

ISA-TR84.00.03-2002



Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS)

NOTICE OF COPYRIGHT

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



**ISA—The Instrumentation,
Systems, and
Automation Society**

Approved 17 June 2002



Documents
Document Sharing Hub

ISA-TR84.00.03-2002

Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS)

ISBN: 1-55617-801-8

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

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

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.03-2002.

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

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

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

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE TECHNICAL REPORT, 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 TECHNICAL REPORT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS TECHNICAL REPORT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE TECHNICAL REPORT 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 TECHNICAL REPORT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE TECHNICAL REPORT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE TECHNICAL REPORT FOR THE USER'S INTENDED APPLICATION.

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

ADDITIONALLY, THE USE OF THIS TECHNICAL REPORT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE TECHNICAL REPORT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED

WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS TECHNICAL REPORT 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 TECHNICAL REPORT.

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

The following people served as members of ISA Committee SP84:

NAME	COMPANY
V. Maggioli, Chair	Feltronics Corporation
R. Webb, Managing Director	POWER Engineers
C. Ackerman	Air Products & Chemicals Inc.
R. Adamski	Invensys
C. Adler	Moore Industries International Inc.
R. Bailliet	Syscon International Inc.
N. Battikha	Bergo Tech Inc.
L. Beckman	HIMA Americas Inc.
K. Bond	Shell Global Solutions
S. Brown	DuPont Company
J. Carew	Consultant
K. Dejmek	Baker Engineering & Lisk Consulting
R. Dunn	DuPont Engineering
P. Early	ABB Industrial Systems Inc.
A. Frederickson	Triconex Corporation
K. Gandhi	Kellogg Brown & Root
J. Gilman	Consultant
W. Goble	exida.com LLC
D. Green	Rohm & Haas Company
P. Gruhn	Siemens
C. Hardin	CDH Consulting Inc.
J. Harris	UOP LLC
J. Jamison	Bantrel Inc.
W. Johnson	E I du Pont
L. Laskowski	Solutia Inc.
T. Layer	Emerson Process Management
N. McLeod	Atofina
G. Ramachandran	Cytec Industries Inc.
K. Schilowsky	Marathon Ashland Petroleum Company LLC
D. Sniezek	Lockheed Martin Federal Services
C. Sossman	WG-W Safety Management Solutions
R. Spiker	Yokogawa Industrial Safety Systems BV
P. Stavrianidis	Factory Mutual Research Corporation
H. Storey	Equilon Enterprises LLC
A. Summers	SIS-TECH Solutions LLC
L. Suttinger	Westinghouse Savannah River Company
R. Szanyi	ExxonMobil Research Engineering
R. Taubert	BASF Corporation
H. Tausch	Honeywell Inc.
T. Walczak	GE FANUC Automation
M. Weber	System Safety Inc.

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

NAME	COMPANY
M. Zielinski	Emerson Process Management
D. Bishop	David N Bishop, Consultant
D. Bouchard	Paprican
M. Cohen	Consultant
M. Coppler	Ametek, Inc.
B. Dumortier	Schneider Electric
W. Holland	Southern Company
E. Icayan	ACES Inc
A. Iverson	Ivy Optiks
R. Jones	Dow Chemical Company
V. Maggioli	Feltronics Corporation
T. McAviney	ForeRunner Corporation
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Westinghouse Process Control Inc.
R. Reimer	Rockwell Automation
J. Rennie	Factory Mutual Research Corporation
H. Sasajima	Yamatake Corporation
I. Verhappen	Syncrude Canada Ltd.
R. Webb	POWER Engineers
W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	KEMA Consulting
M. Widmeyer	Stanford Linear Accelerator Center
C. Williams	Eastman Kodak Company
G. Wood	Graeme Wood Consulting



This page intentionally left blank.

Contents

1	Introduction	11
2	Purpose.....	12
3	Scope.....	12
4	Audience.....	13
5	Definition of terms and acronyms	13
5.1	Definitions.....	13
5.2	Acronyms.....	15
6	Off-line testing.....	16
6.1	When should off-line testing be performed.....	16
6.2	Deferral of scheduled testing of SIF	20
6.3	How to perform off-line testing of SIF	21
6.4	Component testing	23
6.5	Logic solver test procedures	28
6.6	Testing of final control elements.....	29
6.7	Testing solenoid valves	30
6.8	Testing of HMI	30
6.9	Testing of communications.....	30
6.10	Final SIF test procedures	31
7	On-line testing.....	31
7.1	Preparation	31
7.2	When should on-line tests be performed.....	32
7.3	Performing on-line testing	34
7.4	Inspection (observation techniques that enhance SIF availability)	38
7.5	Testing documentation	41
8	Inspections.....	42
9	Auditing.....	43

10	References.....	43
	Annex A — Model procedure for approval required for replacing individual components in SIF	45
	Annex B — Model procedure for deferring scheduled testing of SIF	47
	Annex C — Model procedure for testing turbine thrust position monitors	49
	Annex D-1 — Model procedure for electronic over-speed trip testing.....	57
	Annex D-2 — Model procedure for testing turbine overspeed trip	63
	Annex E — Model procedure for testing permissive start for turning gear motor.....	67
	Annex F — Model procedure for lube oil pumps autostart test	69
	Annex G — Model procedure for testing first-out sequence alarms.....	71
	Annex H — Model procedure for functional testing of TMR-based SIS instrumentation.....	73
	Annex J — Example of a jumper control list.....	77
	Annex K — Model procedure for on-line test of a high level switch	79
	Annex L — Model procedure for on-line testing of flow sensors in a 1oo2 configuration (high or low trip) 81	
	Annex M — Model procedure for on-line testing of pressure sensors in a 2oo3 configuration (high or low trip)	83
	Annex N — Model procedure for testing temperature switches	85
	Annex O — Example visual inspection form for SIF.....	87
	Annex P — Model procedure for testing a permissive pressure logic point	91
	Annex Q — Model procedure for testing a simple SIF	95
	Annex R — Model procedure for testing a complex logic system	99
	Annex S — Model procedure for testing emergency stop switch.....	115
	Annex T — Model procedure for testing a relay implemented SIF.....	117
	Annex U — Model procedure for testing SIF watchdog timer	123
	Annex V-1 — Model procedure for on-line testing of sensor logic	125
	Annex V-2 — Model procedure for testing sensor logic	129
	Annex V-3 — Model procedure for on-line testing sensor logic	133
	Annex W — Model procedure for on-line final control element functional testing.....	137
	Annex X — Model procedure for on-line testing of compressor SIF	141

Annex Y — Model procedure for on-line testing of 2oo3 temperature elements.....	155
Annex Z — Model procedure for testing final control elements when manual bypass valves are provided	169
Annex AA — Example of a testing documentation form for off-line tests.....	173
Annex BB — Model SIF testing policy statement	175
Annex CC — Possible SIF performance metrics.....	177
Annex DD — Model technique for testing SIF valves on-line.....	179
Annex EE — Automated testing of SIF valves on-line	181
Annex FF — Possible audit protocol for safety instrumented functions	185
Annex GG — Example of checklist for auditing an SIF	193
Annex HH — Partial instrument trip test (PITT).....	195
Annex JJ — Vendor packages to perform partial stroke testing of SIF valves.....	201
Annex KK — Possible technique for evaluating benefit of partial stroke testing of SIS valves in PFD_{avg} calculations	203
Annex LL —Example method for partial stroke testing of SIS valves	207
Annex MM — Examples of techniques to perform on-line testing of solenoid valves	211
Annex NN — Model procedure for testing mA pressure transmitters.....	213
Annex PP — Model procedure for testing mA temperature transmitters	215
Annex QQ — Model procedure for testing mV temperature transmitters.....	217
Annex RR — Model procedure for testing pressure switches	219

Tables

Table 1 — Calibration work process for SIF components	22
Table 2 — Tests performed to verify operation of SIF components.....	24
Table 3 — Calibration and testing guidance for repaired or replaced components in SIF.....	25
Table 4 — Sample documentation for high alarm and trip settings.....	26
Table 5 — Sample documentation of high temperature alarm and trip settings	27
Table C.1 — Turbine thrust position	50
Table R.1.6A — Thermocouple input, trip, and bypass action validation	101



Table R.1.7A — Manual trip and reset logic functionality validation.....	110
Table KK.1 — Dangerous failure modes and effects with associated test strategy.....	204
Table NN.1 — Sample documentation for high alarm and trip settings	214



1 Introduction

The best test of the Safety Instrumented Function (SIF) is the full functional test. Because SIF are designed to act upon an abnormal condition being measured and a corrective action taking place, any test must examine the measurement, logic and final control element activity to be considered a full functional test. This should involve creating an abnormal condition of the measured variable such that the input variable first reaches the alarm state and secondly moves to the interlock point making observations that the rest of the system responds as expected. Any less complete test is necessarily a compromise. Understanding what techniques should be used to ensure that this full functional test is complete is vital.

The sense of well being resulting from this successful test unfortunately deteriorates with time. Therefore, determining when subsequent testing is required to maintain this feeling of comfort is critical. The relative value of the functional test versus the cost of running the test can impact this decision. It is necessary to consider the degree of safety risk caused by a Safety Instrumented Function (SIF) initiated nuisance shutdown and at the same time the safety risk associated with an event not stopped due to a dangerous unrevealed fault in the SIF. Real processes are not ideal. Many systems are at maximum expected risk during startup and shutdown conditions.

NOTE 1 In this document the acronyms SIF and SIS will be used for both singular and plural usage of the term.

NOTE 2 The techniques for testing SIF or SIS described in this document apply to demand mode systems only. Continuous mode systems, which are rare in the process industry, require testing considerations beyond the scope of this document.

SIF applications are normally in a standby mode waiting for an indication of some potentially unsafe condition to occur before taking action. Faults may not become visible until the SIF fails to respond to an unsafe condition in the process. In basic process control loops the sensors and valves are exercised continuously during the Distributed Control System (DCS) and Programmable Logic Controller (PLC) cycles making process or equipment faults visible quickly and rendering them hard to ignore. It is vital that some program of testing and observation of each SIF in the SIS be in place. Any testing scheme, though which is burdensome or difficult has the very real probability of being ignored or bypassed. Where on-line testing techniques are implemented, they should not unnecessarily compromise the process safety integrity during the test. The test equipment and procedure must be carefully evaluated to determine whether the danger of causing an incident due to performing the on-line test is greater than the danger of not discovering the failure. Ill-advised maintenance or troubleshooting might actually increase the process risk.

Effective safety testing is strongly affected by local situations. Hazards differ, resources differ, and even the site conditions differ widely. Rapidly changing technology and ever increasing citizen expectations also impact decisions. Safety incidents can have the political result of closing down entire businesses if the local citizens are sufficiently offended. International competition has put tremendous pressure on manufacturing operations to reduce personnel and costs. Whatever testing schemes are used, they need to be very practical and should minimize maintenance and operating costs while ensuring the integrity of the SIF. The techniques suggested in this document are intended to provide guidance in the development of effective and efficient methods to plan and to manage testing and maintenance of SIF. Users of this document should have a good understanding of the applicable standards or guidelines which apply to SIF and SIS such as ANSI/ISA-84.01-1996, ISA-TR84.00.02-2002, OSHA 1910.119, dIEC 61511, and others.

The records resulting from the testing program should be equally valuable to planned and preventive maintenance and address the requirements of all regulations, as well as quality control and mandated standards.

Another important part of process safety in an operating unit is the knowledge and motivation of the operators and maintenance personnel. It is the responsibility of management to provide training and motivation. Any plan, formula, procedure, or even a standard, which attempts to, or claims to substitute

procedures and rules for training, motivation, and support is doomed to failure. Therefore, the testing techniques proposed should not be considered just another set of rules, which become burdens to overworked plant personnel, but rather means of improving the work process and reducing frustration.

2 Purpose

Systematic testing of each Safety Instrumented Function (SIF) is required to ensure that dangerous unrevealed failures have not occurred that could render the SIF unable to perform the function for which it was provided. This testing ensures that all operational functions of the SIF are evaluated on a periodic schedule in accordance with the safety integrity requirement of the SIF. Many processes have operating cycles that are longer than the period between testing required achieving the safety integrity. Thus performing the required off-line testing necessitates shutting down the process. This is costly and puts unnecessary strain on equipment and necessitates going through shutdown and startup (which are usually the most dangerous periods of a process lifecycle) again. Therefore, the ability to perform testing while the process remains in operation is desirable.

There are also different ideas on what constitutes an acceptable test for various components of SIF. Whether the test is performed off-line, with the process down, or on-line with the process in operation, there are methods for performing the testing that ensure a high degree of detection of failures that might have occurred. Guidance is needed in the selection of these testing methods for both off-line and on-line situations.

There is also benefit in performing inspection activities on SIS equipment during normal operation of the process to detect any potential problem creating situations that might be developing. Guidance in what to look for, how often to inspect, and what to do when a condition is observed that could lead to a failure will enhance the safety integrity of the SIF.

3 Scope

Testing considerations of SIF should be included in most of the Safety Lifecycle steps described in ANSI/ISA-84.01-1996. Testing frequency is a part of the determination of Safety Integrity Level (SIL) for the SIF. Provision for conducting tests must be included in the selection of equipment and design of the SIF and the Pre-Startup Acceptance Test (PSAT) is an integral part of ensuring the SIF will provide the risk reduction necessary. When modifications are made to SIF, testing can validate that appropriate SIF action will still take place.

This technical report is an informative document providing guidance on performing testing of SIF components and systems that will help achieve full safety benefits of the SIF in the most cost-effective way. Both manual and automated techniques are presented for off-line and on-line testing of SIF and the benefits of each technique described. Existing techniques and proposed new techniques will be described. Utilizing the techniques described in conjunction with an overall safety management program will allow users to meet the testing requirements of ANSI/ISA-84.01-1996 and IEC 61511. Techniques are described for testing all elements of the SIF including field sensors, final control elements, logic solvers (signal conversion modules included), Human Machine Interface (HMI), communication links with other systems, user application software, and other required auxiliaries such as power. Suggested inspection techniques for regular observation of equipment and components to detect potential problems are also presented.

The techniques described can also be used for testing burner management systems in conjunction with the NFPA 85 code.

These techniques are illustrated by the examples given in Annexes A-MM. **Each Annex is an example of how one company might apply a given technique, and is not intended to represent a consensus solution within the process industry.**

4 Audience

This document is intended as a guide for those responsible for specifying, designing, constructing, scheduling, implementing, and maintaining SIF applied to the process industries.

It is expected that those persons using this document will have adequate understanding of the ANSI/ISA-84.01-1996 standard and its requirements related to testing of SIS.

5 Definition of terms and acronyms

5.1 Definitions

5.1.1 approved substitution:

a replacement item for a component or system that meets the following requirements:

Is specifically permitted as a substitute or duplicate item in a company standard or practice (i.e., the company standard or practice clearly states that more than one brand and/or model number may be used interchangeably in order for a replacement item other than the exact same brand and model number to be considered for use as an approved substitute)

OR

Is approved as an equivalent substitute by the appropriate plant or company personnel, or his/her designee for approving substitutions; meets process-specific operational safety standards; and is covered by existing training and procedures.

See Annex A for an example of a typical approval procedure for making substitute replacements for SIF components.

5.1.2 automatic testing:

a test which consists of simulated process conditions to a logic solver which cause the logic solver to take specified action and signal a final control element to move to a specified position. The simulated process signal is implemented using another programmable device which controls the sequence and range of testing. Humans may observe the action of the system logic and final control element movement but do not intervene in the testing sequence. All steps of this test are documented by the testing device for validation of system performance to specified conditions.

5.1.3 car seal:

a technique consisting of a restraint placed on a valve actuator in such a manner that it cannot be moved from the “sealed” position without breaking the restraint seal. Operations personnel typically maintain a list of those valves “car sealed” in a fixed position for a process.

5.1.4 communications (external):

data exchange between the SIS and a variety of systems or devices that are outside the SIS. These include operator interfaces, maintenance/engineering interfaces, other SIS, etc.

5.1.5 electrical/electronic/programmable (E/E/PE):

logic technology that is based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology. The term is intended to cover any and all devices or systems operating on electrical principles and would include

- electro-mechanical devices (electrical);
- solid state non-programmable electronic devices (electronic); and

- electronic devices based on computer technology (programmable electronic).

5.1.6 field sensors:

field sensors include the process connections, the sensing device, the transmitter, and the signal connection to the logic solver.

5.1.7 final control elements:

final control elements include the signal connection from the logic solver, the actuation medium supply (typically air), solenoid valves, and the device which effects a process flow change (e.g., valves or pumps).

5.1.8 human machine interface (HMI):

the human machine interface includes the connection between the logic solver and the operator station, the graphical display device, the tools available for operating the system (hand-switches, mouse and keyboard) as well as a printer if supplied.

5.1.9 logic solvers:

in the case of PE devices, the logic solver includes the input module, main processor, and the output module. In the case of electrical or electronic devices, the logic solver may be a single relay or redundant, voting relays.

5.1.10 manual test:

a test which consists of simulating process conditions using the input device (i.e., transmitter) to a logic solver causing the logic solver to take specified action and signal a final control element to move to a specified position. Humans typically generate the simulated process signal using appropriate test equipment. Humans also observe the action of the system logic and final control element movement. All steps of this test are documented for validation of system performance to specified conditions.

5.1.11 off-line testing:

testing performed while the process or equipment being protected is not being operated to carry out its designated function. For example, a compressor is designed to take gas from a low-pressure state to a higher pressure state. If the compressor is not running (compressing gas), it is not performing its designated function. Off-line testing would be performed during the time the compressor is not running.

5.1.12 on-line testing:

testing performed while the process or equipment being protected is operating performing its designated function. For example, a compressor is designed to take gas from a low-pressure state to a higher pressure state. If the compressor is operating (compressing gas) while tests are performed on a transmitter providing an input to the SIF, this is an on-line test of the transmitter. When simplex input devices are used, performing such testing typically requires bypassing of the input function to the SIF. When redundant devices are used, bypassing may not be required, depending on the voting configuration.

5.1.13 permissive:

logic action that requires some condition be met before further actions can be taken. For example, a specific temperature might have to be achieved in the process before some additional chemical can be added; a lubrication system must be in operation before a pump can be started; or certain valves must be closed before others can be opened.

5.1.14 proof test:

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

5.1.15 replacement in kind:

an exact duplicate of a component or system or an "approved substitution" that does not require other modifications to the SIF as installed. See Annex A for an example of a typical approval procedure required for making substitute replacements for SIF components.

5.1.16 safety instrumented function (SIF):

a safety function with a specified safety integrity level which is necessary to achieve functional safety. A safety instrumented function can be either a safety instrumented protection function or a safety instrumented control function.

5.1.17 safety instrumented control function:

safety instrumented function with a specified SIL operating in continuous mode, which is necessary to prevent a hazardous condition from arising and/or to mitigate the consequences.

5.1.18 safety instrumented protection function:

safety instrumented function with a specified SIL operating in a standby mode to take action should a situation which could lead to a hazardous condition arise and/or to prevent the hazardous condition or to mitigate the consequences.

5.1.19 turnaround:

maintenance activities associated with a process, unit, or total plant which require that the process, unit, or plant be taken out of normal service and all equipment taken to a shutdown or out of service state.

5.2 Acronyms

ANSI/ISA	American National Standards Institute/Instrumentation, Systems, and Automation Society
BPCS	Basic Process Control System
CCF	Common Cause Factor
DCS	Distributed Control System
FMECA	Failure Mode Effect and Criticality Analysis
HMI	Human Machine Interface
ICS	Letters indicating a specific manufacturer of equipment
IEC	International Electrotechnical Commission
MTTF	Mean Time To Failure
PES	Programmable Electronic System
PLC	Programmable Logic Controller
PSAT	Pre-Startup Acceptance Test
RTD	Resistance Temperature Detector
SIF	Safety Instrumented Function



SIL	Safety Integrity Level
SIS	Safety Instrumented System
SOP	Standard Operating Procedures
SOV	Solenoid Valve
SRS	Safety Requirements Specifications
T/C or TE	Thermocouple
TMR	Triple Modular Redundant
UPS	Uninterruptible Power Supply
WDT	Watch Dog Timer

6 Off-line testing

The most common test of an SIF that uncovers failures or faults that may disable an SIF is the off-line, functional test. This test is performed while the process being protected is not in operation thus allowing all features of the 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. The basic requirements of this test are described in ANSI/ISA-84.01-1996 in Clause 9.7 Functional Testing. There are, however, multiple ways that tests can be performed to accomplish the purpose of this functional test. This clause will describe techniques and procedures that are known to be effective in carrying out the functional test to uncover faults or failures, which could result in potentially unsafe conditions in the process.

Each SIF included in the SIS should be identified. All inputs, outputs, and logic associated with each SIF should be identified. A testing procedure should define how each SIF will be validated. All equipment necessary for performing testing should be identified and verified suitable for tests to be performed. This includes calibration equipment with traceable performance.

If any components are shared among multiple SIF, testing should take this into account.

NOTE The procedures identified refer to SIF exclusively. Similar procedures should be available for all systems with limited monitoring such as equipment protection systems. These procedures are outside the scope of this document.

There are two important questions that should be addressed related to off-line testing – (1) when should off-line testing be performed and (2) how should the off-line testing be performed. These questions are addressed in the clauses to follow.

6.1 When should off-line testing be performed

6.1.1 General considerations

Off-line testing of the complete SIS should be performed prior to introduction of hazardous chemicals to the process. This is described as the Pre-Startup Acceptance Test (PSAT) in ANSI/ISA-84.01-1996 Clause 8.4. This test should be a final validation that the system can in fact perform the function(s) for which it was designed. Off-line testing allows each SIF to be completely tested including the application software and any equipment and associated logic provided for on-line testing.

NOTE After the initial PSAT has been performed, any subsequent tests that validate all SIF in the SIS before placing the system back in service may be referred to as a full functional test.

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

- The test interval included in the performance calculations for the SIF. See ANSI/ISA-84.01-1996 Clause 4.2.6.
- When changes are made to logic, impacting the function of the SIF. See ANSI/ISA-84.01-1996 Clause 4.2.14.
- When the process or equipment is taken out of service for scheduled maintenance activities that require work involving components of the SIF. See ANSI/ISA-84.01-1996 Clause 4.2.13.
- Company policy requiring complete testing of the SIF on a predefined schedule. See ANSI/ISA-84.01-1996 Clause 4.2.13.
- After extended down time of the SIS (see deferral of testing section Clause 6.2)

No modification, which could alter any of the following, should be made without first carrying out a review to ensure the change cannot reduce the level of protection and appropriate testing is done to validate correct operation of the modified SIF:

- Performance of a Safety Protection Layer for the original design intent
- Materials of construction
- Mode of operation
- Operating procedures
- Alarm and trip settings
- Speed of response
- Testing intervals or methods
- Device type, other than replacement in kind
- Architecture or voting logic
- Diagnostics

Dependent on the nature of the repair work, which has been completed, functional testing after repair to a SIF component may include the following activities. When the test does not involve a complete functional test of the component, the test does not alter the specified SIF testing frequency.

- 1) Single input: exercise sensor input and verify alarm and trip setpoints are correct then observe output(s) action. Confirm the process sensor is still connected to the correct input. Use the applicable section of the SIF test procedure and complete the required documentation for the equipment checked.

- 2) Single output: exercise all inputs that will actuate desired final control element and observe output action. Confirm final control element is connected to correct output. Use the applicable section of the SIF test procedure and complete the required documentation for the equipment checked.
- 3) Logic: perform a complete functional test of all SIF affected by the repair using the functional test procedure and complete all documentation. Check for cross contamination in the application software/logic by monitoring for unexpected actions across/between SIFs.

Follow-up testing of individual components in a SIF may be considered at intervals shorter than the complete functional test of the SIF to improve the performance capability of the SIF. Factors, which can impact the frequency of these tests, include

- sensors and final control elements installed in severe environment;
- accuracy of measurements required for safety;
- need for positive isolation of streams by valve action;
- mechanical wear and tear on components; and
- desire for longer test interval between complete functional tests.

In selecting a test interval for an SIF to match the SIL determined during the hazard and risk analysis of the process, the severity of the process characteristics should be considered. For example, a shorter test interval might be used initially for process fluids that are known to be more severe (corrosive, erosive, tending to plug, etc.). The minimum test interval should be determined by the user based on the SIL assigned to the SIF. Typically, annual testing is a reasonable starting point for the determination, which should include the examination of the component failure rate in the operating profile, the voting architecture, and the component diagnostics. The test interval chosen should be re-evaluated periodically and adjusted accordingly, based on the results of several functional tests. Based on user experience, shortening the test interval will not correct a faulty design or equipment problem. Instead, shortening the test interval will at most only allow earlier detection of an equipment problem.

It may also be appropriate to establish a maximum period of time between full functional tests of SIF that does not exceed 3-5 years. Few processes can operate for longer periods of time without some maintenance activity requiring process shutdown, and test schedules should not range beyond these shutdown schedules. There may also be some questions concerning the applicability of the failure rate data used in the SIL verification calculations and subsequent test interval determination that would point toward setting maximum test intervals for the SIF.

The incorporation of internal or external diagnostics in the SIF design often results in the reduction of the required test interval due to the ability to detect faults on-line. Diagnostics may not be able to detect all faults of the component. For example, a plugged tap may not be detected by internal diagnostics within the transmitter, but may be detected using external diagnostics (i.e. comparison of redundant transmitter analog signals using a PE logic solver). Consequently, any diagnostic should be carefully evaluated to determine which faults could be detected by the diagnostic prior to using the diagnostic as justification for reduction of the testing interval.

6.1.2 Sensors (transmitters, switches)

Whether switches or transmitters are used for input signals impacts testing requirements. Transmitters provide signals which indicate the current status of the variable being measured. This gives an indication that the input device is functioning. A switch on the other hand gives no indication of its status until the process variable passes through the trip point of the switch. Therefore, it may be necessary to test switches more often than transmitters used as input devices to SIF.

Transmitters can also provide diagnostics such as out-of-range high/low and out-of control range indications which switches cannot do. Such diagnostics may reduce the frequency of testing required for transmitters.

The calibration stability of an input device may require testing frequencies that are shorter than that for the complete SIF. Devices that are known to drift due to environmental changes in temperature, for instance, may require more frequent testing and calibration to ensure proper process variable input to the SIF. Devices that maintain their calibration stability through wide changes in temperature may not require frequent testing as long as a signal consistent with other process conditions is being transmitted from the device.

Redundancy of components may impact their testing frequency. Where redundant sensors have their outputs monitored and they are compared with each other, agreement usually means viable measurements which do not need frequent testing or calibration. When the outputs drift apart, testing or calibration is indicated for all the redundant components.

Diversity in the detection of the hazardous condition can provide a means to improve the SIF availability without adding redundant components. For instance, a pressure measurement may be used in redundancy with a temperature measurement for some process conditions. A comparison of the temperature and pressure to expected thermodynamic data can provide diagnostics on the validity of the process measurements, reducing the required testing interval.

User experience with specific sensors and service should be used in determining the test frequency of the device to ensure proper performance of a sensor.

Some companies require yearly performance checks of sensor calibration and verification of set points. Other companies have established testing frequencies based on past history with the equipment they use. **Established company policy for testing frequency should take precedence if more frequent than the guidelines of this document.**

6.1.3 Logic solvers (E/E/PE)

When changes are made to the logic solver, the potential effects of these changes must be evaluated to determine how much of the E/E/PE must be tested. If the program changes can be isolated to a particular section, and it can be shown conclusively that the change does not impact other logic implemented in the logic solver, only that section needs to be fully tested (complete functional test). This applies to logic whether it is electromechanical relay based, solid-state relay based, pneumatic, or Programmable Electronic System (PES) based. Where Watch Dog Timers (WDT) are implemented as external diagnostics on PE logic solvers, they should be tested at the same frequency as the logic solver. For guidance in testing WDT see the American Institute of Chemical Engineers, Center for Chemical Process Safety, guideline series book, "Guidelines for Safe Automation of Chemical/Petrochemical Processes."

Some companies require that functional performance of logic solvers be verified on a schedule that ranges from one year to several years depending on the risk associated with the process, the complexity of the logic, and company experience with the logic solver being used.

6.1.4 Final control elements (valves, motors)

Valves used for final control elements should be tested when full system functional tests are performed. They should be tested at the frequency used in the performance calculations for the SIF. Final control element (valves) should be tested each time the process is taken out of service. This can typically be performed by verifying appropriate operation of all valves when the process is taken out of service (either manually or due to a failure of some nature that caused the process to trip). For batch operations, verification of proper operation during each batch should provide this function.

Other devices used as final control elements such as motors should be tested at the frequency used in the performance calculations for the SIF.

Frequency of testing valves as final control elements depends on a number of factors:

- Type of valve used as the final control element
- Service in which the valve is applied
- Whether the valve is used during normal operation or as a standby valve for use only when the SIF takes action
- Whether the valve must provide minimal leakage isolation or some leakage can be tolerated
- Whether the valve actuator has a spring to drive it to the safe state or it depends on motive power to drive it in both directions

When testing final control elements, auxiliaries such as valve positioners, position or limit indicators/sensors, air pressure regulators, etc. should be tested at the same frequency as the valve.

6.1.5 HMI

The Human Machine Interface (HMI) should be tested at the same frequency as the full SIF. When changes are made to information displayed in the HMI, the changes should be tested to confirm appropriate status is displayed. If the HMI is used to initiate the SIF logic, all devices associated with the initiation should be tested, including the HMI, output circuit, and final element.

6.1.6 Communications

Communications between the SIF and other control equipment such as the Basic Process Control System (BPCS) should be tested at the same frequency as the SIF. When completing full functional tests of the SIF, the testing should include all communication to auxiliary equipment such as the DCS. When changes are made to the communications links between the SIF and any other equipment, testing should confirm that appropriate information is being communicated.

6.2 Deferral of scheduled testing of SIF

Documented justification for deferral of scheduled inspection and/or testing activities should make use of failure rate data and/or quantitative methods to establish that the design intent and the performance requirements are not compromised. Company or plant-specific failure rate data for the process of concern should be used when available, because this provides the best estimation of component performance. When company or plant specific data is not available, published failure rate data can be used as long as it has been determined that the data agrees with past operational experience and includes the failure modes of interest. The method(s) used for validating the failure rate data should be appropriate to the complexity of the system and the severity of the event consequence.

Scheduled testing of SIF may be deferred if it meets the following criteria:

- The equipment that the SIF is protecting is out of service. An analysis of the impact of such a deferral on the SIF provided should be made prior to the decision to defer. The SIF should be tested prior to the equipment being returned to service in this case.

A plant turnaround is scheduled shortly after the scheduled full functional test of the SIF. This turnaround will allow a complete functional test of the SIF. The time period of this delay should not result in a compromise of the SIF or its safety integrity level. When the SIF is designed with the intent to be full

functional tested every three to five years, the time delay should not exceed three months unless a safety assessment has determined that the longer delay would not compromise the SIF.

See Annex B for an example of a deferral procedure for SIF testing. The approval process, including levels of management and technical responsibility required for deferring a scheduled test, should be pre-determined, understood, and documented before an SIF is put into service

6.3 How to perform off-line testing of SIF

6.3.1 General guidelines

This clause will outline techniques for performing tests that have been proven and some proposed techniques, including automated techniques that can achieve adequate off-line testing of SIF. The advantages and disadvantages of each technique will be discussed where appropriate.

A key question concerns whether testing of the SIF must be done as an integrated system or whether various parts of the SIF can be tested at different times and credit be taken for the testing required to achieve the SIL specified. The requirement for testing stated in ANSI/ISA-84.01-1996 does not say that all testing of the SIF must take place at the same time. However an integrated test must be performed as the Pre-startup Acceptance Test (PSAT) (ANSI/ISA-84.01-1996, clause 8.4), prior to introduction of hazardous chemicals to the process, to ensure that the SIF can provide the functionality specified in the safety requirement specification. After that, the user is free to structure testing consistent with the integrity requirements of their SIF.

It is highly recommended that a complete functional test of the SIS including all implemented SIF be performed on some prescribed interval to ensure proper functioning of the entire system. Where the dynamics of the entire end-to-end SIF is crucial—i.e., the thermowell, the T/C, the transmitter, the input cycle time, the logic cycle time, the output signal cycle time, as well as all necessary components of the final control elements, such as volume boosters, pneumatic tubing size and length—the complete SIF should be tested together to ensure specification compliance.

Why would a user desire to perform non-integrated testing of the SIF? Testing is looking for dangerous unrevealed or covert failures that have taken place and would prevent a SIF from performing its function. Whether these are uncovered piecemeal or in a total integrated functional test is immaterial. The important factor is that they are discovered and corrected before a demand is placed on the SIF and it cannot perform the specified function.

The properly applied logic solver is generally the most available component of the SIF and thus should require complete tests less frequently than the field devices. Sensors can easily be tested on-line when provisions for testing and/or device redundancy is included in the design. Valve testing may require bypassing in order to perform a full functional test, when a short interruption of the process cannot be tolerated. But, the valve may be partially tested while in operation with a complete functional test performed off-line. Any partial testing should be evaluated to determine which failure modes and components are tested during the partial test, so that this can be considered in the SIL verification calculations. It should be emphasized that provision for this non-integrated testing of SIF components must be factored into the SIF design as required in ANSI/ISA-84.01-1996, Clause 7.9 and into the SIL verification for the SIF.

Many recognized and generally accepted good engineering practices such as NFPA and FM suggest on-line testing of valves using the process chemicals at normal operating pressure to do performance testing. This often provides better validation of the functional performance of the valve and can be a cost-effective alternative to removing the valve and taking it to a calibration facility. This type of testing could be performed as a part of a scheduled shutdown of the process with the appropriate documentation of results.

6.3.2 SIF component calibration and performance validation

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

6.3.3 Calibration procedures

Calibration procedures should be available for each type of component in the SIF. In general, calibration procedures recommended by the manufacturer of the component should be used. Where additional requirements (e.g., response time of sensors or valves) are necessary to meet the specified function in the SIF, these should be taken into account in the calibration procedures.

Procedures for calibration of SIF components should include a final step in which Operations verifies the "reasonableness" of the newly calibrated, field sensor(s) actual process readings. This step is very important to minimize the likelihood of a Common Cause Failure (CCF), during calibration of redundant process sensors.

NOTE Common cause calibration failure can arise where redundant sensors are calibrated at the same time by the same person using the same test equipment or standard. Where an instrument technician mis-calibrates one sensor, he/she is very likely to mis-calibrate the other(s). Special concerns for these failures arise in calibration of redundant process analyzers using a single mixed sample and SIL 3 safety controls in batch processes.

Table 1 offers guidelines for calibration tasks and resources for calibration of SIF components:

Table 1 — Calibration work process for SIF components

Devices Being Calibrated	Calibration Tasks and Resources
Most SIF Components	- Trained staff using plant procedures and/or technical data on an "as-needed" basis when performing periodic component calibrations. - Calibration procedures and/or vendor technical data that include step-by-step calibration instructions applicable to each SIF component are available.
Safety instruments not covered in specific Maintenance Staff Training	Skilled staff using manufacturer's step-by-step calibration instructions to calibrate devices that are not part of the staff maintenance qualification process.
Process Analyzers	Analyzer calibration may require special considerations in addition to using the manufacturer's step-by-step calibration instructions. Example: Limited availability of check-gas may make executing a standard three-point calibration difficult. A calibration procedure that proves operation using one known composition sample that is close to the safety-critical trip point is often adequate.

Many field devices require periodic calibration and checkout to ensure that the process service has not affected the device's ability to respond to process changes. The use of redundancy in process measurements will allow early detection of many device failures, reducing maintenance costs by focusing

efforts on known problems. An example¹ of what might be achieved in a reasonable process service with instrumentation redundancy is as follows:

- Smart pressure transmitters can go 2 to 4 years between calibrations.
- Coriolis and magnetic flow meters should not be calibrated unless there is evidence of a problem. *(Coriolis and magnetic flow meters should be calibrated using a prover loop at turnaround.)*
- Smart four-wire RTD transmitters should only be calibrated if there is evidence of a problem.
- Smart thermocouple transmitters can go 5 years between calibrations.
- Vortex meters should only be calibrated if the kinematic viscosity permanently changes.
- Radar level gauges should only be calibrated if vessel internals change.
- Smart nuclear level gauges should only be calibrated if process density permanently changes.
- Smart digital positioners on valves should only be calibrated when valves are overhauled.

6.4 Component testing

Both general and specific guidelines are presented in the following clauses for performing off-line testing of SIF components.

6.4.1 General guidelines

Verify permissive values of field sensors and any other devices such as timers used in permissive logic. Note that permissive logic may have manual or logic implemented bypass capability for startup. Both techniques, if provided, should be tested prior to placing the SIF in operation. Verify all alarms and or lights associated with each sensor and switch by observing and documenting correct indication when alarm conditions are reached. See Annex P for a model procedure for testing permissive logic.

Verify all hand trip switch action by observing and documenting observed action when switch is actuated.

An example of a test procedure for a simple SIF is shown in Annex Q.

Table 2 provides general guidance on testing required for verifying proper operation of components typically used in SIF.

¹ *Process/Industrial Instruments and Controls Handbook*, edited by Gregory K. McMillan, Fifth Edition, copyright 1999.

Table 2 — Tests performed to verify operation of SIF components

To verify the operation of ...	Test ...
sensors	- the operation of the complete field sensor, including - primary sensing element, - switch or transmitter, - wiring, and - logic solver input module.
logic solver	- the operation of the logic solver, including - hardware and software associated with each input device, - combined inputs, - trip setpoints, - operating sequence, - diagnostics, and - computations.
alarm functions	operation of alarm functions and readout, including the alarms that signal the bypass of automatic trips
final control elements	- the operation of the complete final control element, including - logic solver output module, - wiring, - actuation device (e.g. relay or solenoid), and - final control element affecting the process operation.
safety system functions	- individual SIF and complete system functionality, - speed of response, when a safety parameter must act in a specified period of time, - manual trip function to take the SIF outputs to a safe state, - user-implemented diagnostics, and - SIF operability following testing. NOTE A separate manual trip function, which is not dependent on SIF logic solver, is recommended per ANSI/ISA-84.01-1996 and this function should also be tested.

Where repair or replacement of SIF components has taken place, the guidance in Table 3 may be used.

Table 3 — Calibration and testing guidance for repaired or replaced components in SIF

Field Device Examples: transmitters computational relays switches, and valves.	• Calibrate the transmitter; verify switch setting and valve stroke • Verify correct operation of replacement/repaired component in the SIF; e.g., ❖ Functional testing of all inputs and outputs of the repaired or replaced component. ❖ Functionally verify correct signal flow from replacement transmitter-to-next component in SIF (typically the Logic Solver) ❖ Functionally verify correct signal flow from Logic Solver to replacement valve
Logic Solver and/or I/O module	• Input-to-output functional tests of a replaced Logic Solver component (e.g., a CPU card, and I/O module) is not necessary if the Logic Solver system contains internal self-diagnostics and reporting that verifies component operability.
All	• Document the component calibration and performance verification. NOTE Documentation for replacement of a Logic Solver component includes recording diagnostic information observed that proved component operability.

A test to confirm SIF action on total power supply failure should be carried out and if battery supplied power is provided, it should also be tested to confirm that desired time of backup is available.

Measure the power supply voltage, AC or DC, for the SIF components and verify that the power is within the acceptable range (AC ± 2.5 volts; DC ± 0.4 volts).

Check the power line-to-ground voltage and the phase angle between the current and voltage for each phase line for motors, heaters etc., where applicable.

6.4.2 Component specific guidelines

6.4.2.1 Sensor testing – transmitters

Testing sensors may involve (1) use of process to drive transmitter, (2) simulating the sensor input via appropriate measurement source, or (3) simulating the sensor output via a mA simulation tool. The particular technique used should be specified in the test procedure for the SIF. Using the process to drive the transmitter will provide assurance the transmitter can measure the process conditions but this technique may not always be available if the process is not in operation. Using simulated measurement input to the transmitter is probably the most reliable and available technique. This technique tests the function of the transmitter, the wiring, and the receiving device. Using a current simulation on the output tests the wiring and the receiving device but does not test the transmitter function.

Measure the sensor output conditions; if the output is linear, measure the output level with respect to the current process condition such as temperature, pressure, product level etc.

Sensor testing will vary depending on the type of sensor used. The guidelines which follow outline proven in use techniques for verifying sensor operation in the SIF.

Root valves on all sensors should be verified open at end of test. Secondary valves, manifolds, vents, etc., on all sensors should also be verified as being in the “in the service” condition at end of test.

Each individual component's off-line condition should be checked and verified based on the expected value with respect to the process off-line conditions.

6.4.2.2 mA pressure transmitter

Refer to Annex NN for example procedure for testing mA pressure transmitters.

Table 4 is an example of a way to document test results for this testing.

Table 4 — Sample documentation for high alarm and trip settings

Pressure Input	Input Range P1234 (0-xxx psi) (0-yyy " H ₂ O)	High Pre-Alarm Setpoint P1234 (xxx psi) (yyy "H ₂ O) (zzz mA)	High Trip Setpoint P1234 (xxx psi) (yyy " H ₂ O) (zzz mA)	Pre-Alarm Setpoint (As Found)	Pre-Alarm Setpoint (As Left)	Trip Setpoint (As Found)	Trip Setpoint (As Left)
PT1234							

Note that this same procedure can be used for differential pressure transmitters with the appropriate test equipment.

6.4.2.3 mA temperature transmitters

See Annex PP for example procedure for testing mA temperature transmitters.

6.4.2.4 mV temperature transmitters

See Annex QQ for example procedure for testing mV temperature transmitters.

Table 5 is an example of how temperature transmitter testing might be documented.

Table 5 — Sample documentation of high temperature alarm and trip settings

T/C Input	T/C Fault (Upscale Burnout) T1234	Input Range T1234 (0-xxxx Deg F)	High Pre- alarm Setpoint T1234 (xxx Deg F)	Pre-alarm Setpoint (As found)	Pre-alarm Setpoint (As Left)	High Trip Setpoint T1234 (xxx Deg F)	Trip Setpoint (As Found)	Trip Setpoint (As Left)
TE1234								

6.4.2.5 Process analyzers

Process analyzers should be calibrated in accordance with manufacturers' specific instructions.

Signals from process analyzers to SIF are typically current signals representing values and ranges of components being measured. Verification of correct setpoints for pre-alarm and trip values should be done using current sources in like manner to that for other current transmitters. (See Annex NN.) As found and as left values for pre-alarm and trip setpoints should be documented.

6.4.3 Sensors – switches

6.4.3.1 Pressure switches

See Annex RR for example procedure for testing pressure switches.

6.4.3.2 Temperature switches

See Annex N for example procedure for testing temperature switches.

6.4.3.3 Level switches

Testing of level switches can be performed using the procedure outlined in Annex K. This procedure was developed for use in on-line testing but is applicable for off-line testing as well.

6.4.4 Miscellaneous sensors

This clause will offer guidance for testing a variety of sensors that might be included in SIF.

6.4.4.1 Vibration monitors

Refer to Annex C for example procedure for testing vibration monitors.

6.4.4.2 Thrust position monitors

Refer to Annex C for example procedure for testing thrust monitors.

6.4.4.3 Overspeed trip

See Annex D-1 and D-2 for example procedures for testing overspeed trip logic.

6.4.4.4 Permissive start of turning gear motor

See Annex E for example of a turning gear motor permissive start test procedure.

6.4.4.5 Lube oil pump auto start test

See Annex F for example procedure for lube oil pump auto start test.

6.4.4.6 First out alarm tests

See Annex G for example procedure for testing first-out sequence alarms.

6.5 Logic solver test procedures

Use SIF-specific functional test procedures when testing the logic solver. Functional test procedures may include

- written procedures;
- logic diagrams;
- control loop drawings;
- electrical control schematics; and/or
- checklists.

Using HMI, test each SIF manually by creating each fault condition and verifying proper response on the HMI and observation of the final control device(s).

Using PLC programmer for the logic device being tested and HMI screen, test the logic programmed function by function. Thoroughly check and verify the internal scaling factors for calibration and test range limit flags with manual input and output value variation. Test each individual sensor, the measured value with separate certified Test Meter and the value measured in PLC. Verify that the PLC value is scaled to match the Test Meter measured value. Performance should be considered unacceptable if variation between Test Meter measurement and Logic Solver indicated values exceeds $\pm 2\%$ of measurement range.

Validate logic solver performance by executing the appropriate procedure from the following tests.

6.5.1 Complex application logic systems

For an example functional test procedure for a complex application logic system, refer to Annex H.

6.5.2 PLC logic solvers connected to field devices

An example of a test procedure for complex logic that involves field devices also included as Annex R.

6.5.3 PLC logic solvers connected to simulators – Hardwired simulators

Some companies have developed hardwired simulators for use in testing PLC logic. These simulators consist of panels with potentiometers, lights, and switches to represent all input devices and lights to represent output device positions. The simulators may be connected to the input terminals of the PLC directly or an arrangement using plug connection cables may be used. With the simulator connected, a procedure which exercises all possible combinations of logic that the PLC might encounter is conducted to validate that the logic solver will perform as required for each safety function implemented. In some instances the simulation panel is arranged graphically to represent the process being protected. When this is done, the simulator can also be used as an operations training tool for the SIF functionality.

6.5.4 PLC logic solvers connected to simulators – Software based simulators

Some companies have developed software-based simulators to accomplish the testing described in the clause above. In this instance, the test program is developed in application software using another PLC or in some instances a personal computer. Connection to the logic solver for testing is similar to above. However, the use of such a simulation requires complete validation of the embedded, application and utility software in the simulator prior to testing the SIF Logic Solver. The software simulator might also be used in training operators in the functionality of the SIF. In some instances this software simulator might operate in an automated mode in performing the test.

6.5.5 PLC logic solvers not connected to field or simulators

Testing PES based logic solvers that are not yet connected to field devices or a simulator is limited to manual testing of application logic using the PES configuration device. This type of testing primarily takes place during the initial programming and configuration phases of the PES implementation for the SIF application. Since changes are numerous during these phases, formal documentation of this "testing" should not be necessary. The final application logic documentation should reflect the results of this testing.

6.5.6 Electromechanical relay logic solvers

See Annex T for an example of a procedure for testing an electromechanical relay based SIF.

6.6 Testing of final control elements

Manually open or close valves and start or stop motors individually. In some applications, this test might have to be repeated 2 or 3 times to ensure proper functioning of the valves. Failure to properly open or close on the first attempt might be considered a failure by some companies and repeating the test 2 or 3 times to see the valves function would not ensure proper operation when the SIF called for a trip. Others might just want to see the valves operate more than once to obtain a confident feeling of proper functioning.

Manually change the output value for linearly controlled devices such as control valves. Observe the response of the device by watching the feedback value on the HMI and directly at the device. Document response of each valve in field and indication on HMI.

A test of the SIF valve should determine whether the valve can meet the functional requirements provided in the safety requirements specification. In addition to full stroke testing, the valve test may involve leak testing in cases where the valve has been specified with a maximum leak rate. Stroke times may be determined and recorded if valve stroke speed is critical. Stroke time should include the time from output signal change to valve position change, not just from start to finish of valve stroke. It has been shown

that the pre-stroke dead time as actuators fill or exhaust and achieve breakaway force on the valve is generally the longest time component of the total stroke time.

Leak testing of SIF valves may require installation of bleed valves with pressure gauges downstream of the valve so that the valve can be monitored for positive shutoff. The burner management standard NFPA (8502)² gives guidance on this for fuel valves to furnaces and boilers that is also applicable to other process valves requiring positive shutoff.

6.7 Testing solenoid valves

Verify solenoid valve normal and trip condition status. If solenoid is normally energized during process operation, verify that coil is energized and no air is venting through vent port. If solenoid is normally de-energized during process operation, verify that coil is de-energized and vent port is open to vent. De-energize or energize coil as required and verify that air is either vented from valve actuator or applied to valve actuator as required by SIF logic. Verify that solenoid installed position allows gravity assist in taking valve to de-energized position. For examples of testing solenoid valves see example procedures for testing of final control elements (Annexes W, Z, DD, and MM).

6.8 Testing of HMI

All indications of SIF variables that are displayed on a human machine interface whether they be the BPCS operator workstation, a separate operator display station, or lights on a panel should be verified as each variable is tested. The correct range of process variable, the pre-alarm and trip setpoints, and any other variable information that is provided should be verified and documented during the testing. Both as found and as left values should be documented. Where multiple pages (video, CRT, etc.) of SIF information are provided, all displayed pages should be verified for appropriate labeling and access control.

If the HMI is used to initiate output functions for the SIF such as may be the case in batch control applications or a manual shutdown function, this function should also be tested.

6.9 Testing of communications

Where provided all communications with other systems such as the BPCS should be tested to verify correct transfer of information and data from the SIF to the other system(s). All information transferred should be verified by comparing the sent information with the received and displayed information on the system(s) other than the SIF.

Techniques used for blocking communications from the BPCS operator workstation to the SIF logic solver, especially those used to prevent unintended logic changes to the SIF application software, should be validated. Attempts at changing logic in the SIF should be made from the BPCS operator workstation to verify that this action cannot take place. The security technique used to protect against changes to logic from the configuration station should also be tested. If this involves connecting the configuration station only when changes are to be made, verify that another PES station cannot perform this function. If password protection is the technique used, verify that the password cannot be easily discovered through normal "hacking" in computer software. This is especially important if the SIF display station is also used as the configuration station with key lock and or password protection.

Where a separate operator display station is provided for the SIF, tests should confirm that changes to logic in the SIF logic solver cannot be made from this station.

² NFPA 8502, published by the National Fire Prevention Association.

6.10 Final SIF test procedures

Verify that all inputs, outputs and logic are in correct state at end of test and ready for process startup to proceed. This includes removing all bypasses, jumpers, etc. and returning all final control elements to pre-startup positions. Verify that any temporary jumpers used for bypassing are accounted for by comparing to list provided for each SIF. See Annex J for example of a jumper control list.

Perform a final inspection on the logic solver and all SIF components. The intent of this inspection is to make sure all work on the SIF is complete and that the system can safely be returned to normal operation. The inspection should include, but not be limited to, the following items.

- Verify that all alarms are cleared. Exceptions might be low process variable alarms that cannot be satisfied until process has been advanced to some operation state other than out of service.
- Verify that all problems and failures identified have been addressed.
- Check any components and devices that were replaced to ensure proper working condition.
- Verify all switches and hand switches are in their proper positions.
- Visually inspect all SIF pressure and instrument gauges to insure proper working condition.
- Visually inspect tubing, wiring terminations, and wiring to insure that they are secure. This might include actually trying to pull wire from the connections.
- Verify that all final control elements are in the correct position for the process out of service state.
- Verify that all instrument air supply regulators are at their proper settings.
- Verify that field junction boxes and housings are secured and weather tight.
- Verify that all wiring conduit and conduit access plates are secure and weather tight.
- Verify that all process root valves to transmitters and switches are open and any bleed valves are closed.

7 On-line testing

Successful on-line testing requires planning, design provisions, and procedures. When possible, the SIF should be designed to minimize or eliminate the need for bypassing or jumpers for testing. Any installed equipment for on-line testing, such as bypasses or instrumentation, should be thoroughly tested, along with its associated logic during commissioning. Detailed test procedures are essential for on-line testing to ensure that the test is correctly implemented. It is important to emphasize that any on-line testing presents the risk of a process upset or unintentional shutdown as the result of an incorrectly performed test.

7.1 Preparation

Prior to any on-line 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 group should review the following items at a minimum:

- Discuss the importance of operators on shift being given notification that a SIF system is about to be tested or worked on.

- Review the SIF system description.
- Review the SIF system functional test procedure.
- Discuss whether the on-line test will affect other systems, such as the BPCS, alarms, or other SIFs.
- Discuss the work scope, exactly what will be checked, what flows, pressures, temperatures, levels, etc.
- Discuss why craftsman should notify the operator when activating each alarm.
- Discuss what devices will no longer function when bypassing the system.
- Review with Operations any special precautions required during the test.
- Discuss what operations and maintenance should do if an unplanned SIF trip occurs while the input being tested is in bypass.
- Discuss what operations and maintenance should do if the operator must initiate the SIF while the bypass is in place.
- Discuss what procedures will be used to ensure that the SIF is returned to service once the SIF testing is complete; e.g., automatic verification, independent review, etc.

7.2 When should on-line tests be performed

On-line testing should never be performed when it would compromise the safety of the process.

The SIF components should be calibrated based on the plant's Preventative Maintenance (PM) schedule for the process equipment. The calibrations should be performed according to the company calibration procedures.

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

Testing SIF on-line introduces stress on both the process and those performing the testing. It is therefore imperative that on-line testing be performed under closely controlled conditions using procedures that have been proven. This section will outline guidelines for when such tests should be performed and how this can be accomplished without compromising the safety of the process.

7.2.1 Sensors

Process sensors that are going to require on-line testing should generally be installed with some level of redundancy to allow testing of one sensor while another is still making the necessary measurement. If on-stream reliability of the process is critical, a 2oo2 or 2oo3 voting of sensors may be used. The designer then determines whether bypasses will be used to facilitate testing. For either 2oo2 or 2oo3 voting, one sensor can be tested at a time without the need for bypasses. When on-line diagnostics are used to detect transmitter failure, the designer determines whether the voting logic will be changed. For example, the logic for the SIF may be reduced from 2oo3 voting to 1oo2 if a failed transmitter is voted toward the trip condition. In contrast, it would reduce from 2oo3 voting to 2oo2 if the failed transmitter is voted away from the trip condition. If a 1oo2 configuration is used for sensors, a bypass will be necessary to allow on-line testing of each sensor while maintaining measurement capability with the other sensor.

Logic during such a test will reduce to 1oo1, which is a lower SIF integrity than the 1oo2, and appropriate precautions should be taken during the testing to ensure safety is not compromised.

The testing frequency for sensors can be more or less frequent than that of other SIF components depending on the MTTF of the components used and the voting configuration. Where analog sensors are installed in redundant configurations, the testing interval for individual sensors can often be extended due to diagnostic coverage provided by analog signal comparison and alarming on deviation of the signals. Testing and calibration of the sensors would then be performed when the deviation alarm is generated. Depending on the voting configuration, on-line testing may not be necessary to maintain SIF integrity. This assumes that common cause failures such as mis-calibration of all three sensors has been accounted for in the calibration procedures.

7.2.2 Logic solvers

Testing of logic solvers for SIF is not practical while the process is on-line. Therefore the full functionality of the logic solver should be tested and validated prior to placing the SIF in operation as a layer of protection for the process. Further testing of the logic solver should be performed at the scheduled down time for the process and any time the SIF is taken out of service for logic changes.

7.2.3 Final control elements

Final control elements often have limited on-line diagnostic capability. Consequently, final control elements generally contribute the greatest amount toward the probability to fail to function when a demand is placed on the SIF. These devices typically remain in one position for long periods of time without moving until they are called on to respond to a process demand. Final control elements may also be installed under process operating conditions that can be severe, e.g. corrosive, plugging, or polymerizing services. They also contain many moving parts which must function together to accomplish the desired action they are to perform. Since the test interval to achieve the required safety integrity is often shorter than the turnaround interval for the process, on-line testing of final control elements becomes a desirable alternative.

Whether simplex or redundant valves are utilized, on-line testing requires additional design provisions, e.g., full flow bypasses, partial stroke testing equipment, test instrumentation, etc., to allow testing to occur without process interruption.

Final control elements may have common components, which could render multiple devices unavailable when these common components fail. For example, if air were used to move valves, which are used for process isolation, the loss of air supply would be a potential common cause failure. If the air supply fails to provide the necessary pressure or volume to move either of the valves, the SIF will fail to accomplish its design function.

The testing interval required to achieve the SIF integrity is affected by the severity of the service the valve encounters. Temperature (high or low), erosion, corrosion, and polymerization are a few of the factors which may have an impact on the required testing interval. In many cases, on-line testing is required in order to achieve the SIF integrity. On-line testing may consist of a full functional test or a partial test of the valve failure modes. When on-line diagnostics or partial stroke testing is used to supplement full functional testing, an assessment of the failure modes detected by the diagnostics should be performed. The diagnostic coverage factor used in the SIL verification should be substantiated by failure modes and effects analysis (FMEA). Many users limit the coverage factor assumed in the SIL verification to a certain maximum, e.g. 60%. The SIL calculation is then performed by splitting the PFDavg calculation into two parts. A portion of the valve failure modes is tested at the partial stroke testing frequency. The remainder of the valve failure modes is tested at the full stroke testing frequency.

A visual inspection according to an approved procedure should be carried out regularly, e.g. every three months. See Annex O for a sample procedure or checklist for this visual inspection.

7.2.4 HMI

Testing of the HMI during normal operation of the process should be done any time that there is an indication of a malfunction of the HMI display itself. This could result from a fault in an input to the display or a fault in the display component itself. When repairs are made or a HMI is replaced, all features of the original HMI specified for the SIF should be tested.

The HMI should also be tested on the same schedule as the logic solver.

7.2.5 Communications

Communications between the SIF and other systems should be tested on the same schedule as the logic solver and at any time that there is an indication of a malfunction of the communication link. If communication with another system has an impact on the safety integrity of the SIF, the test interval included in the integrity evaluation should be used. Any on-line testing of a communication link should not reduce the capability of the SIF to perform its function.

7.3 Performing on-line testing

7.3.1 Precautions

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 control system operator should monitor the process continuously using means independent of the SIF. The operator should be capable of initiating a manual trip of the SIF or other installed systems in the event of a process demand during the test. Once the manual block valves are opened or closed, a dedicated field operator should be available to open or close the block valves quickly if a process demand occurs. All personnel involved in on-line testing of the SIF components should be aware of the mitigation steps to take in case a process demand occurs while the testing is in progress. The following caution should be included at the beginning of all on-line test procedures:

CAUTION — THE OPERATOR (S) MUST FULLY UNDERSTAND AND BE PREPARED TO IMPLEMENT THE MITIGATION PLAN FOR THIS PROCESS IN THE EVENT THAT A TRUE TRIP DEMAND OCCURS DURING THE CONDUCT OF THIS PROCEDURE.

Similar to the off-line testing procedure, measure the power supply voltage, AC or DC, for the SIS components and verify if the power is within the acceptable range. Test values should be within $\pm 2\%$ of normal values.

Check the line-to-ground voltage per line.

7.3.2 Sensors - Transmitters

Several examples of testing sensor (transmitter) logic on-line in SIS are shown in Annexes L, M, and V. In each of these procedures a slightly different approach is used but all of them accomplish the same result of verification of sensor operation and logic in the SIS.

7.3.3 Thermocouple test for 2oo3 configuration

See Annex Y for model procedure for performing a 2oo3 test of thermocouple operation and logic in SIF.

7.3.4 Sensors – Switches

7.3.4.1 Level switch technique

See Annex K for example of a procedure for on-line testing of a level switch.

7.3.4.2 Pressure switches

Pressure switches can be tested on-line using the same procedure as off-line tests with provision for bypassing the input during the testing.

7.3.4.3 Temperature switches

Only the output portion of temperature switches can be generally tested on-line. Use the same procedure as off-line tests for the output portion of the switch with provision for bypassing the input during the testing.

7.3.5 Logic solvers

In general testing logic solvers while the process is in operation is not recommended. The logic solver is typically the most reliable portion of a SIF and once the application program is fully validated by the PSAT, there is no need to retest the logic solver unless changes have been made to the logic contained in the logic solver. When changes are made to the logic, the logic solver should be retested prior to placing the SIF back in operation.

Testing electromechanical based logic solvers on line would require extensive modifications to allow this testing. These modifications could result in a system with less integrity than one without the provisions for testing. It is therefore not considered a good practice to attempt testing electromechanical based logic solvers while the process is on-line.

Where the SIF is functioning during a startup of the process, a test of SIF logic typically occurs each time the process is started up. If more frequent test intervals than the normal process turnaround schedule is required to achieve the SIL required, credit might be taken for unplanned startups due to downtime forced by equipment or utility failures.

7.3.6 Final control elements

On-line testing of final control elements can be the most difficult testing associated with the SIF. Any test of the valve on-line may result in process disruption if the test is not properly conducted. Valve tests can consist of a full stroke using process bypasses or a partial stroke to a specific percentage of valve movement. Any valve test should be evaluated to determine what failure modes are detected during the test. Of particular significance with respect to partial stroking of valves is that the partial stroke does not determine whether the valve will function to its full open or closed position. This can only be determined by a full stroke test.

Some companies take credit for on-line valve tests when an unplanned trip of the system takes place. They verify that all valves went to their correct position as required by the trip condition and that all indications of valve position indicated this to be true. They then document what has occurred and count this as a test of the valves affected. When taking such credit, consideration should be given to the performance requirement of the operation of the valve (i.e. speed of response and shutoff performance). The documentation should include the rationale for acceptance of the performance based on additional in-line testing while the opportunity is available or noting that prior testing could lead one to believe the performance is adequate until the next scheduled test.

Techniques have been devised to allow some measure of testing of final control elements, particularly valves. These include use of manual block valves around the SIF valve for use while the testing is being performed. A drawback of this approach is high capital cost and the chance of leaving them in the wrong position after a test has been performed. Using this technique requires special attention to operation of the manual valves before and during the test. Annex Z is an example of testing valves that have installed manual block valves for testing. A valve lineup procedure has been developed by one company to follow during testing involving manual block and bypass valves. The procedure follows:

VALVE LINE-UP ACTIVITIES

During the course of this test, the Technician Performing the Test will be instructed to have an Operator close the upstream manual valve associated with this system. Since the upstream manual block valve is Car Sealed, the Operator must first remove and dispose of the Car Seal before closing this valve. Closing the manual block valve shall be performed in accordance with all existing site procedures.

Upon completion of this test, the Technician Performing the Test shall inform the Operator the upstream manual block valve may be opened. Opening of the manual block valve shall be performed in accordance with all existing site procedures. The Operator must install and lock a new Car Seal on the manual block valve and record the Car Seal Number in the space provided at the end of this test.

Another technique involves testing only through the final solenoid valve on the final control element actuator. This is common practice by many companies today and allows validation of elements of the SIF except the movement of the final valve itself. In this type of testing, the air supply to the valve actuator from the final solenoid is shutoff to prevent venting the actuator and operating the valve when the solenoid is tripped. Since about half of the final control element failures probably involve the solenoid, this technique can account for about half of the potential failures of the final control element package.

Some companies use redundant solenoids on each SIF valve to improve the availability or reliability of the SIF. Dependent on the solenoid configuration, bypassing may be required to test each solenoid one at a time and to verify that the solenoid has vented. When the test is complete, the technician should verify that the solenoid has been returned to service. Simply testing that the solenoid coil has energized or de-energized is not a complete test, since the solenoid must move to a specified vent state for correct functioning. For example, a test of the solenoid coil will not detect that the vent port is plugged with debris, preventing the venting of the air from the process valve. The following provides an example of a test for dual solenoid which is implemented using a bypass valve on the air line and a defeat switch in the logic.

- a) Turn the bypass valve slowly to "Bypass" while watching the pressure gauge to ensure air pressure remains unchanged.
- b) The trip solenoids are now bypassed. Check ()
- c) With the system in trip condition, temporarily place the defeat switch to OFF. Both solenoid valves should trip.

Solenoid valves tripped. Check ()
- d) Return all bypass valves to normal operating position. Check ()

Other techniques for testing solenoids but not the valve are shown in Annexes W and MM.

Another technique proposed and used by some companies involves doing a partial stroking of the final

control element valve to verify movement at least begins when called for by the SIF. This movement does not ensure that the valve will go to its full open or closed position when a real demand is placed on the system but does give some indication that the valve will at least attempt to go to its tripped position. Several examples of procedures for performing a partial stroking test of a SIF valve are shown in Annexes DD, EE, HH, and LL.

The following guidelines have been suggested for on-line testing of valves:

- SIL 1 SIF systems typically do not require any on-line testing.
- At turnaround intervals of less than 3 years and a target SIL of 2, double block valves seldom need to be partial stroke tested unless a dirty process increases the valve failure rate beyond the value normally used in PFD calculations.
- For SIL 3 applications, the testing frequency must be less than three years and on-line testing of some type (i.e., partial stroke) must be performed. Fortunately, only about 10% or less of the installations in the process industries are SIL 3. This means that for a small percentage of shutdown systems or for turnaround periods greater than 3 years, some type of on-line testing of valves is typically required.

Some cautions should be noted with regard to partial stroke testing of SIF valves. These include:

- One user noted that a failure occurred in a process valve which had been partial stroke tested to a specific mechanical stop position for years. The valve only moved 1/4 of its full stroke when actually called upon to move to its full trip position.
- If positive isolation, i.e. tight shutoff, is required, a partial stroke test does not test this capability. Since a partial stroke test cannot detect all failure modes of the valve, full credit should not be given for partial stroke testing. The following application limitations should be considered when evaluating the use of partial stroke testing:
 - 1) The service is clean. No dirt, polymerization products, deposition, crystallization, corrosive chemicals, etc.
 - 2) No documented history of a test that revealed valve failure due to process-related seat failure.
 - 3) It must not be a tight shutoff application. This specification indicates that the valve seating is extremely important, so the only valid test is a full seat test.

Partial stroke testing must consist of verification that the valve moved a set percentage of valve range. It is not considered a valid test to only confirm open or closed limit switch contacts. Percent movement of the valve should be confirmed using position indication, such as limit switches or positioners, or using visual observation. To prevent buildup of ridges on the valve stem at the percent range for the test, it is recommended that the percentage of travel periodically be changed.

Several companies now have a package, which allows assessment of the torque required to move the certain valve types during the stroke. This does not verify tight shutoff capability, but does provide some diagnostic coverage. A listing of some vendors providing these techniques is shown in Annex JJ.

7.3.7 HMI

On-line testing of the HMI is not required unless changes have been made in the information presented to the operator. Any changes that modify information to the operator about the status of the SIF should be tested when they are made and verified as being appropriate.

7.3.8 Communications

Any changes made to communications from the SIF to any other system should be tested when the changes are made. It is not recommended that changes be made while the SIF is providing protection to the process as these change activities could result in nuisance trips of the SIF or result in program errors, which could render the SIF incapable of performing its function.

7.4 Inspection (observation techniques that enhance SIF availability)

Almost as important as testing of the SIF is having a program in place that monitors the apparent condition of components of the system and their capability to provide the performance required to meet the safety requirements. An example of a condition that could limit the performance capability of a SIF component would be corrosion buildup around the stem of a sliding stem valve used to isolate a process stream when called upon by the SIF. The buildup, if not noticed and tended to, could prevent the valve from stroking all the way or even at all when called upon to take action. Inspection activities, which monitor such a condition and others, which might occur, can enhance the safety integrity of the SIF. Considerations that should be a part of these inspection programs are discussed in clauses that follow.

7.4.1 General considerations

The physical condition of the components of a SIF should receive a thorough mechanical inspection on a regular scheduled basis. This is especially true for field components exposed to environmental conditions, changes, and things like corrosion, process spills, leaks, etc. This inspection should be documented and any action that is found to be necessary initiated immediately or scheduled for the first opportunity if that is satisfactory.

7.4.2 Responsible personnel

The process unit Operations Department should be responsible for scheduling the inspections. The inspections should be scheduled to coincide with the scheduled functional test at a minimum. A schedule of once each quarter or twice a year may be appropriate for processes where conditions tend toward potential problems. In very serious environmental conditions the inspection might be necessary more frequently.

Maintenance Craftspeople should be responsible for performing and documenting inspections. Documentation records should be maintained for reference. These records may provide information relative to MTTF values for components that are used for SIF evaluation calculations and might be useful in relating process changes to problems which occur.

The maintenance and operations departments should be responsible for following up on the repair of any deficiencies discovered during the inspection to ensure repairs are completed satisfactorily.

7.4.3 Evaluation criteria

Each component of a SIF should be in good condition with no visible physical defects, which could impact the performance or reliability of the system.

The instrument craftsmen should complete a Safety Instrumented System Inspection Form during the course of the system inspection. See Annex O for an example inspection form.

Examine all parts of the SIF for damage, deterioration, missing parts, or other physical damage. The physical examination should include:

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

If a defect is found during the inspection it should be corrected as soon as possible. If the defect cannot be corrected immediately, a work order should be generated to repair the defect as soon as practical. The nature of the defect should be described on the Safety Instrumented System Inspection Form.

The inspection should include, but not be limited to the following items.

- Verify that all components of the SIF are properly tagged and labeled.
- Visually inspect devices for excessive corrosion.
- Visually inspect all components, including alarm lights, to insure proper working condition.
- Visually inspect all SIF pressure and instrument gauges to insure proper working condition.
- Visually inspect tubing, wiring connections, and wiring to insure proper working condition.
- Inspect heat tracing if appropriate to ensure proper operation.
- Verify that all instrument air supply regulators are at their proper settings, bug screens in place and not plugged, etc.
- Verify that boxes and housings have proper seals and covers and are secure.
- Verify that all conduit and conduit access plates have proper seals and are secure.
- Verify that tubing and cables are properly routed and secure.

7.4.4 Sensors

The following inspection criteria, at a minimum, apply to field sensors:

- Are instruments tagged with a special tag identifying them as part of a SIF?
- Are process connections in good condition with respect to leaks, insulation, corrosion, etc?
- Are process root valves in correct position?
- Is instrument properly supported?
- Is required heat tracing and insulation in good condition?

- Is conduit connection in good condition and covers in place?
- Are drains, seals, and covers in place, if required, and in good condition?
- Are process tubing lines properly supported?
- Is conduit properly supported?

7.4.5 Logic solvers

Logic solver cabinets should be inspected for proper ventilation or cooling, buildup of dust or other foreign material, proper closure hardware in good condition, absence of moisture, wiring and grounding connections secure, cabinet security devices in good working order, and proper operation of any lights that are meant to indicate a status condition of the logic solver itself. Some vendors of this equipment have recommended routine maintenance schedules that may offer other items that should be checked.

7.4.6 Final control elements

Control valves should be inspected for the following conditions as a minimum:

- Bug screens in place and not plugged up
- Tubing condition for air supply, connections to positioner or topworks; connections tight with no leaks
- Solenoids properly mounted with tubing and electrical connections in good condition
- Valve piping gaskets not leaking
- Valve stem not leaking
- Topworks in good condition; no cracks, leaks at gaskets, etc.
- No corrosion buildup around valve stem
- Instrument pressure gauges in good condition
- Any auxiliary equipment such as signal converters and positioners, in good condition
- Any other conditions which might hinder proper operation of the valve
- Appropriate tagging of valve is in place

7.4.7 Switches

Switches used as hardwired bypasses should be inspected for proper position, security measures in place, and wiring connections secure.

7.4.8 Wiring connections

Any critical wiring connections in junction boxes, scramble boxes, or other terminations should be checked for proper tightness, labeling and mechanical protection. The use of wire nuts for making connections in SIF is not recommended. Seals where required should be checked. Conduit covers should be in place. Conduit drains should be in place and working properly. Cabinet doors should be closed, water tight, and properly labeled.

7.5 Testing documentation

7.5.1 SIF test procedures

A specific written test procedure should be available for each SIF included in the SIS. 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:

- List of safety function(s) included in the SIF
- Equipment description and location for each safety function
- Functional logic for each safety function
- Inspection procedures to be followed
- Calibration and testing methods to be followed
- Frequency of calibration, testing, inspections, and maintenance activities
- Specify acceptable performance limits ($\pm 2\%$ of full range if no limits specified)
- Specify sequence of testing if required
- Specify who should perform test
- Specify state of process when test is performed
- If SIF logic is mirrored in the BPCS, test should show that SIF actuated final control device.
- Verification of operational state of SIF after test complete
- Test of internal and external diagnostics (WDT, etc.)
- Verify auxiliary service components are operational (fans, filters, batteries, UPS, etc.).
- Define a means of ensuring testing is performed and documented.

All test procedures should have system being tested, page numbers, and revision date on each page of procedure. The responsible person for maintaining each procedure should be identified in the procedure.

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

7.5.2 Documentation of functional testing of SIF

Document the results of functional tests for all SIF components and systems.

Test documentation should include but not be limited to the following data:

- Date of inspection and testing
- Name (signature) of the person(s) performing the work
- Tested equipment serial number or other unique identifier, such as loop number, tag number, or, equipment number

- Results of the inspection and test (as found and as left conditions)

Important: Confirm and document that alarm and/or shutdown trip devices and process actuators operate within specified tolerances. This can be accomplished individually as a component test or as part of the loop or system test.

Retain records of these functional tests and inspections in accordance with plant policy. It is recommended that at least the two most frequent records of functional testing of the SIF be kept at the plant site. If a regulating body such as OSHA requires records retention, the retention period in that regulation should be followed.

7.5.3 Documentation of SIF component calibration

Document each calibration of a SIF component. Calibration documentation should include the following data:

- Date of inspection and calibration
- Name of the person performing calibration
- Calibrated equipment serial number or other unique identifier, such as loop number, tag number, or equipment number
- Before and after results of the calibration; i.e., “As Found” and “As Left” condition
- Test equipment (by manufacturer and model/serial number) used for the calibration

Calibration records should be maintained to confirm that this work was completed and to build a historical database of SIF component performance.

NOTE These records become the basis for adjustment to the calibration interval specified for each safety system component. The frequency(s) of testing and calibration of the SIF or portions of the SIF is re-evaluated at a periodic interval set by the site. The re-evaluation frequency is based on historical data, plant experience, hardware degradation, software reliability, etc.

7.5.4 Off-line tests

A good example of a test documentation form for off-line testing documentation is shown in Annex AA.

7.5.5 On-line tests

The same forms used to document off-line testing can be used to document on-line testing with the proper notations provided. Special forms may be developed if the user desires.

7.5.6 How test results are analysed

The results of the calibration and testing should be reported to the site engineer responsible for the SIF for review and approval. If necessary, the site engineer will consult with the site safety and environmental personnel for his/her review and recommendation with regard to the impact on the safety and/or environmental issue(s).

8 Inspections

An example of a form for documenting results of an inspection program is shown in Annex O.

9 Auditing

Audits should be performed to verify that the procedures related to SIF and, in particular, those outlined in the SIF testing document remain in force throughout the life of the SIF. Records of audits and their results should be documented and maintained in plant records. Two types of documents that might accomplish this audit may be found in Annex FF and GG.

10 References

This document was compiled from input provided by operating companies, manufacturing companies, consultants, and individual engineers who have experience in the application, design, installation, operation, and maintenance of SIF. The best practices and procedures of these companies and individuals were combined and edited to allow use without disclosing any proprietary information from any one company or individual.



This page intentionally left blank.

NOTE This procedure was developed by an operating company for a specific application. It has been modified to remove any reference that might tie it to a specific company. This procedure should only be used as an example of how a user might develop a procedure specific to their SIS application. Any references to specific brands of instrumentation in the procedure are to clarify the intent of the procedure only and are in no respect meant to suggest these brands are acceptable or preferred for the user's specific application. The instrument identification numbers used in the procedures are for clarification purposes only and should in no way be taken as indicative of a particular company's instruments on a particular process.

CAUTION — PRIOR TO APPLYING THE INFORMATION IN THIS ANNEX TO DEVELOP A PROCESS SPECIFIC PROCEDURE, THE USER SHOULD REVIEW AND UNDERSTAND THE GUIDANCE IN THE BODY OF ISA-TR84.00.03-2002.

Annex A — Model procedure for approval required for replacing individual components in SIF

Scenario: A SIF instrument or valve needs to be replaced.

The following guidance should be followed in replacing the SIS component:

1. An instrument or valve with the exact model number of the failed SIF component is available from plant stores or a commercial supplier.

Instrument Craft Person can make this decision.

2. An instrument or valve with the exact model number of the failed SIF component is not available from stores or commercial supplier.

CASE 1:

A list of equivalent instruments or valves has been prepared and approved for look-up use at plant site.

Instrument Craft Person selects component from the list.

CASE 2:

1. Functional and physical specifications for the SIF component to be replaced are available in the SIF documentation.
2. A substitute component with specifications that are equal to or exceed those of the failed component is identified. Equivalent functional performance of the available substitute instrument or valve is certain.

Maintenance Technical Staff approves substitute.

CASE 3:

1. Functional and/or physical specifications for the SIF component to be replaced are INCOMPLETE in the SIF documentation, or
2. The substitute instrument or valve available requires a change of
 - piping or process equipment;
 - measurement technology; and/or

Procedure No.
Revision Date
Page _ of _

- functional performance of the SIF.

Engineering personnel with responsibility for SIF integrity of this process approves substitute.

NOTE This procedure was developed by an operating company for a specific application. It has been modified to remove any reference that might tie it to a specific company. This procedure should only be used as an example of how a user might develop a procedure specific to their SIS application. Any references to specific brands of instrumentation in the procedure are to clarify the intent of the procedure only and are in no respect meant to suggest these brands are acceptable or preferred for the user's specific application. The instrument identification numbers used in the procedures are for clarification purposes only and should in no way be taken as indicative of a particular company's instruments on a particular process.

CAUTION — PRIOR TO APPLYING THE INFORMATION IN THIS ANNEX TO DEVELOP A PROCESS SPECIFIC PROCEDURE, THE USER SHOULD REVIEW AND UNDERSTAND THE GUIDANCE IN THE BODY OF ISA-TR84.00.03-2002.

Annex B — Model procedure for deferring scheduled testing of SIF

Decision to defer

The scheduled test of a SIF may be deferred provided certain guidelines are followed. The following guideline will insure all proposed deferrals are properly reviewed and approved prior to granting a deferral. Note that the personnel titles used may be different from location to location. The intent is to reflect approval positions and not exact titles.

Deferral request

Deferral request shall be transmitted from Operations to the Instrument Specialist prior to the scheduled time to test a SIF. The timing shall allow ample time for the Instrument Specialist to conduct a fact based deferral analysis.

Reason for the request

There are several potential reasons for deferring the test of a SIF.

A turnaround is scheduled shortly after the scheduled test and the risk of off-line testing is lower than on-line testing. Also, the off-line test may enable the final control element to be tested whereas an on-line test may not allow the final control element to be tested.

1. The process equipment that the system is safeguarding is out of service. The agreement in this case is that the SIF will be tested prior to the process equipment being activated.

Deferral length

Suggested maximum length of time for a deferral should not exceed one quarter. If additional time is needed for a deferral after one quarter, it is suggested the deferral analysis be revisited along with approvals.

Deferral analysis

A deferral analysis should be conducted prior to granting a deferral. This analysis should include prior test results. A record of successful tests of the SIF should be the minimum acceptable criteria for deferring a test. The Instrument Specialist should participate in this deferral analysis and his/her concurrence should be required prior to forwarding to the approving authorities noted below.

Approvals required for a deferral

SIL I and SIL II systems: Operating and Technical Area Superintendent.

Procedure No.
Revision Date
Page _ of _

SIL III systems: Site Operations Manager and Control Systems Manager

Communication of deferral

The following should be made aware of any approved deferrals.

- Site Operations Manager
- Operating Area Superintendent
- Technical Manager Control Systems
- Technical Superintendent
- Engineering/Maintenance Manager
- Instrument Specialist
- Control Systems Engineer

Documentation of deferral

All deferrals should be documented with each of the items above captured.

NOTE This procedure was developed by an operating company for a specific application. It has been modified to remove any reference that might tie it to a specific company. This procedure should only be used as an example of how a user might develop a procedure specific to their SIS application. Any references to specific brands of instrumentation in the procedure are to clarify the intent of the procedure only and are in no respect meant to suggest these brands are acceptable or preferred for the user's specific application. The instrument identification numbers used in the procedures are for clarification purposes only and should in no way be taken as indicative of a particular company's instruments on a particular process.

CAUTION — PRIOR TO APPLYING THE INFORMATION IN THIS ANNEX TO DEVELOP A PROCESS SPECIFIC PROCEDURE, THE USER SHOULD REVIEW AND UNDERSTAND THE GUIDANCE IN THE BODY OF ISA-TR84.00.03-2002.

Annex C — Model procedure for testing turbine thrust position monitors

PROBE V-1234

1. Put **VT-1234** in the defeat position.

Red defeat light on the face of **VT-1234A** should be on - verify.

2. Check calibration of **VT-1234**. Record findings below, make no adjustments until initial checks are made.

.....

Table C.1 — Turbine thrust position**Calibrate 0 – 30 mils. Active.**

ANY FAILURES? _____

VT-1234	ORIGINAL CALIBRATION					FINAL CALIBRATION		
	GAP VOLTS	TEST PT VOLTS	FAILURE LIMITS TEST PT.	MONITOR INDICATION	SWITCH SETTING	TEST PT VOLTS	MONITOR INDICATOR	SWITCH SETTING
ACTIVE +40 MIL.								
ACTIVE +30 MIL.			8.4 TO 9.1 V					
DANGER VSHH-1234 ACTIVE +30			27 to 33 mils					
ALERT VSH-1234 ACTIVE +20								
0 MIL.			4.6 to 5.4 V					
ALERT VSH-1234 INACTIVE - 25								
DANGER VSHH-1234 INACTIVE - 30			-27to -33mils					
INACTIVE -30 MIL.			0.9 to 1.6 V					
INACTIVE -40 MIL.								

3. Using wobulator pass **VT-1234** through its alarm point in the **active** direction. Do not pass VT-1234 through its trip point at this time.

- a. Red danger light on **VT-1234A** should be off - verify.

Procedure No.
Revision Date
Page _ of _
