performing testing and routine maintenance, and responding to diagnosed failures. It is inherently safer to have the sensors, logic solvers, and final elements contained within the same unit boundaries.

Nevertheless, in situations where a safety function depends on activating final elements in another unit, the proof test strategy will be required to ensure that all devices necessary to execute the safety function, including communication systems, are tested at the specified interval. Doing so will typically involve addressing:

- coordination of tests between the units to ensure that the full communication path is tested;
- communication of all use of bypasses to allow management of risk in a unit where a hazard would occur;

- management of change approval between the units to avoid inadvertent degradation of safeguard effectiveness;
- shared ownership responsibility over the safety system for routine performance monitoring and functional safety auditing, particularly when the two units belong to different organizations or companies.

### 5.2.5 Managing useful life

The AAI 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 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 ensures it remains in its useful life. 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. This is an indication that the device has reached the end of its useful life. The useful life achieved by the SIS equipment will depend on many factors, including its exposure to the operating environment.

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-61511-1-2018, 5.2.5.

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 automation asset integrity plan to bring the SIS performance into alignment with expectations; it can also indicate the need to remove equipment from service.

In regard to useful life, there are two important considerations: (1) understanding what components/parts limit the overall equipment useful life, and establishing an automation asset integrity plan to deal with those components/parts in a timely manner, 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 which components limit the useful life of the SIS equipment. If it is a replaceable component, consider whether it is feasible and cost effective to replace the consumable parts at a defined interval in order to extend the useful life. It may also be possible 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.

An increased failure rate above the assumed reliability parameters 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. Clear criteria should be provided in the test procedure regarding indications of wear out specific to that device technology. The test procedure should also include a review of maintenance events on the device since the last complete replacement, with clear guidance on the frequency that might indicate impending wear out or other failure mechanisms that should be promptly investigated. Finally, the test procedure should include comparison of the current device service time versus the specified useful life constraints. If the useful life will be exceeded prior to the next scheduled test, replacement planning should be performed.

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 this example, the user should consider the capacitor and the remaining equipment components. In most cases, an AAI 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.

The mean time between work orders or the frequency of diagnostic alarms are examples of performance metrics that can also be periodically examined as part of the AAI program management. A short mean time between work orders or high diagnostic rate would indicate wear out or some other failure mechanism that requires further investigation and resolution.

### 5.3 Planning and performing reactive maintenance

As described in 4.2, reactive maintenance is only performed in response to complete functional failure of the device. If reactive maintenance is the only AAI strategy established for an automation device, the detection of functional failure will typically be through a spurious impact on performance of the process equipment or upon failure of the automation system to perform upon demand. For this reason, reactive maintenance plans should not be used as the sole strategy for devices used to execute instrumented safeguards.

Since the device in question has already failed, performing reactive maintenance on instrumented safeguard devices is typically accompanied by a compensating measure procedure by which the safety risk is being managed. Due to the nature of temporary alternative risk management practices, compensating measure procedures might only remain effective for a limited amount of time. If no compensating measures are available for a particular failure, the common practice would be to manage risk by reducing, stopping, or removing the presence of hazardous materials. For this reason, completion of reactive maintenance procedures is often the most time sensitive of the AAI maintenance activities.

## 6 References

ANSI/FCI 70-2-2013, *Control Valve Seat Leakage*, Fluid Controls Institute, www.fluidcontrolsinstitute.org.

ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*, www.isa.org.

ANSI/ISA-61511-2018, Parts 1-3, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, www.isa.org.

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

API 598, *Valve Inspection and Testing*, Tenth Edition, American Petroleum Institute, 2016 Edition, www.api.org.

Center for Chemical Process Safety (CCPS), *Process Equipment Reliability Database (PERD)*, American Institute of Chemical Engineers, www.aiche.org.

Health and Safety Executive (HSE), *Findings from Voluntary Reporting of Loss of Containment Incidents 2004/2005*, Hazardous Installations Directorate, Chemical Industries Division, www.hse.gov.uk.

IEC 60534-4:2006, *Industrial-Process Control Valves – Part 4: Inspection and Routine Testing*, www.iec.ch.

ISA-RP105.00.01-2017, *Management of a Calibration Program for Industrial Automation and Control Systems*, www.isa.org.

ISA-TR108.1-2015, *Intelligent Device Management Part 1: Concepts and Terminology*, www.isa.org.

ISA-TR84.00.02-2015, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions (SIF)* , www.isa.org.

ISA-TR84.00.03-2019, *Automation Asset Integrity of Safety Instrumented Systems (SIS)*, www.isa.org.

ISA-TR84.00.04-2015, Part 1, *Guideline for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*, www.isa.org.

ISA-TR91.00.02-2003, *Criticality Classification Guideline for Instrumentation*, www.isa.org.

ISA-TR96.05.01-2017, *Partial Stroke Testing of Automated Valves*, www.isa.org.

NAMUR NE 43, *Standardization of the Signal Level for the Failure Information of Digital Transmitters*, User Association of Automation Technology in Process Industries, 2003, www.namur.net.

NFPA 70E, *Standard for Electrical Safety in the Workplace*, National Fire Protection Association, 2018 Edition, www.nfpa.org.

NFPA 86, *Standard for Ovens and Furnaces*, National Fire Protection Association, 2019 Edition, www.nfpa.org.

# 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 facility's training documentation and management system. The first document (Figure A.1) shows how one company documents the training in an electronic database to track the training of each individual. The second example (Table A.1) 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.

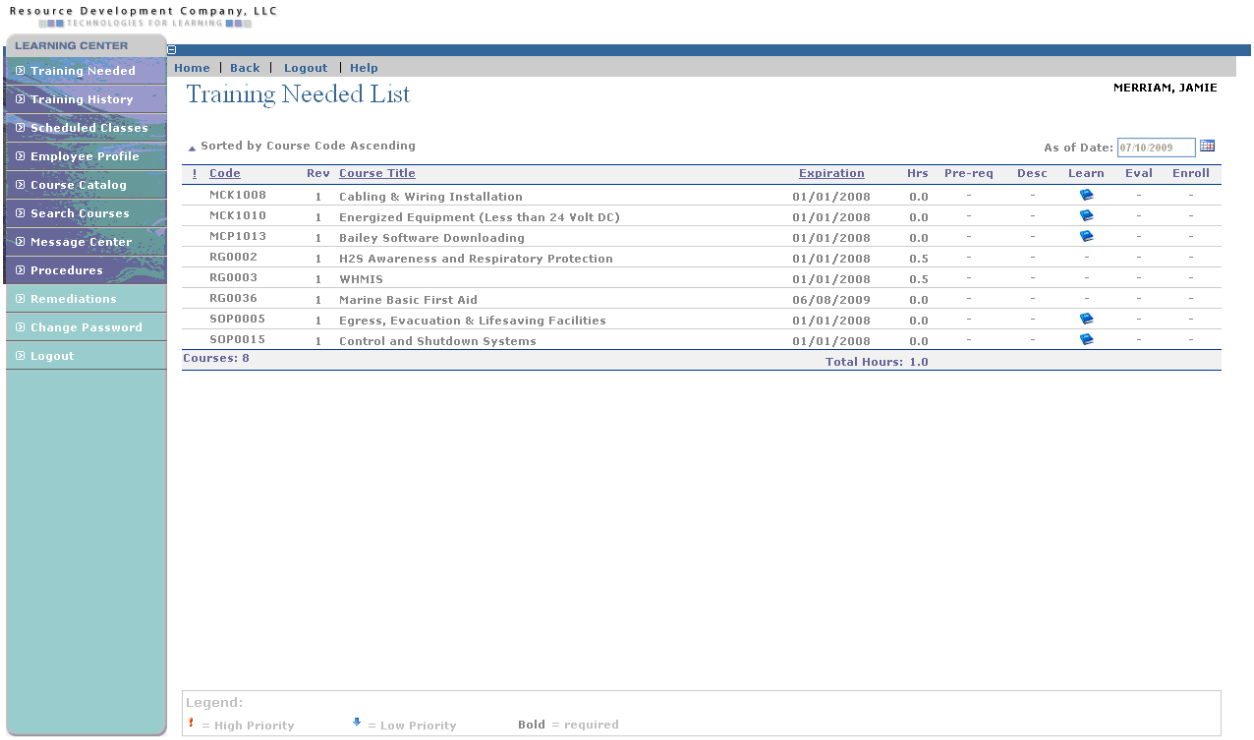



**Figure A.1 – Example training list**

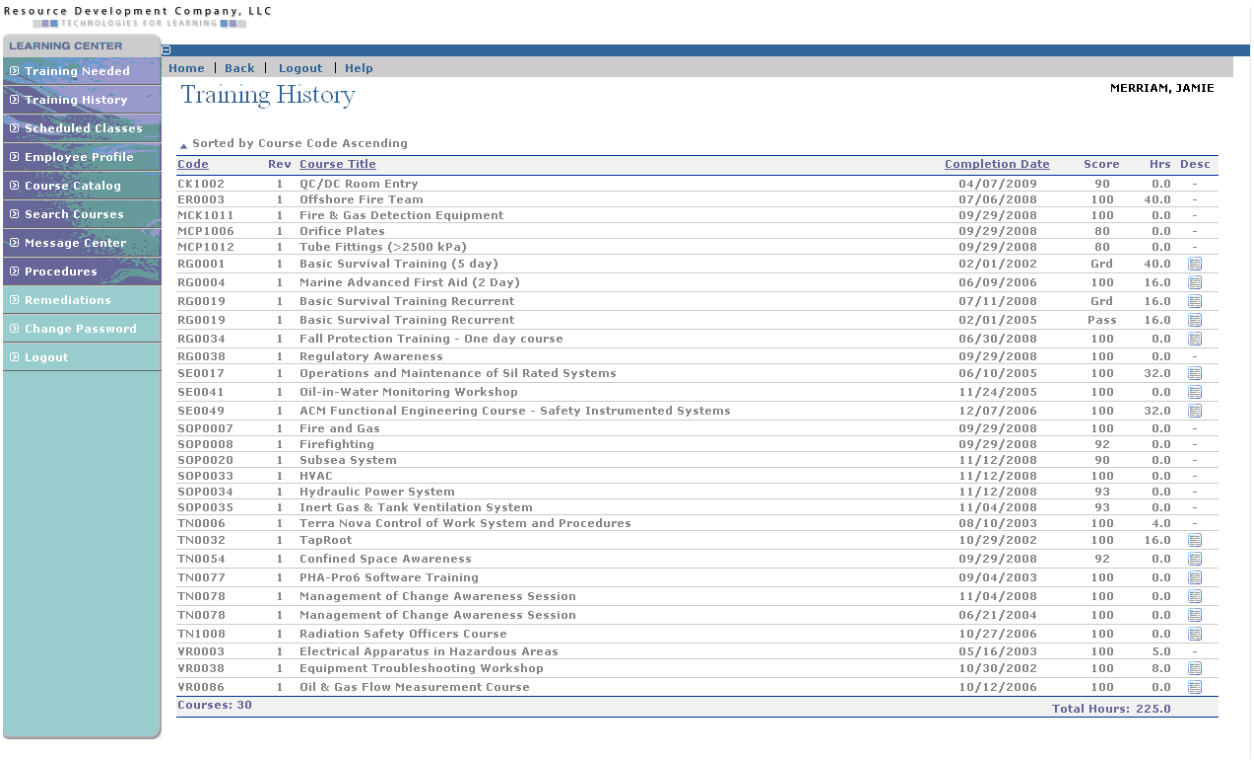



**Figure A.1 – Example training list (continued)**

**Table A.1 – 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:<br>a) pneumatic signal lines<br>b) electrical/electronic signal lines<br>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:<br>**EXPLAIN** the purpose<br>**STATE** the inputs and outputs of the SIS PLC system<br>• Using the PLC operating instructions, ACCESS data in PLC to determine the source of a problem<br>**IDENTIFY and REPLACE** failed board<br>**COPY** error codes and fault details to diskette<br>**PERFORM** functional checkout | | P/S | |
| TASK 10 | **CALIBRATE** the following transmitters:<br>• differential pressure<br>• pressure | | P/S | |
| TASK 11 | **PERFORM** a SIS bypass | | P/S | |
| TASK 12 | **COMPLETE** bypass authorization form<br>• **EXPLAIN** the different levels for bypass approvals<br>• **STATE** location of an active SIS bypass form<br>• **STATE** the location of a completed (inactive) bypass form<br>• Using corporate SIS document as a reference, **STATE** the acceptable reasons for bypassing a SIS | | P/S | |

| | | | | |
|---|---|---|---|---|
| TASK 13 | **PERFORM** the following SIS valve performance tests:<br>• TIMING TEST<br>• BUBBLE TEST<br>• FUNCTIONAL TEST (what is the content of this test?)<br>• EXPLAIN the purpose of each of the above tests<br>• STATE the location of the test sheets<br>• 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.

**Table 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)

| **Shutdown info** | | | | |
|---|---|---|---|---|
| Did shutdown function? | Yes | No | (Circle one) | |
| Did process variable reach or exceed set point? | Yes | No | (Circle one) | |
| Comments: | | | | |
| | | | | |
| | | | | |
| **Permissive info** | | | | |
| Did permissive function correctly? | Yes | No | (Circle one) | |
| If no, circle one of the following:<br>Permissive failed to prevent unsafe state<br>Permissive spuriously initiated action | | | | |
| Comments: | | | | |
| | | | | |
| | | | | |
| **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: | | | | |
| | | | | |
| | | | | |

**Table 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 |

**Table B.3 – Trip investigation report**

Distribution list:
SIS Specialist:
Operations Manager:

| | |
|---|---|
| SIF tag number or loop ID: | Plant ID: |
| SIF description:<br>(If there is a documented SRS, provide document reference) | |
| ☐ Process demand ☐ Spurious trip<br>(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<br>☐ Process upset ☐ Wind<br>☐ Control failure ☐ Ground movement<br>☐ Operator error ☐ Loss of containment detection<br>☐ Equipment failure ☐ Fire<br>☐ Lightning ☐ Explosion<br>(What caused the process to shut down or to be interrupted?) | |
| Did all of the SIS equipment operate as designed? ☐ yes ☐ no<br>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:<br>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:<br>(Attach DCS trends, alarm journals, first out, sequence of events logs, manufacturer failure reports) | |
| Comments: | |
| Assessment led by: Date:<br>(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.

**Table 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 automation asset 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.

**Table C.1 – Failure investigation report form**

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

**Table 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:<br>☐ Failed to operate according to specification<br>☐ Operated without cause | | |
| What caused the failure:<br>☐ Sensor ☐ Process connection ☐ Electrical connection<br>☐ Electrical contact ☐ Power supply<br>☐ Impulse line plugged ☐ Root valve/manifold closed ☐ Configuration<br>☐ Other (describe) | | |
| Comments: | | |
| Assessment led by: _____Date:_____<br>SIS specialist/engineer or equivalent | | |

**Table 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:<br>☐ Failed to operate according to specification<br>☐ Operated without cause | | |
| What parts contributed to the failure:<br>☐ Actuator ☐ Seat ☐ Air set/Air supply<br>☐ Solenoid valve ☐ Spring ☐ Pneumatic connection/tubing<br>☐ Body/Bonnet ☐ Gasket ☐ Pneumatic accessory (e.g., booster, quick vent, etc.)<br>☐ Guide ☐ Packing ☐ Power supply<br>☐ Shaft ☐ Position switch ☐ Electrical connection | | |
| Comments: | | |
| Assessment led by: _____Date:_____<br>SIS Specialist/Engineer or equivalent | | |

## Annex D – Effective procedure writing, verification, and implementation

A comprehensive AAI 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, such as accessibility, communication, and ergonomics. Procedures should be in place before the startup 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 preventive maintenance, diagnostics monitoring, inspection, and testing. In addition to being in place before process equipment is put in service, the procedures should be updated before any change is implemented and be 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 AAI 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, you should identify responsible personnel or departments, the required permits and notifications, the required test equipment and tools, and any appropriate hazard or safety warnings. 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 SIFs, 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) an alarm, or (3) an alert. 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 with a disabled SIF requires compensating measures to ensure safe operation during the out-of-service period. Refer to ISA-TR84.00.04 Annex P for more guidance on compensating measures. Refer to ISA-TR84.00.04 Annex R on tracking out of service periods.

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 MPRT established in the design

and operating basis. The MPRT is 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 should be executed. The review should also address the priority status for the repair activity.

A specific written test procedure meeting the specified test coverage requirements 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 the following, where appropriate:

- the safety requirements specification;
- equipment description and location for each SIF;
- functional requirements for each SIF;
- inspection procedures to be followed;
- calibration and testing methods to be followed;
- frequency of calibration, testing, inspections, and maintenance activities;
- acceptable performance limits (± 2% of full range if no limits specified);
- sequence of testing if required;
- who should perform the test;
- 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 (such as watchdog timer, diagnostic comparators);
- verification that ancillary equipment components are operational (fans, filters, batteries, UPS, climate control, air supply, etc.);
- defined means of ensuring testing is performed and documented.

All test procedures should have the 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 be appropriately loaded in the maintenance management system.

All drawings used to describe the 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 not 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-startup safety review for any new or modified SIS. New personnel should complete training on the SIS operation before taking responsibility for the process equipment.

Once a 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 minimal 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 diagnostic 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 flowcharts, should be considered. Flowcharts 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, such as:

- 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 SIFs);
- 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, lockout, 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 to ensure it will not prevent the SIF safety action.
- 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 are returned to normal operation. Verification that each sensor and final control element is returned to pretest operation.
- permits required;
- manufacturing authorization of the procedure.

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

In order to properly carry out the test, the technician may need additional information not contained in the test procedure, 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 that puts the operator at risk. In order for technicians 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 for 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 the 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 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 lock-out 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 AAI activity. For example, operating procedures may restrict when maintenance activities are conducted, e.g., prohibited during certain operating modes due to risk.

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.

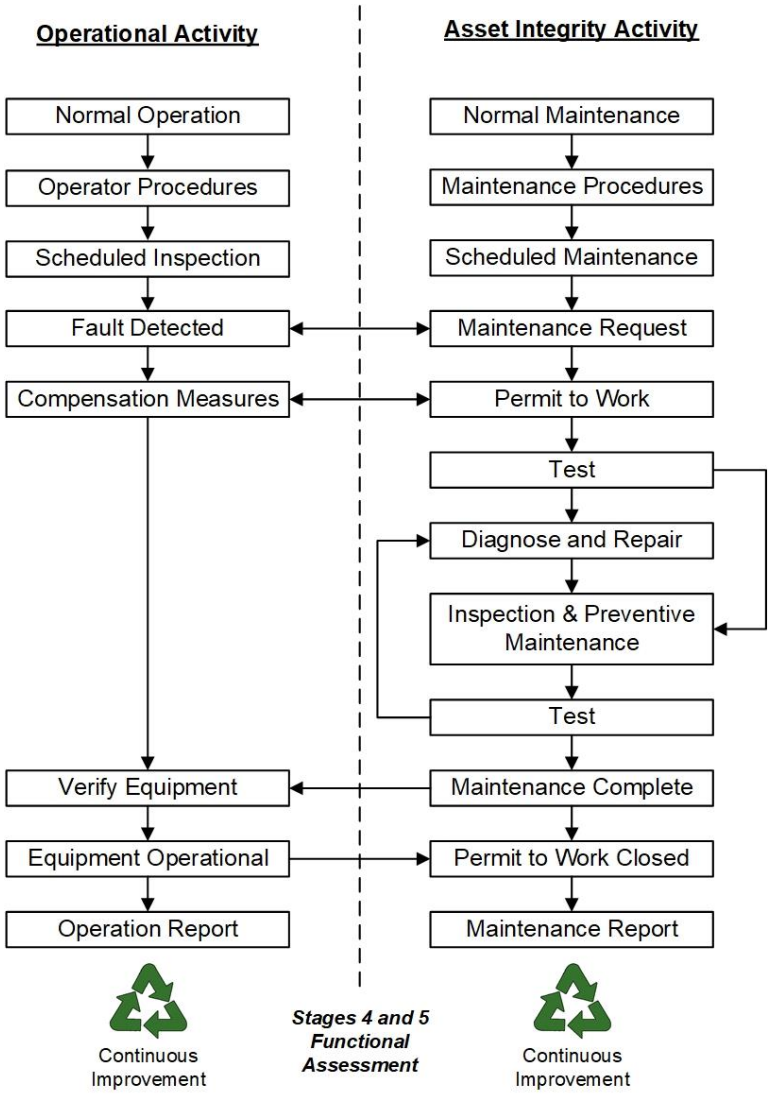



**Figure D.1 – Simplified operation and maintenance work process**

## 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 has 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 the 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)<br>Capture error<br>Identification error<br>Impossible tasks<br>Input or misperception errors<br>Lack of knowledge<br>Over-motivation or under-motivation<br>Reasoning error<br>Task mismatches |
| **Situation-oriented errors** |
| Environmental<br>Stress<br>Timing |
| **System-oriented errors** |
| Errors by others<br>Procedural<br>Violations |
| **Human errors in system design** |
| Mistakes<br>Specification errors<br>Communication breakdown<br>Lack of competency<br>Functional errors<br>Common errors in instrument design |

## D.10 Continuous improvement

Personnel should contribute their experience and knowledge to the continuous improvement of procedures and practices. The 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 automation asset integrity plan. The bullet lists are not exhaustive and do not include everything that should be covered by the inspection program for the 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 walk-through 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 is 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,
- ancillary equipment (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 pushbuttons), and
- warning signs (e.g., radiation or high voltage hazard).

Each component of a SIF should be in good condition with no visible physical defects, which could affect 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, and
- 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 the 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 the 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 buildup 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 that 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);
  - enclosure hardware installed per design standards;
  - access security (e.g., doors locked) is in place.
- logical checks
  - verify application program revision;
  - 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 the 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, watertight, 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, and ground resistance. 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 there is 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 buildup;
- power operating within acceptance range.

**Table 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:**_____

# 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.

**Table 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) × 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 | Dead band | Comments |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Switch Settings:** | | **Serial Number:** | | | |
| Tag Number | Switch Setting | Signal As-found | Signal As-left | Dead band | Comments |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

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

REMARKS: _____

☐ DIGITAL ☐ DOWNSCALE B/O ☐ SS TAG ATTACHED

☐ ANALOG ☐ UPSCALE B/O

TRANSMITTER ☐ PROPERLY COLOR CODED ☐ SQUARE ROOT

AS-LEFT: ☐ PMI PERFORMED ☐ LINEAR

TECHNICIAN: _____ DATE: _____/ /_____

# Annex G – Preventive and predictive maintenance

Preventive maintenance is a proactive activity performed on a fixed schedule 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 includes performing maintenance to extend the equipment life, such as changing an air filter and replacing disposable parts like batteries. Common preventive maintenance tasks include timely

- battery replacement,
- climate control parts 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, and
- electrical contact replacement.

In contrast, predictive maintenance reduces the frequency of equipment failure through periodic restoration of the equipment condition upon detected degradation. Detection of degradation may include activities that occur based on fixed schedules, such as inspections and tests, in addition to ongoing monitoring for degradation through automated diagnostics and observation of the impact on operations metrics, such as quality and productivity.

Important considerations in establishing a rigorous AAI program include:

- integrating preventive and predictive maintenance efforts with other plant tasks, resulting in a cost effective, efficient, multitasking maintenance program;
- availability of 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 AAI and reliability processes to identify chronic failure issues (e.g., possible improper selection of equipment/materials).

## G.1 Identification of preventive and predictive maintenance tasks

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

Appropriate preventive maintenance tasks may be identified from sources such as manufacturer’s literature, brainstorming, operating experience, maintenance experience, and best practices. 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 from 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.

Predictive maintenance strategies are dependent on detecting degradation prior to complete loss of functionality. For predictive maintenance tasks to be effective, the degradation must be sufficiently slow that there can be an effective response to the detection of degradation before the device fails completely. Table G.1 shows the relationship between the speed of degradation and the diagnostics, inspection, and testing activities that might be beneficial.

**Table G.1 – Fault detection and handling**

| Fault Degradation Time Scale | Action |
|---|---|
| Milliseconds: These faults reach a failure condition instantaneously or with little or no warning and have no process tolerance. | Voting redundancy algorithms execute with every cycle of logic or control—these can prevent impact from instantaneous failures. |
| | Multiple layers of protection can potentially be as fast as voting but execute asynchronously. |
| Seconds to Minutes: These faults reach failure condition quickly but have some process time tolerance. Various strategies can reduce or eliminate the impact of these faults if action is taken within the process fault tolerance time. | Automated diagnostic algorithms generally run much slower than logic or control algorithms—diagnostics can handle faults with slightly longer time tolerance and can shorten time for repair.<br>• Hot Standby redundancy depends on diagnostic algorithms for initiation.<br>• Algorithmic automated fault handling (such as mode shift to manual) depends on diagnostics for initiation.<br>• Operator actions based on diagnostic alarms can reduce the impact of faults. |
| Days to Weeks: These faults progress to a failure condition over a period of weeks and can be detected while the condition is incipient. | Repair and failure prevention based on automated diagnostics with optimized monitoring and planning work processes can accomplish repair before a full failure condition develops. |
| Months to Years: Time scale for moderately slow failure mechanisms for which degradation is usually detectible well before complete failure. | Manual Inspection and testing: Manual procedures are effective in this time frame for finding latent faults but may not be as useful for detecting incipient faults. These procedures can be used to prevent very slow failure modes (see below). Latent faults can include faults in any sort of standby system, including protective systems or intermittent use systems such as freeze protection. |
| Decades: Time scale for very slow failure modes with a more or less constant degradation rate (such as some wear or corrosion phenomena). | Manual procedures are effective for prevention in processes with this time scale. Nonlinear or episodic degradation mechanisms are better suited to automated measurement and diagnostics. |

## G.2 Criticality

Some preventive 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 preventive and predictive maintenance 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 is affected by the following:

- shutdown schedule;
- on-line vs. off-line tasks;
- unexpected as-found condition during preventive or predictive 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 or predictive maintenance on-line. While inspections can usually be performed on-line, the available amount of maintenance resources may limit this activity. 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 and predictive maintenance tasks may by based on how long the equipment is operating or may need to be scheduled just prior to unit startup.

The frequencies of preventive maintenance activities and of the manual inspection and testing procedures used to trigger predictive maintenance may need to be adjusted over time based on the demonstrated performance of the automation system. As part of the continuous improvement part of the lifecycle, the timing of the activities needs 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 AAI plan is achieving its goals. Failure investigation, such as root cause analysis, can potentially identify weaknesses in the maintenance program, which should be corrected. 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. This approach helps facilitate an overall reliability-centered maintenance program that would additionally measure and analyze equipment performance, looking to maintain expected performance as well as to identify opportunities to improve reliability.

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 Preventive maintenance

Preventive maintenance is often used to address parts that predictably wear out, gum up, foul, corrode, etc. 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 include:

- allowing the 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;
- sustained warranty protection;
- reduced spares inventory.

### G.3.2 Predictive maintenance

Predictive maintenance, sometimes referred to as 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 checklists, such as those listed in Annex E, can be used to identify corrosion and wear and to determine what parts need to be replaced. The replacement of the part can be scheduled so that it is replaced prior to the complete functional failure of the device.

Sometimes the degradation can be detected through automated means. For example, in a 2oo3 voting level sensor architecture where two sensors are DP level and the third a radar level, comparison diagnostics can be used to identify the onset of excessive drift or 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;
- an alert provided to the appropriate personnel, giving them some time to optimize the performance of critical maintenance activities;
- integration with other automation asset integrity efforts resulting in a cost-effective, efficient, multitasking maintenance program;
- automated documentation of specifically defined degraded conditions to support proven in use;
- extended life as degraded conditions are repaired before more complete failures;
- analysis of actual equipment “wear-out” versus estimated “wear-out” performance, allowing AAI plan upgrade;
- controlled analysis of replaced equipment for evidence of unexpected application limitations or potential unsafe failures;
- optimized spares inventory.

For predictive maintenance, the necessary response to a defect identified through inspection, test, or diagnostics is related to the expected rate of degradation. As shown in Table G.1, the speed of degradation is a significant factor in determining which predictive maintenance activities will be effective. The AAI plan should define the response required once a deficiency has been identified and when the task becomes overdue. The response to an overdue predictive maintenance task will need to consider how fast the equipment is degrading. This response is generally more time critical than preventive maintenance, since degradation that is in need of an intervention has already been identified and documented.

Initiating a predictive maintenance strategy relying on diagnostics is dependent upon there being an effective response to the diagnostic alarm. Refer to 5.2 and 5.2.4.7 regarding essential elements of an effective predictive maintenance program that uses diagnostics to provide notification of degradation.

## G.4 Documentation

Preventive and predictive maintenance activities 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 the 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 more frequent predictive maintenance via diagnostics.

This page intentionally left blank.

# 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.<br>This document explains the basic rules of the test procedures and provides directions for the development of plant-specific procedures and/or new procedures.<br>(Define the task along with explaining when to apply it 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: _____<br>Plant code number: _____<br>Safety instrumented function (SIF) identification number: _____<br>Protective system type (circle applicable type)<br>• Alarm<br>• Shutdown interlock<br>• Permissive interlock<br>• Auto-start interlock<br>Protective circuit description: (Reference applicable interlock table or master alarm summary as appropriate)<br>_____ |

***Continued on next page***