

Supplementary Specification to IEC61511 - Safety instrumented systems for the process industry sector



Acknowledgements

This IOGP supplementary specification was prepared by the Instrumentation and Automation Standards Subcommittee of IOGP's Standards Committee.

Front cover photography used with permission courtesy of
© Mr.PK/Shutterstock

About

This supplement has been developed to support owner/operating company standards harmonization for safety instrumented systems. This document acts as a supplement to the established industry standard IEC61511.

Feedback

IOGP welcomes feedback on our reports: publications@iogp.org

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither IOGP nor any of its Members past present or future warrants its accuracy or will, regardless of its or their negligence, assume liability for any foreseeable or unforeseeable use made thereof, which liability is hereby excluded. Consequently, such use is at the recipient's own risk on the basis that any use by the recipient constitutes agreement to the terms of this disclaimer. The recipient is obliged to inform any subsequent recipient of such terms.

Please note that this publication is provided for informational purposes and adoption of any of its recommendations is at the discretion of the user. Except as explicitly stated otherwise, this publication must not be considered as a substitute for government policies or decisions or reference to the relevant legislation relating to information contained in it.

Where the publication contains a statement that it is to be used as an industry standard, IOGP and its Members past, present, and future expressly disclaim all liability in respect of all claims, losses or damages arising from the use or application of the information contained in this publication in any industrial application.

Any reference to third party names is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement.

Copyright notice

The contents of these pages are © International Association of Oil & Gas Producers. Permission is given to reproduce this report in whole or in part provided (i) that the copyright of IOGP and (ii) the sources are acknowledged. All other rights are reserved. Any other use requires the prior written permission of IOGP.

These Terms and Conditions shall be governed by and construed in accordance with the laws of England and Wales. Disputes arising here from shall be exclusively subject to the jurisdiction of the courts of England and Wales.

Supplementary Specification to IEC61511 - Safety instrumented systems for the process industry sector

Revision history

VERSION	DATE	AMENDMENTS
1.0	March 2022	First release

Contents

Introduction	6
Part 1: Supplementary Specification to IEC 61511-1	7
1. Scope	7
2. Normative references	7
3. Terms, definitions, and abbreviations	7
4. Conformance to the IEC 61511-1:2016	8
5. Management of functional safety	8
5.2.2 Organization and Resources	8
5.2.4 Safety Planning	8
5.2.6 Assessment, auditing and revisions	9
5.2.7 SIS configuration management	10
6. Safety life-cycle requirements	10
7. Verification	10
8. Process H&RA	11
9. Allocation of safety functions to protection layers	11
10. SIS safety requirements specification (SRS)	12
11. SIS design and engineering	14
12. SIS application program development	17
13. Factory acceptance test (FAT)	17
14. SIS installation and commissioning	18
15. SIS safety validation	18
16. SIS operation and maintenance	19
17. SIS modification	19
18. SIS decommissioning	19
19. Information and documentation requirements	19

PART 2: Supplementary Guidance to IEC 61511-2	20
A.1. Scope	20
A.2. Normative references	20
A.3. Terms Definitions and Abbreviations	20
A.4. Conformance to the IEC 61511-1	20
A.5. Management of Functional Safety	20
A.6. Safety life-cycle requirements	21
A.7. Verification	21
A.8. Process hazard and risk assessment	21
A.9. Allocation of safety functions to protection layers	21
A.10. SIS safety requirements specification	21
A.11. SIS Design and Engineering	22
A.12. SIS application program development	25
A.13. Factory acceptance testing	25
A.14. SIS installation and commissioning	25
A.15. SIS safety validation	25
A.16. SIS operation and maintenance	26
A.17. SIS Modification	26
A.18. SIS decommissioning	26
A.19. Information and documentation requirements	26

Introduction

The purpose of this supplementary specification is to define a common implementation of IEC61511-1 and support adoption of aligned additional requirements for the engineering and lifecycle management of safety instrumented systems in accordance with IEC61511-1, Edition 2.1, 2017.

This specification is to be applied as follows.

IOP S-636: Supplementary Specification to IEC 61511-1 Safety Instrumented Systems

Part 1 of this specification defines the technical requirements and is written as an overlay to IEC61511-1, following the IEC 61511-1 clause structure.

Part 2 of this specification provides additional guidance in the implementation of IEC 61511-1 and is written as an overlay to IEC61511-2, following the IEC 61511-2 clause structure.

Clauses from IEC61511-1 and 2 not amended by this specification apply as written.

Modifications to IEC61511-1 and 2 defined in this specification are identified as Add (add to clause or add new clause), Modify (part of or entire clause) or Delete.

The terminology used within this specification follows that of IEC61511 and is in accordance with ISO/IEC Directives, Part 2, as appropriate.

Part 1: Supplementary Specification to IEC 61511-1

1. Scope

No changes

2. Normative references

No changes

3. Terms, definitions, and abbreviations

Add to clause

Functional Safety Lead (FS-Lead)

Person(s) responsible for managing the relevant phases of the safety lifecycle.

Interlock

A feature that makes the state of two or more mechanisms or functions mutually dependent; e.g., permissive preventing one element from changing state, or enabling it to change state, due to the state of another element.

SIF Response Time

Time taken for SIF detection (including filters and process connection lag), SIF logic processing (including processing and time delays) and SIF action completion.

3.2.31 Independent organization

Add to subclause

Note 1 to entry: Depending upon the owner/operating company organization and expertise within the owner/operating company, the requirement for an independent assessor may have to be met by using an external organization. Conversely, companies that have internal organizations skilled in risk assessment and the application of SISs, which are independent to and separate (by ways of management and other resources) from those responsible for the project, may be able to use their own resources to meet the requirements for an independent organization.

3.2.67 Safety Instrumented System

Add to subclause

Note 4 to entry: A SIS may include unit control panel (UCP) system(s) handling safety instrumented function(s) (e.g., within the package equipment).

3.2.86 Validation

Modify subclause

A demonstration that the SIF(s) and SIS after installation meet the SRS in all respects.

4. Conformance to the IEC 61511-1:2016

No changes.

5. Management of functional safety

5.2.2 Organization and Resources

5.2.2.1

Add to subclause

- i) Each project or entity/asset with SIFs shall designate a person or persons [referred to in this document as Functional Safety Lead (FS-Lead)], who will be responsible for managing the relevant phases of the safety lifecycle.

5.2.2.2

Add to subclause

- j) knowledge of relevant Owner/operating company practices and procedures;
- k) understanding of the impact of activities they are accountable for on other phases of the safety lifecycle.

5.2.2.3

Add to subclause

- i) The FS-Lead shall verify the competence of those performing functional safety activities, or verify procedures that assure such competence are being followed.

5.2.4 Safety Planning

Add to subclause

- i) A SIS safety lifecycle plan shall be defined in projects during early engineering phase, e.g., FEED.
- ii) A SIS safety lifecycle plan shall be defined for operational facilities.
- iii) A SIS safety lifecycle plan shall be developed per 5.2.1 that includes the following minimum requirements:

- 1) Accountabilities, responsibilities, and resources per 5.2.2.1
 - 2) Competence of organizations and individuals per 5.2.2.2 and 5.2.2.3
 - 3) Risk evaluation and risk management per 5.2.3
 - 4) Planning and interface management including integration of SIS activity planning into project planning per the project stages (e.g., FEL, design, execution) per 5.2.4 and 5.2.6
 - 5) Tracking and resolution of recommendations per 5.2.5.1
 - 6) Quality and safety management systems of SIS suppliers per 5.2.5.2
 - 7) Procedures to evaluate the performance of the SIS per 5.2.5.3
 - 8) Functional safety assessment per 5.2.6.1
 - 9) Functional safety audit and revision per 5.2.6.2
 - 10) SIS configuration management per 5.2.7
 - 11) Verification requirements per 7.2
 - 12) Documentation requirements per 19.2
 - 13) Method(s) of tracking functional safety related actions such as those resulting from FSAs
- iv) Functional safety planning shall include Unit control panel system(s) handling safety instrumented function(s) (e.g., within the package equipment).

5.2.5.4 Safety Planning

Modify subclause

For existing SIS designed and constructed in accordance with code, standards, or practices prior to the issue of the first version of this standard the user shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner. Such SIS shall meet all lifecycle management requirements in this document applicable to existing SIS (i.e. sections 5, 6, 7, 16, 17, 18 and 19).

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional Safety Assessment (FSA)

Add to subclause

- i) All $\geq$ SIL 3 SIFs shall be individually reviewed in detail as part of FSA.
- ii) The FSA scope shall additionally include sufficient SIL1&2 SIFs to satisfy clause 5.2.6.1.1.
- iii) An FSA shall be conducted at regular intervals (at least every 5 years) during operations (FSA stage 4).
- iv) Greenfield projects shall undertake functional safety assessment stages 1 to 3.
- v) Tools previously approved by Owner/operating company do not require assessment.

5.2.7 SIS configuration management

Add to subclause

- i) Revision control for logic solver application programs and system software shall be either:
 - a) implemented on completion of the FAT, where a FAT is required per 13.2.1; or
 - b) implemented on completion of the SAT, if a FAT is not required.
- ii) Revision control for configuration of field programmable devices shall be implemented after SAT.

5.2.7.1

Add to subclause

The firmware and application program versions of each SIS shall be documented.

6. Safety life-cycle requirements

No changes.

7. Verification

7.2.4

Add to subclause

- i) For $\geq$ SIL 3 SIFs, verification shall be carried out by a peer not involved in the design, implementation, operation, maintenance, or modification of the SIF or SIS.

NOTE: This would normally include verification of:

- a) the results of the allocation process per 9.2.9
- b) the safety requirements specification per 10.3.2
- c) the calculated failure measure per 11.9
- d) the FAT per 13.2.4
- e) installation and commissioning per 14.2.3
- f) validation per 15.2.7
- g) operations and maintenance per 16.2.2
- h) proof tests per 16.3.1
- i) modifications per 17.2.3

8. Process H&RA

8.2.1

Add to subclause

- The hazard and risk assessment (H&RA) safety integrity (SIL) review shall ensure packaged equipment SIFs are either adequate or supplemented by alternative protection layers not forming part of the equipment package.

Add to subclause

- i) A review team used to determine SIL levels and associated integrity targets shall:
 - a) Include representatives from process engineering, process or technical safety, operations, instrumentation and control and other disciplines when the SIFs of a particular engineering speciality are classified (e.g., rotating equipment or subsea)
 - b) Include at least one senior competent, independent person not involved in the project design team (the facilitator may serve in this role)
 - c) Be led by a facilitator demonstrably competent in the use of the methodology being applied.

8.2.4

Add to subclause

The security risk assessment which is completed for each SIS shall consider the overall facility (multi-system) network topology, including connections to other SIS, BPCS and equipment packages.

9. Allocation of safety functions to protection layers

9.3.2

Add to subclause

Instrumented protection layers that have been allocated a risk reduction of ≤ 10 and are not intended to conform to the IEC 61511 series shall be treated as a BPCS protection layer.

9.3.4

Add to subclause

- i) BPCS protection layers may take the form of Interlocks, Alarms or control loops.

9.3.5

Delete from subclause

NOTE 2.

9.4

Add to subclause

9.4.1

- i) Where there are multiple SIFs on a single threat to consequence line, the demonstration of adequate risk reduction shall include a consideration of the potential for CCF between the SIFs.

- 9.4.3 Where the control (BPCS) and safety system (SIS) vendor is the same, a justification should be provided to demonstrate there is sufficient independence between the control and safety parts of the system, and that any common cyber threat to both parts has been adequately addressed, to satisfy the SIL claim per 9.4.1 and 9.4.2. This should include assuring the independence of the application code programming.

Commentary: It is likely that integrated control and safety systems (i.e., from a single vendor) will utilize common processors, power supplies, and even I/O cards. Although the safety system part will be subject to more rigorous design and higher levels of redundancy, the potential for CCF is nonetheless greater than it would be for diverse (i.e., supplied by different vendors) control and safety systems.

10. SIS safety requirements specification (SRS)

10.1

Add to subclause

- i) The SRS may be supplemented with reference to other documents, such as equipment safety manuals and SIS logic diagrams.

10.2

Add to subclause

- traceable to a specific revision of the H&RA with a unique name/ID for each SIF

10.3.2

Add to subclause

- i) For each SIS the applicable requirements listed in IEC 61511-1 clause 10.3.2 shall be determined. The default is that all apply.
- ii) The SRS shall be presented in such a way and contain the necessary information as to satisfy clause 9.2.9.

- iii) The SRS shall include the targets for the following:
 - 1) SIL
 - 2) PFD or PFH
 - 3) SIF response time
- iv) Maximum allowable leakage rate that enables SIF action to be successful to prevent the hazardous scenario shall be specified for valves.
- v) Maximum allowable leakage rate may take account of ability of downstream equipment to relieve small leakage or procedures to manage leakage within a given time.
- vi) When a SIF activation causes process conditions that will activate another SIF (i.e., a cascade trip) and there is insufficient time for credible operator or control system response to avoid the cascade trip, the first SIF to activate shall include actions of the second SIF as non-critical actions that are not included in the SIL reliability calculations of the first SIF.
- vii) The sensor and final element diagnostic (where applicable) fault failure mode (e.g., fail low or high) shall be specified in the SRS.
- viii) The SIF response time and SIF activation point (trip setting) shall be such that the design limit will not be exceeded (including any process dynamic lags) if the SIF activates at the required setpoint.

Commentary: Design limit will be defined by company, some examples might be; the maximum allowable working pressure (MAWP), vessel stated design temperature (maximum or minimum). Note that it is preferable, though not always possible, to have discrimination between protection layers, e.g. a SIF will normally be designed to operate in sufficient time that the next protection layer will not activate. Refer ISA TR84.00.04 Annex Q.

- ix) In determining SIF response time, a minimum 10% margin shall be incorporated.

Commentary: Note this is a minimum. For SIFs for which the response time is close to the process safety time, e.g. fast-acting SIFs such as HIPPS, a much larger margin may be required to account for uncertainty in the process model.

10.3.5

Add to subclause

- i) [Bullet 6] SIS logic solver fault detection shall match the sensor fault values and be distinct from sensor saturation values.
- ii) [Bullet 6] For inputs with diagnostic fault detection, the application program shall include a sufficient time delay to allow diagnostic faults to be differentiated from healthy sensor values and take appropriate action per 11.3.1.

11. SIS design and engineering

11.2.7

Add to subclause

- i) Resets for SIFs shall:
 - be permitted only after the process has returned to a safe state
 - require a reset from the HMI
 - be momentary
- ii) Resets for SIFs shall not override the safety signal

NOTE: For example, a field reset cannot be used to manually operate (e.g., open/close) a SIS valve that is in the tripped state.

11.2.9

Add to subclause

- i) With the exception of ii, SIS sensors shall not share common process connections with another sensor.
- ii) Primary flow elements (e.g., orifice plate, venturi, bluff bodies) may be shared by SIF and monitoring or control functions, but the SIF and monitoring or control functions shall have separate process connections

11.2.11

Modify subclause

For any SIS device that on loss of utility (e.g., electrical power, air, hydraulics or pneumatic supply) or critical support system (e.g., heat tracing, purge) does not fail to the safe state, loss of utility, critical support system, and SIS circuit integrity shall be detected and alarmed (e.g., end-of-line monitoring, supply pressure measurement, hydraulic or pneumatic pressure monitoring, heat trace temperature monitoring, purge flow/pressure monitoring) and action taken according to 11.3.

11.3.1

Modify subclause

When a dangerous fault in a SIS has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures shall be taken to maintain safe operation. If safe operation cannot be maintained, a specified action to achieve or maintain a safe state of the process shall be taken. Where the compensating measures depend on an operator taking specific action in response to an alarm (e.g., opening or closing a valve) then the alarm shall be subject to management of change and proof testing similar to that applicable to a SIF.

Add to clause

11.3.3 When a dangerous fault in a SIS has been detected per 11.3.1 or when a bypass is applied per 11.8.5 the actions specified in table 5.5 shall be taken, unless clause 11.3.3 applies.

Commentary: Refer 11.3.2 and 11.8.3 for dangerous fault alarm and bypass requirements.

- a) Faults detected by a deviation between measurements need not apply table 5.5. If table 5.5 is not applied the deviation fault shall activate an alarm subject to the requirements of 11.3.2.
- b) When a dangerous fault is detected in a in non-redundant SIF and the action is not to trip (table 5.5, note 2), the delay timer shall be restricted to the minimum necessary.

Commentary: For some processes, tripping automatically upon detection of a fault can lead to undesirable consequences. As such, it is sometimes acceptable to delay tripping to enable application of compensating measures (refer 11.3.1). The maximum time will be defined by the Company.

- d) Where a dangerous fault is detected in a SIF (see Table 5.5, notes 1&3), the delay timer shall be restricted to no more than the SIF MTTR.

Commentary: The MTTR is used as part of the SIF PFD calculation.

Table 5.5: SIF voting system behaviour on detection of a fault

Initial voting	Action on fault		
	1 Fault	2 Faults	3 Faults
1oo1	1oo1 ^[1,4]	NA	NA
1oo1 (No delay)	TRIP ^[5]	NA	NA
2oo2	1oo1	TRIP ^[1,4,5]	NA
1oo2	1oo1 ^[2,4]	TRIP	NA
2oo3	1oo2	1oo1 ^[2,4]	TRIP ^[5]

[1] Start delay timer and activate SIF function when the timer expires.

[2] Degrade the voting logic, start delay timer and activate SIF function when the SIF MTTR is exceeded.

[3] Timer which started upon degradation to 1oo2 continues to run.

[4] Upon manual activation of a bypass it is expected that appropriate risk assessment will have taken place, compensating measures will be applied, thus the timer can be stopped.

[5] No trip in response to bypass, trip in response to fault only

11.4.5

Add to subclause

- i) If the HFT of the SIS is in accordance with 11.4.5 to 11.4.9, then the prior use clauses (11.5.3 to 11.5.6) shall apply.

11.5.3.1

Add to subclause

- i) The prior use evaluation process shall be approved by Owner/operating company.

11.5.3.3

Modify subclause

All devices selected on the basis of prior use shall be identified by a specified model number or series number and shall be under the control of a management of change procedure. In the case of a change being made to the functional design of the device, the continued validity of the evidence of prior use shall be justified by evaluating the significance of the change made.

11.6.1

Add to subclause

- i) Mechanically adjustable settings for SIF components shall be protected against inadvertent adjustment (e.g. through means of a secondary locking device or restricted access).
- ii) Devices used for SIS process measurements shall have diagnostics enabling signal loss and sensor failure detection.

11.7.2.2

Add to subclause

- i) If an automatic start-up bypass is necessary (e.g., for a low level or low pressure trip), the bypass shall be automatically removed based on a defined process condition (e.g., setpoint +/- deadband) and/or a time delay.

11.8.1

Add to subclause

- i) Where valve proof testing requires in-situ verification of leak tightness, the design shall include facilities to enable such testing.

11.8.3

Add to subclause

- i) All bypass related events such as bypass enable, bypass active and bypass removal shall be logged (journaled) with date and time stamp.

11.9.1

Add to subclause

- i) The calculation tool to determine failure measure of each SIF shall be approved by owner/operating company.

11.9.2 a)

Modify subclause

- a) the architecture of the SIS and of its SIS subsystems, including process connections, as they relate to each SIF under consideration;

Commentary: Adding the random failure rate of the process connection to the sensor failure rate accurately accounts for the increased failure rate contribution of the process connection based on the operating environment.

11.9.3

Add to subclause

- i) The reliability data (e.g., failure rates) used when quantifying the effects of random failures shall be approved by owner/operating company.

11.9.5

Add to subclause

- e) Review H&RA and allocation of protection layers (e.g., HAZOP, LOPA) to confirm the integrity (SIL) target.

Commentary: For SIL 2 or higher SIFs, it is a good practice to review the H&RA and the allocation to protection layers to reduce the target failure measure before attempting to add additional hardware or accept short test intervals. Some items for review are use of appropriate protection layers and modifiers.

12. SIS application program development

No changes.

13. Factory acceptance test (FAT)

13.2.1

Add to subclause

- i) For new SIS, a FAT shall be conducted to test the SIS hardware and application program and associated infrastructure components. The SIS FAT may be split to test the hardware and application program separately.

13.2.2

Add to subclause

- i) The FAT shall verify that:
 - a) non-safety functions implemented in the SIS logic solver do not interfere with the safety functions.
 - b) the logic solver processor loadings are within expected levels including allowance for future expansion where applicable.
- ii) The FAT scope shall include both positive (verification of intended function) and negative (performs as expected under fault conditions) testing.
- iii) FAT shall be witnessed and accepted by person(s) appointed by owner/operating company.

13.2.7

Add to subclause

- i) Post FAT, all changes to the SIS shall be subject to a management of change (MoC) process.

14. SIS installation and commissioning

14.2.5

Add to subclause

- i) A competent designated person shall approve all modifications during installation and commissioning based on safety impact analysis.

15. SIS safety validation

15.2.1

Add to subclause

- i) Validation procedure(s) shall be approved by the relevant FS-Lead. For SIL 3 SIFs, validation procedures shall be verified by a person independent of the design of the SIS (can be within organization).

15.2.3

Modify subclause

Where measurement accuracy is required as part of the validation then instruments used for this function shall be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

16. SIS operation and maintenance

16.2.9

Add to subclause

- i) Failures of equipment forming part of a SIF which is the final protection layer shall be investigated to identify the root failure cause and any systematic causes contributing to the failure.

16.3.1.2

Modify subclause

The entire SIS shall be tested including the process connection(s), sensor(s), logic solver and the final element(s) (e.g., shutdown valves and motors).

The SIS behaviour on detection of a fault (per 11.3) shall be tested as determined by company..

When testing in segments, sufficient overlap shall be provided between segments to ensure that all components of the SIF are tested.

16.3.1.6

Modify subclause

Any change to the SIS application program shall require a full validation and a proof test of any SIF impacted by the change. Exceptions shall require appropriate review and partial testing of changes carried out to ensure the changes were designed per the updated safety requirements and correctly implemented.

17. SIS modification

No changes.

18. SIS decommissioning

No changes.

19. Information and documentation requirements

No changes.

PART 2: Supplementary Guidance to IEC 61511-2

A.1. Scope

No changes.

A.2. Normative references

No changes.

A.3. Terms Definitions and Abbreviations

Add subclause

A.3.2.71

When a collection of documents is used for the safety manual, there should be an umbrella document making the links between all those documents and the safety manual section, pointing to the relevant sections. All referenced documents should be made available and auditable.

A.4. Conformance to the IEC 61511-1

No changes.

A.5. Management of Functional Safety

A.5.2.6.1.1

Add to subclause

It is not practical to review the integrity of every SIF. The purpose of the FSA is to enable a judgement to be made as to the FS achieved by each SIF within the SIS. A judgement can be made without reviewing every SIF. As such the reviewer needs to exercise their judgement as to the extent of individual SIFs that need to be included within the review scope.

A.5.2.6.1.4

Modify subclause

A FSA should be performed at Stage 1 and 2 for major projects (e.g. those installing whole SIS). The relevant FS-Lead should decide when a FSA is required at Stage 1 and 2 for all other projects or modifications.

A.5.2.6.2

Add to subclause

A functional safety audit, per IEC 61511-1 clause 5.2.6.2, should be conducted:

- during project FEED and Execution to ensure all the systems and procedures required to deliver functional safety through to project commissioning and handover are in place, and to confirm the adequacy of the FSP.
- annually during the operations phase

A.6. Safety life-cycle requirements

No changes.

A.7. Verification

No changes.

A.8. Process hazard and risk assessment

No changes.

A.9. Allocation of safety functions to protection layers

A.9.4.2

Add to subclause

Functionally, emergency or process shutdown (ESD/PSD) and fire and gas (F&G) parts of SIS should be implemented in separate nodes of the SIS. Where the plant size and complexity is sufficiently small/simple, the Logic Solver of the ESD and F&G parts of SIS may be integrated within the same node(s). In this case input/output (I/O) cards should be separate for ESD and F&G systems.

A.10. SIS safety requirements specification

A10.1

Add to subclause

SRS should be developed from early project stage, as a key document to support proper SIS design in accordance with safety requirements.

A.10.3.2

Modify subclause

SIS sensor measurement range, accuracy and trip points should be determined based on the maximum variation of the process conditions (e.g., density, temperature, dielectric constant).

A.10.3.5

Add to subclause

A deviation fault alarm for a sensor (e.g., input) group between the highest and lowest sensor should be configured:

- for voted sensor groups in the SIS (e.g. 1oo2, 2oo3);
- for a sensor group including a 1oo1 sensor in the SIS and a BPCS sensor measuring the same process variable, where available (e.g., existing control or alarm sensor).

A.11. SIS Design and Engineering

A.11.2.6

Modify subclause

Graphics should be built in a consistent, repeatable and unambiguous fashion, with the same conventions and behaviours reflected throughout.

A.11.2.7

Add to subclause

Resets for SIFs should be performed via the HMI.

Commentary: An overview of the process state should be seen by the individual pressing the reset, hence the HMI requirement.

A.11.2.9

Add to subclause

SIS should not share cables, junction boxes, conduit, or marshalling with non-SIS equipment.

For existing installations, packaged equipment, or small facilities where it is not technically feasible to provide full separation between SIS and non-SIS wiring, separation using separate terminal strips, barriers, and labelling are methods to identify SIS from non-SIS wiring.

A.11.2.10

Add to subclause

Inputs shared between the SIS and BPCS should be hardwired to the SIS and repeated to the BPCS:

- using hardwired signals with an isolator such that a failure of any portion of the BPCS input will not result in a failure of the SIS input. The power for the field device and isolator should be provided by the SIS with an isolator used to repeat the signal to the BPCS input.
- using a redundant communications network such that a failure of the BPCS or communication network will not result in a failure of the SIS. The communications network should have diagnostics and alarms to reveal any failures that may impact availability of the network.

A BPCS final control element shared with SIS as a SIF final control element should meet the following:

- the final control element is not part of the initiating cause or another IPL associated with that SIF;
- the final control element is failsafe on loss of power (e.g., pneumatic, electrical)
- an output device (e.g., solenoid) independent of the BPCS and controlled by the SIS is provided to take the final element to the failsafe state
- the SIF contains at least one other final control element that will take the SIF to the safe state independent of the BPCS final element
- the BPCS final control element is inspected, tested, and maintained as a SIF component

A.11.2.11

Add to subclause

Critical SIS support systems (e.g., power supplies, instrument air, network switches, cabinet temperature) health and SIS system faults should be monitored and associated alarms classified as critical fault alarms.

A.11.6

Add to subclause

- i) SIS Sensors and SIS final elements should be connected to independent SIS inputs or outputs.

Commentary: Use of bus communications for sensors and final elements introduces potential for systematic failures. Use of multi-drop (e.g. parallel) wiring and a common output for multiple final elements reduces the ability to perform diagnostics and online testing of individual final elements.

- ii) Each SIS sensor (including multiple sensors) should have its own process connection(s) and impulse line(s).
- iii) SIS transmitters should communicate with the SIS in 4-20 mA signal mode. This signal should comply with NAMUR NE 43 enabling signal loss and sensor failure detection.
- iv) Analogue sensor signals should be connected directly to input cards integral to the SIS. Separate trip amplifiers should be avoided.

- v) The SIS sensor dead band should be set wide enough to accommodate the process noise level.
- vi) Level sensors should have either:
 - separate connections to the vessel for SIS sensors and control sensors, or;
 - control and SIS sensors connected to a level bridle (no separate connections to the main vessel/column are required) provided that the connections of the bridle to the main vessel are not smaller than DN50 (2 inch) and their block valves are locked using auditable controls such as trapped key or car seal systems.
- vii) A SIS temperature sensor should not share the thermowell with control sensors.
- viii) Manual emergency trip switches should be:
 - hardwired directly to the SIS (not “daisy-chained”)
 - normally closed during normal operation (de-energise to trip)
 - physically protected to prevent inadvertent activation
 - have an input time delay sufficient to avoid spurious activation
 - have a diagnostic fault alarm for circuit integrity monitoring
 - not shutdown for a diagnostic fault unless otherwise specified in the SRS
- ix) Position feedback for valves and other final elements should be provided so that the operator can confirm that a SIF trip is successful, an alarm being generated by the DCS if a SIF output does not trip to the correct state.
- x) If a control valve also functions as a SIF valve, the SIF should have priority over the process control function.
- xi) If the control valve is fitted with a positioner, the solenoid valve driven by the SIS should be fitted between the positioner and the actuator diaphragm or piston.
- xii) Valves that require leak test should be identified in the SIF SRS, with maximum allowable leak rate defined and the proof test procedure including the leak test requirement. If feasible, provisions should be made for online tightness testing (e.g., pressurization testing for fuel gas valves during a heater start-up sequence).
- xiii) Minimum (if applicable) and maximum allowable time for trip valve full stroke should be specified in the SRS.

A.12. SIS application program development

A.12.1

Add to subclause

It is important to note that application program requirements extend beyond the cause and effects, which are often the only document provided to vendors. SIFs must be properly defined per IEC 61511-1 clause 10.

A.13. Factory acceptance testing

No changes.

A.14. SIS installation and commissioning

No changes.

A.15. SIS safety validation

A.15.2.1

Add to subclause

Validation testing of the SIF can be in segments or end-to-end (e.g., from process fluid at sensor to process fluid at actuation end), with end-to-end preferred. The testing should:

- stimulate the process condition at the sensor to exceed the trip value
- observe the final element at the actuation end to move to the safe state (e.g., valve moves closed)
- reveal dangerous undetected failures in the SIF
- reveal systematic failures which could affect the SIF's ability to function

Where it is not practical to test the SIF from end-to-end in one continuous test and testing in segments is necessary, testing in segments should be designed such that there is overlap in the test portions.

Commentary: A good practice is to use the proof test procedure per IEC 61511-1 clause 16.3.1.2 as the validation test for the SIF.

Some examples of systematic failures that can be detected during validation include inadequate facilities for isolation and testing, common mode failure points (e.g., shared process taps), uncontrolled bypasses (e.g., field bypass, start-up bypass), and inadequate environmental controls (e.g., sealing, shielding, painting, material of construction).

A.16. SIS operation and maintenance

A.16.2.9

Modify subclause

SIS key performance indicators (KPIs) should be developed to analyse discrepancies between expected and actual behaviour of the SIS. KPIs should be regularly reviewed by the FS-Lead and accountable operations and maintenance representatives. Discrepancies should be investigated to identify the underlying systemic causes with actions tracked to closure.

Commentary: some example KPIs include tracking failures, demands, and use of bypasses. The intent is to identify systemic issues such as high failure rates in specific applications or equipment types, high demand rates due to underlying process or equipment conditions, or excessive use of bypasses.

Refer ISO 14224:2016, Annex E.

A.17. SIS Modification

A.17.2.6

Modify subclause

During the operation and maintenance stage, the FSA may be incorporated into the facility MoC process for minor SIF and SIS changes (e.g., setpoint change). These changes should be reviewed and approved by the relevant FS-Lead.

A.18. SIS decommissioning

No changes.

A.19. Information and documentation requirements

No changes.

This page is intentionally blank

London Office

City Tower, Level 14
40 Basinghall Street
London EC2V 5DE
United Kingdom

T +44 (0)20 3763 9700
reception@iogp.org

Brussels Office

Avenue de Tervuren 188A
B-1150 Brussels
Belgium

T +32 (0)2 790 7762
reception-europe@iogp.org

Houston Office

15377 Memorial Drive
Suite 250
Houston, TX 77079
USA

T +1 (713) 261 0411
reception-americas@iogp.org

www.iogp.org

Follow us on Twitter:

[@iogp_news](https://twitter.com/iogp_news)

Connect with us on LinkedIn:

www.iogp.org/linkedin

Follow us on Facebook:

www.facebook.com/IOGPNews

This supplement has been developed to support owner/operating company standards harmonization for safety instrumented systems. This document acts as a supplement to the established industry standard IEC61511.