400 Series:
Process Safety

EHS Design and Maintenance of Safety Instrumented Functions (Plant Trips)

Standard Number:	IVL EHS-409
Version:	1.0
Issue / Revision Date:	09 August 2024

Global Environmental, Health and Safety
Indorama Ventures

Table of Contents

1. Purpose

This standard establishes Indorama Ventures process and minimum requirements for the specification, design, and maintenance of Safety Instrumented Functions (SIFs) to meet target Safety Integrity Levels (SILs) to ensure Indorama risk reduction criteria are met as defined in the IVL EHS-208 Risk Management Standard and Matrix, and as required by the IVL EHS-406 IPL/SIL Assessment Methodology Standard and the IVL EHS-415 Mechanical Integrity Standard.

2. Scope

This standard applies to all Indorama Ventures owned/operated sites as defined in IVL EHS-417 Process Safety Management Applicability Standard. This standard does not apply to third-party warehouses and tollers. This standard also does not apply to joint ventures (JVs) in which Indorama Ventures is a minority owner, unless specifically requested by the related Segment EHS Leader.

This standard describes SIFs operating in demand mode. This standard does not apply retrospectively to existing installed SIFs; however, for existing SIFs installed prior to the issue of this standard, the site must determine and document that the equipment is designed, maintained, inspected, tested, and operating in a safe manner. This standard does apply to new safety instrumented designs, to modifications made to existing safety instrumented designs, and is to be used for the regular revalidation of existing installed SIFs to determine if the existing SIFs meet the required level of risk reduction per the IVL EHS-208 Risk Management Standard and Matrix. SIL 4 SIFs (see section C.4 in Attachment C) are not permitted on Indorama Ventures facilities and are therefore excluded from the scope of this standard.

For the purpose of this standard, the term ‘EHS’ includes process safety, transportation, and security, as well as environmental, health and safety.

This standard must be implemented by each site. Until implementation of this standard is complete, each site must at a minimum be in compliance with the local applicable regulations.

3. Responsibilities

Following is an overview of key responsibilities for this standard. Additional responsibilities, as applicable, are included in Section 4, Requirements.

3.1 Corporate EHS

3.1.1 Provide ongoing technical assistance related to this standard.

3.1.2 Periodically audit sites to determine compliance with this standard.

3.1.3 Review, update and communicate to all Indorama Ventures sites any updates or changes to this standard and associated documents and tools.

3.1.4 Periodically review this standard to ensure its continuing adequacy and suitability to Indorama Ventures operations.

3.1.5 Ensure this standard is consistently implemented from site-to-site within Indorama Ventures.

3.1.6 Communicate, as applicable, any lessons learned as a result of best practices identified or any non-compliances associated with the development and update of this standard.

3.2 Site Head or Designee

3.2.1 Ensure implementation of and compliance with this standard including that it is adhered to and a site-specific program is developed so all personnel receive the proper training, resources, and communications.

3.2.2 Assist with the implementation of the site-specific program; in particular:

- Be thoroughly familiar with the requirements of this standard, the site-specific program, and any associated procedures and work practices.
- Provide support, resources and training needed to carry out the requirements of this standard and the site-specific program.
- Ensure required records are maintained on file.
- Ensure compliance with site-specific program by employees and contractors (as applicable).

3.2.3 Ensure that the existing SIF designs meet the requirements of this standard and/or local regulatory requirements, and that maintenance procedures are determined, documented, and updated within the SIFs Safety Requirement Specification (SRS) documentation.

3.2.4 Ensure new or modified SIFs meet the requirements of this standard and/or local regulatory requirements and that maintenance procedures are determined and documented during the initial design of the new or modified equipment.

3.3 Segment EHS

3.3.1 Ensure that any site or local standard or procedure related to the same topic follows the corporate requirements at a minimum.

3.3.2 Support the site on any technical point related to the standard, including implementation.

3.3.3 Periodically evaluate each site’s level of compliance with this standard.

3.4 Program Owner

3.4.1 Be thoroughly familiar with the requirements of this standard and local regulatory requirements.

3.4.2 Develop and implement a site-specific program that meets the requirements of this standard and any local/regional regulatory requirements.

3.4.3 Periodically review and monitor for compliance with the requirements of this standard, and per local regulatory requirements, at least every five (5) years.

3.4.4 Develop an action plan to correct any non-conformance with local regulatory or Indorama Ventures requirements.

3.5 Project Managers

3.5.1 Ensure that design and maintenance assessments are carried out for expense or capital projects that add or modify SIFs.

3.5.2 Ensure new SIF designs for expense or capital projects meet the compliance requirements.

3.5.3 Ensure new SIF designs have a Functional Safety Assessment (FSA) done by an independent person per Attachment C and industry standards.

3.6 Employees and Contractors

3.6.1 All personnel must understand and follow the requirements of the site-specific program including:

- Being aware of and trained on, as applicable, the legal, regulatory and other associated requirements.
- Immediately reporting any situations that may cause or have a potential to cause a non-compliance.
- Completing any assigned regulatory tasks or actions.
- Being aware of and trained on the process safety information relevant to the process(es) they operate and/or maintain.

3.7 In addition to the roles and responsibilities detailed above, the site-specific program must define and document the roles and responsibilities for all personnel who play a role in implementing the site-specific program, at a minimum:

- Supervisors
- Engineering and Maintenance
- EHS Personnel
- Other applicable functions, as staffed at individual site level

4. Requirements

The site shall establish and maintain a site-specific program to determine the design and maintenance of SIFs that fulfils the following requirements or local regulatory requirements, whichever are the most stringent.

4.1 SIFs shall be used for target SIL 1, SIL 2 or SIL 3 as defined in Attachment C and IVL EHS-406, IPL/SIL Assessment Methodology Standard.

4.2 Instrumented functions that contribute to the risk reduction strategy, but are below SIL 1, shall be designed and maintained per the IVL EHS-415 Mechanical Integrity standard and other recognized and generally accepted engineering practices (RAGAGEPs).

4.3 Flow charts of the methodology required to be used in the design, maintenance, and for regular reviews of safety instrumented functions are shown in Attachment B, and Key SIF Concepts are further explained in Attachment C.

4.4 An SRS shall define the SIF and shall be developed and agreed to by the appropriate personnel, who may include subject matter experts such as the process, instrumentation, and automation engineer. An Example SRS Form is provided in Attachment M.

4.5 The SIF shall be designed to deliver the functionality required by the SIL Target Assessment (see IVL EHS-406 IPL-SIL Assessment Methodology). Details for the SIF design phase are given in Attachment G.

4.6 The design of the SIF and achieved SIL or Probability of Failure on Demand (PFDavg) calculations shall be reviewed by a competent person. Guidance on the use of independent people is given in Attachment C1. An example Design Review Checklist is given in Attachment H. Worked examples are given in Attachment I.

4.7 The SRS shall document the maintenance and testing requirements of the SIF that are required to meet the achieved Safety Integrity Level. Details of maintenance and modification activities are given in Attachment K.

4.8 The SIF shall be designed to enable proof testing.

4.9 The SIF shall be proof tested per the defined SRS requirements. The frequency of testing shall be calculated, unless restricted by national or local codes. Details of the testing activities are given in Attachment J.

4.10 Where minimum proof test periods are governed by operational requirements, for example turnaround frequencies, then this proof test period should be the targeted proof test period specified in the SRS to ensure that the SIF proof testing is completed at the frequency required.

4.11 In the event there is a demand on the SIF, or the SIF fails to operate as intended, or the SIF is found to be in a degraded state at the time of a maintenance activity, a near miss incident investigation should be performed per Attachment K.3. The design of the SIF should be reviewed and evaluated at that time in accordance with Attachment L.

4.12 The following changes shall be managed in accordance with IVL EHS-204, Management of Change Standard:

4.12.1 Changes, including decommissioning, to the SIF.

4.12.2 When changes are made to the manufacturer of any safety instrumented systems which result in a change in reliability data.

4.12.3 For approval of continued plant operation during periods when the SIF is unavailable, such as when bypassed, continued plant operation shall be approved via IVL EHS-204.

4.13 Once a SIF is installed, the basis for the SIF design and maintenance shall be reviewed as necessary based on the performance of the SIF. See details in Attachment L.

4.14 The SIF design, PFDavg calculation, supporting instrument data and required proof test information shall be documented and retained for the life of the SIF.

4.15 SIF installation shall be verified to be consistent with the SRS prior to commissioning of a new or modification of an existing SIF.

5. Training

Training requirements must be defined for the site-specific design and maintenance of safety instrumented functions. At a minimum, all training must be documented with the training date, the names of personnel trained, the names of the trainer(s), the content of the training (or reference to content) and other site-specific/business segment requirements, when applicable.

5.1 Initial

Training on the requirements of this standard and the site-specific program must be provided to Indorama Ventures personnel based on their relevant responsibilities and shall be provided in the local language. At a minimum, personnel and/or management with direct responsibilities for this standard and site-specific program must be trained prior to conducting activities associated with the site-specific program.

5.2 Refresher

Refresher training shall be provided periodically according to the requirements of this standard, the site-specific program, and any local legal requirements, at appropriate intervals (e.g., changes to regulatory requirements, observed user deficiencies), or at least once every three (3) years.

6. Recordkeeping

Records associated with this standard and/or site-specific/regulatory requirements and SIF design and maintenance determinations must be controlled and retained in accordance with regulatory or site business segment record retention requirements, whichever is more stringent. Examples of records to be maintained include but may not be limited to historical instrument failure rates and associated maintenance and proof testing, as well as all data required to be documented for the equipment.

7. References

7.1 IVL EHS-106 Incident Investigations

7.2 IVL EHS-204 Management of Change

7.3 IVL EHS-208Risk Management Standard and Matrix

7.4 IVL EHS-403 Process Hazard Analysis

7.5 IVL EHS-406 IPL/SIL Assessment Methodology

7.6 IVL EHS-415 Mechanical Integrity

7.7 IEC 61508 Functional safety of electrical / electronic / programmable electronic safety related systems

7.8 IEC 61511 Functional safety – Safety instrumented systems for the process sector

7.9 ISA-TR84.00.02 – Part 2 Safety instrumented functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations

7.10 CP-005b, Process Safety Key Performance Indicator Reporting

7.11 Guidelines for Safe and Reliable Instrumented Protective Systems, Centre for Chemical Process Safety, 2007. ISBN 978-0-471-97940-1

7.12 ISA-TR84.00.03-2002 Guidance for Testing of Process Sector Safety instrumented functions (SIF) Implemented as or Within *Safety Instrumented Systems (SIS)*

8. Terms and Definitions

See IVL EHS Glossary and Attachment A.

9. Revision History

Version	Date	Summary of Update	Owner	Approver	Next Review Date
Original	22 June 2023	Initial Release	Chad Wyble, Global Process Safety Program Director	Todd Hogue, VP, Global Head of EH&S	22 June 2026
1.0	09 August 2024	Updated implementation timeframe (Section 2) and Responsibilities (Section 3); made minor editorial updates.	Chad Wyble, Global Process Safety Program Director	Todd Hogue, VP, Global Head of EH&S	09 August 2029

Attachment A: Definitions and Glossary

A.1 Assessment

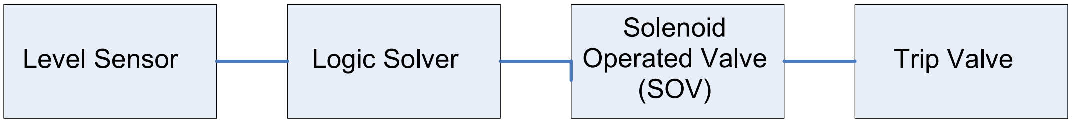
This is the process of examining the design of a *trip* system to verify that it will meet its design requirement. It should cover all stages from Design Specification through to operation, testing, maintenance and management of the system.

A.2 Architecture

The configuration of equipment that makes up the Safety Instrumented Function is termed the architecture. The architecture may involve multiple, redundant (duplicate) or diverse equipment designed to deliver higher integrity levels or availability. The most common architectures are detailed below.

A.2.1 1 out of 1 (1oo1)

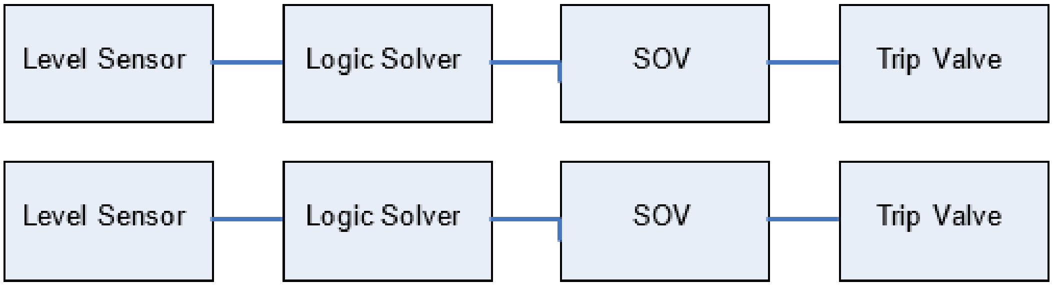
Also called a single channel or simplex loop, this consists of a single sensing device, single logic solver and single *final element*. An example of a 1oo1 level safety instrumented function would be:



In a 1oo1 configuration, the safety function will fail if there is a single equipment failure. For example, if the hazardous event is a tank overfill and the level sensor is a level switch which sticks, then it cannot detect the high level and the hazardous event will occur. A 1oo1 configuration is said to have a Hardware Fault Tolerance of zero (HFT = 0). This defines that the configuration can tolerate zero hardware *faults*.

A.2.2 1 out of 2 (1oo2)

Also called a duplex channel, in its simplest form this consists of two independent Safety Instrumented Functions.



In this case, if either of the level sensors detects the hazardous condition, then the safety function takes place. This configuration can tolerate a single undetected hardware failure and still deliver the safety function. For example, if the level sensors were level switches looking for a high level and one of the switches stuck, then the second level switch is still able to detect the high level and trip the valve. A 1oo2 configuration is said to have a hardware fault tolerance of 1 (HFT = 1), it can tolerate one undetected hardware failure and still deliver the safety function.

Because there is twice the amount of equipment as in a 1oo1 safety instrumented function, the probability of a random detected hardware failure causing an unwanted trip, or *spurious trip*, is twice as high.

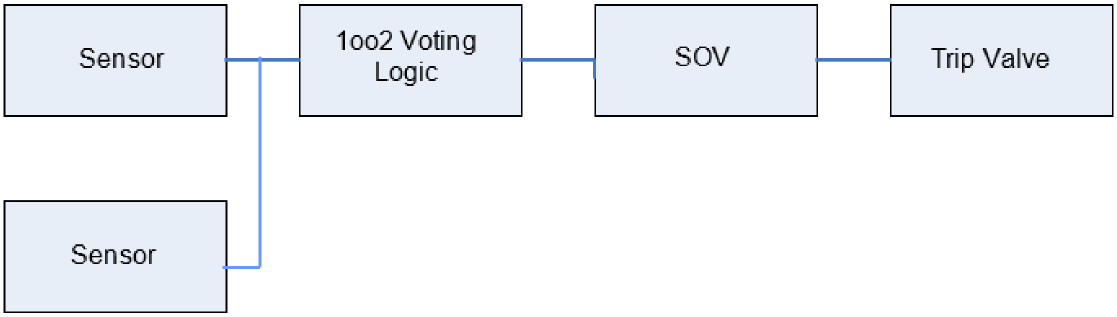
If the same model and type of equipment is used in both channels of the 1oo2 safety function (for example the same level switch is installed in both channels), then the system is said to have *redundancy*.

If a different make or model of equipment is used in each channel (for example a Manufacturer ‘A’ level switch in one channel and a Manufacturer ‘B’ level switch in the other) then the architecture is said to be partially diverse.

If different measurement technologies are used in each channel (for example a level switch and radar level detector or a level switch and a flow meter) then the architecture is said to be diverse.

A.2.3 1 out of 2 (1oo2) subsystem

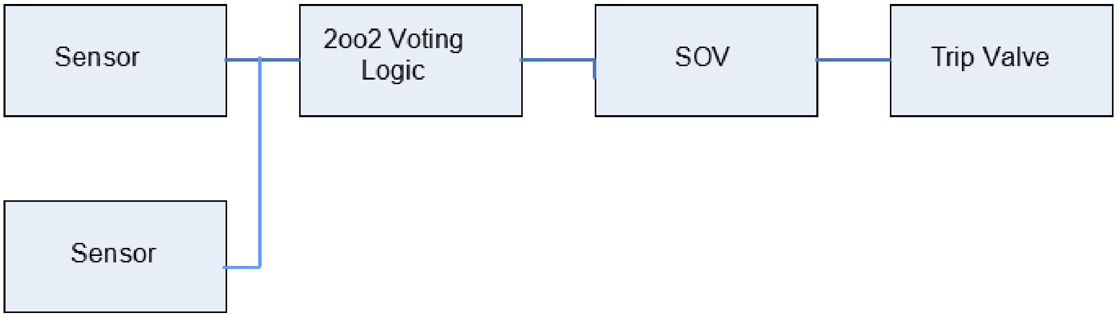
Redundancy can be applied to part of the safety function, for example where two sensors are used to detect the hazardous condition. This configuration allows the testing of one of the sensors while the other remains in service to monitor for the hazardous condition.



A.2.4 2 out of 2 (2oo2)

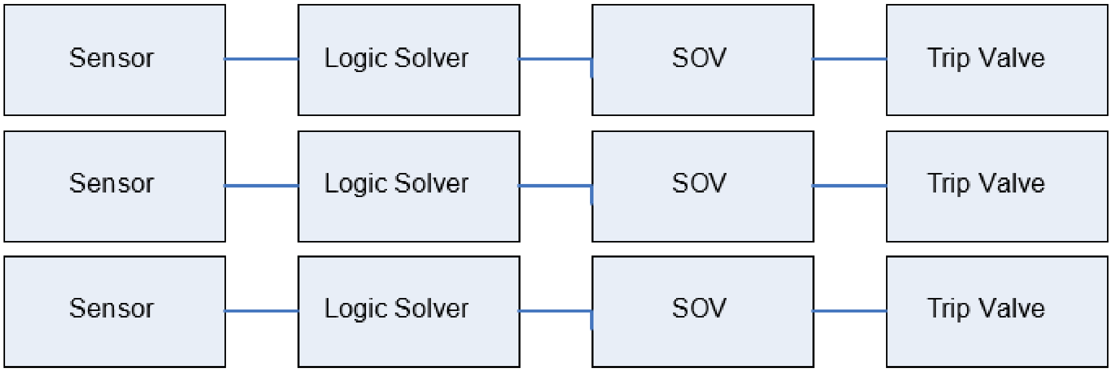
Where the sensors are known to give a high spurious trip rate (for example gas detectors), then higher availability is given by a 2oo2 architecture where both sensors must detect the hazardous event in order to initiate the safety function.

The 2oo2 architecture should be used with caution as a single dangerous failure will render the safety instrumented function in-operable.



A.2.5 1 out of 3 (1oo3)

Three independent channels, if any one of the three sensors detects the hazardous event, then the safety function is delivered.

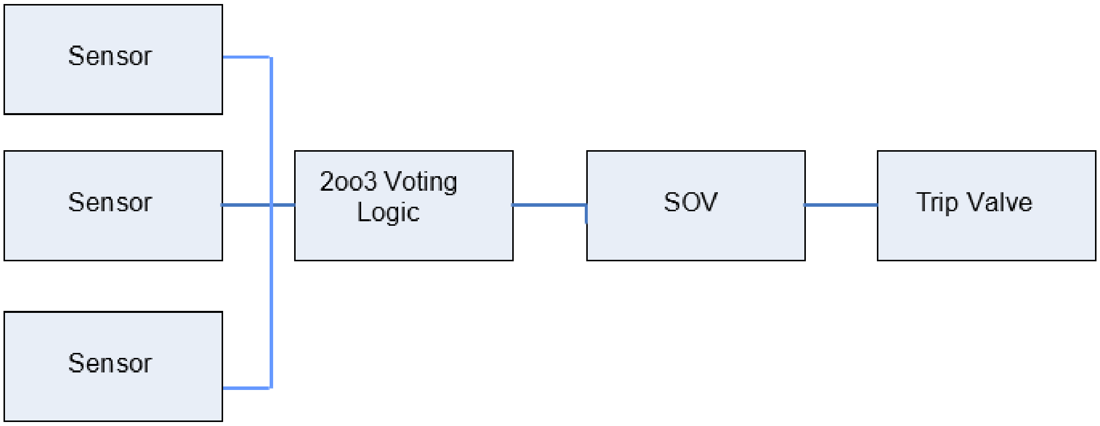


This configuration can tolerate two undetected hardware failures and still deliver the safety function. For example, if the level sensors were level switches looking for a high level and one of the switches stuck and one of the trip valves seized, then two level switches are still able to detect the high level and two trip valves are still available. A 1oo3 configuration is said to have a hardware fault tolerance of 2 (HFT = 2), it can tolerate two undetected hardware failures and still deliver the safety function.

Because there is three times the amount of equipment as in a 1oo1 safety instrumented function, the probability of a random, detected hardware failure causing an unwanted trip, or spurious trip, is three times greater.

A.2.6 2 out of 3 (2oo3)

The most common three channel architecture is where three channels are installed, and two out of the three sensors must detect the hazardous condition before the safety function is initiated. The 2oo3 logic, or voting, is performed in the logic solver. This architecture is a compromise between high levels of integrity and improved rate of unwanted or spurious trips.



A.3 β factor

This is a methodology for quantifying the contribution to the PFDavg made by common cause failures. Values of the β factor will vary depending upon diversity of equipment or diversity of measurement techniques utilised. The value of the β factor depends upon the amount of diversity used in the redundant channels. A range of values for the β factor is quoted below reflecting the different history, culture and methodologies used in facilities. The β factors used at a facility shall be validated by a competent person.

A.3.1 For two identical safety instrumented functions, or two identical subsystems (see Architecture, A.2), the probability of dependent failure is quite high and a value of β in the range of β = 0.15 (15%) to 0.05 (5%) is used.

A.3.2 Where instruments from different manufacturers are used in each safety instrumented function or subsystem, but they utilise the same physical measurement principles, a lower value of β in the range 0.04 (4%) to 0.01 (1%) is used.

A.3.3 Where the safety instrumented function or subsystem works on a different physical principle (for example measuring a temperature and a pressure), then the probability of dependent failure is very low and a value of β in the range 0.01 (1%) to 0.001 (0.1%) is used.

A.4 Common Cause Failure

A single source of failure that causes multiple elements to fail. (The single source can be internal or external to the process or system.)

This is a failure which affects the operation of more than one item in the same time period. It may be a fault causing a demand on the safety instrumented function and at the same time affecting the ability of the safety instrumented function to operate. It may also be a fault affecting more than one channel of a safety instrumented function using multiple channels or redundancy.

A.5 Continuous (or High) Demand Mode

This is where the frequency of demand made by the process upon the safety instrumented function is much greater than once per year, or greater than the proof test period. Continuous or high mode is most commonly found in machinery protection or situations where a gate or guard prevents access to a hazardous area on a process plant.

A.6 Defeat (also known as Bypass, Override or Forcing)

This term describes the prevention of operation of a trip system by an operator or by instrument personnel, usually for trip system maintenance or testing, or to allow plant operation when part of the protective system has failed. The practice of operating a plant when part of the protective system has failed is not normally an acceptable practice, and when adopted should be subject to IVL EHS-204, Management of Change.

A.7 Demand

This is a plant fault condition which requires a protective system or device to take appropriate action in order to prevent a hazardous event.

A.8 Diversity

This term describes performance of the same overall protective function by a number of independent and different means.

A.9 Fail Danger Fault

This is a fault which causes the process to move towards a dangerous condition, or which prevents a trip system from responding to a demand. Such faults are revealed only by testing or by occurrence of the demand.

A.10 Fail Safe Fault

This is a fault which causes the trip system to operate spuriously when no genuine hazardous event exists.

A.11 Failure

This is a change in the condition of an item which makes it unable to perform as designed. A condition of a device under which it is rendered incapable of performing adequately in the desired manner. Failures may be apparent i.e., revealed or hidden i.e., unrevealed.

A.12 Fault

This is a state or condition of an item which makes it unable or potentially unable to perform as designed.

A.13 Final Element

Part of a safety instrumented system which implements the physical action necessary to achieve a safe state.

A.14 Frequency

This is the number of events which occur, divided by the total time during which they happen. (For a function periodic in time, the reciprocal of the period)

A.15 Hardwired Systems

These are systems, e.g., emergency shutdown systems, which are wired directly to accomplish an action in response to an initiating event. These are not programmable and require physical changes to wiring or links to change their function. Examples include relay logic and fixed configuration electronic devices.

A.16 Hazardous Event

The occurrence of an incident with a potential for human injury, damage to property, damage to the environment or some combination of these.

A.17 Independence

Each safeguard must be separate and independent from all other safeguards in order for it to be included in the risk reduction measures for a scenario. For active safeguards (such as trips or interlocks), this means that there must be separation/segregation and independence all the way from the means of sensing that there is a problem through to (and including) the means of action. The active safeguard shall also be separate and independent from the control means that may have failed.

Complete independence is a necessary requirement when using a simple method such as a Risk Matrix. More sophisticated methods, such as with a Fault Tree Analysis, can accommodate a different degree of interdependence.

A.18 Initiator

This is a device which, in response to a plant fault condition, generates a signal to the logic system to initiate the safety instrumented function (trip).

A.19 Interlock Systems

An interlock system consists of one or more initiators, a logic or relay element and one or more output mechanisms (usually valves). The logic element is bi stable and is arranged so that in the event of a pre-defined combination of initiators indicating the approach of an unsatisfactory plant condition, then the logic will switch and operate the output mechanism to prevent the condition from occurring. When the initiators indicate that normal plant conditions have resumed, the logic will switch back to the normal state without any resetting action being taken by the operator. Interlocks are less frequently used than trips because the requirement for the operator to take action to reset a trip makes a contribution to safety and prevents unobserved re-start of a process when plant conditions return to normal. A typical application for an interlock would be to prevent opening of a vessel access cover when the vessel is under pressure or an agitator is operating.

A.20 Logic System

This is the term used for the relay or solid state system which receives the on/off signals from the trip initiators (and from manual trip initiation) and sends out the controlling on/off signal to the trip mechanisms. Where majority voting is required, this would be part of the logic system.

A.21 Low Demand Mode

This is where the frequency of demand made by the process upon the safety instrumented function is not greater than once per year. Low demand mode is the most common demand mode in process plants.

A.22 Majority Voting

This is a means of reducing spurious trips by tripping only when the majority of several measuring devices indicate that a trip is necessary. The most common use is in 2 out of 3 trip initiator systems; in this case at least 2 of the trip initiators have to detect a demand before the trip will occur.

A.23 Neutral Fault

This is a fault on an item which has no effect on its functioning as designed. For example, failure of a 'power on' indicator lamp.

A.24 Probability

This is a dimensionless measure of the uncertainty of the outcome of an event expressed numerically between:

0 impossibility and

1 absolute certainty;

A.25 Probability of Failure on Demand Average (PFDavg)

This is the term used to describe the proportion of the total relevant time for which a component, equipment or system is incapable of providing protection; a dimensionless quantity.

This is also referred to as the average probability of a function failing to respond to a demand.

A.26 Process Safety Time

The amount of time available to detect, diagnose, and take action to bring the process to a safe state once an out of control condition has occurred.

A.27 Programmable Electronic System (PES)

This is the term used to describe digital computers which execute calculations and logical operations using programs stored in memory. It includes Programmable Logic Controllers (PLCs) and microprocessors which are an integral part of an instrument, e.g., microprocessor used in a 'smart' transmitter. See Attachment F – Use of Programmable Devices.

A.28 Proof Tests

A functional test that demonstrates that the instrument, or equipment, will execute its required function and to expose any undetected dangerous or un-revealed faults.

A.29 Proof Test Period

This is the length of time between successive proof tests.

A.30 Redundancy

This term is used to describe the provision of the same overall protective function by a number of independent but identical means.

A.31 Safety Instrumented Function (SIF)

A safety function implemented by instrumented means that puts the plant, process, or activity into a pre-defined safe state.

A SIF consists of a combination of sensors, the logic solver and final elements with a specified safety integrity level that detects an out-of-limit (abnormal) condition and brings the process to a functionally safe state without human intervention, or by initiating a trained operator response to an alarm.

The SIF:

- protects against a specific hazard,
- performs a specific safety function, and
- has a defined range or probability of failure on demand related to a specific SIL and is independent from other protection or mitigation systems.

A.32 Safety Instrumented System (SIS)

Instrumented system used to implement one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), Logic Solver(s), and final elements(s). This can include either safety instrumented control functions or safety instrumented protection functions and may or may not include software.

A.33 Spurious Trip

This is the operation of a safety instrumented function when no process demand is present, usually caused by a failsafe fault.

A.34 Trip

This is the action of a safety instrumented function (plant trip), either when initiated by trip initiators or manually, including spurious operation, to protect against the perceived plant fault condition developing into a hazardous event. Operator action is required to reset the safety instrumented function after normal conditions have been restored.

A.35 Un-revealed Fault

This is a condition which will prevent the function of a component on a system, but which remains unapparent until revealed by a demand or test.

A.36 Validation

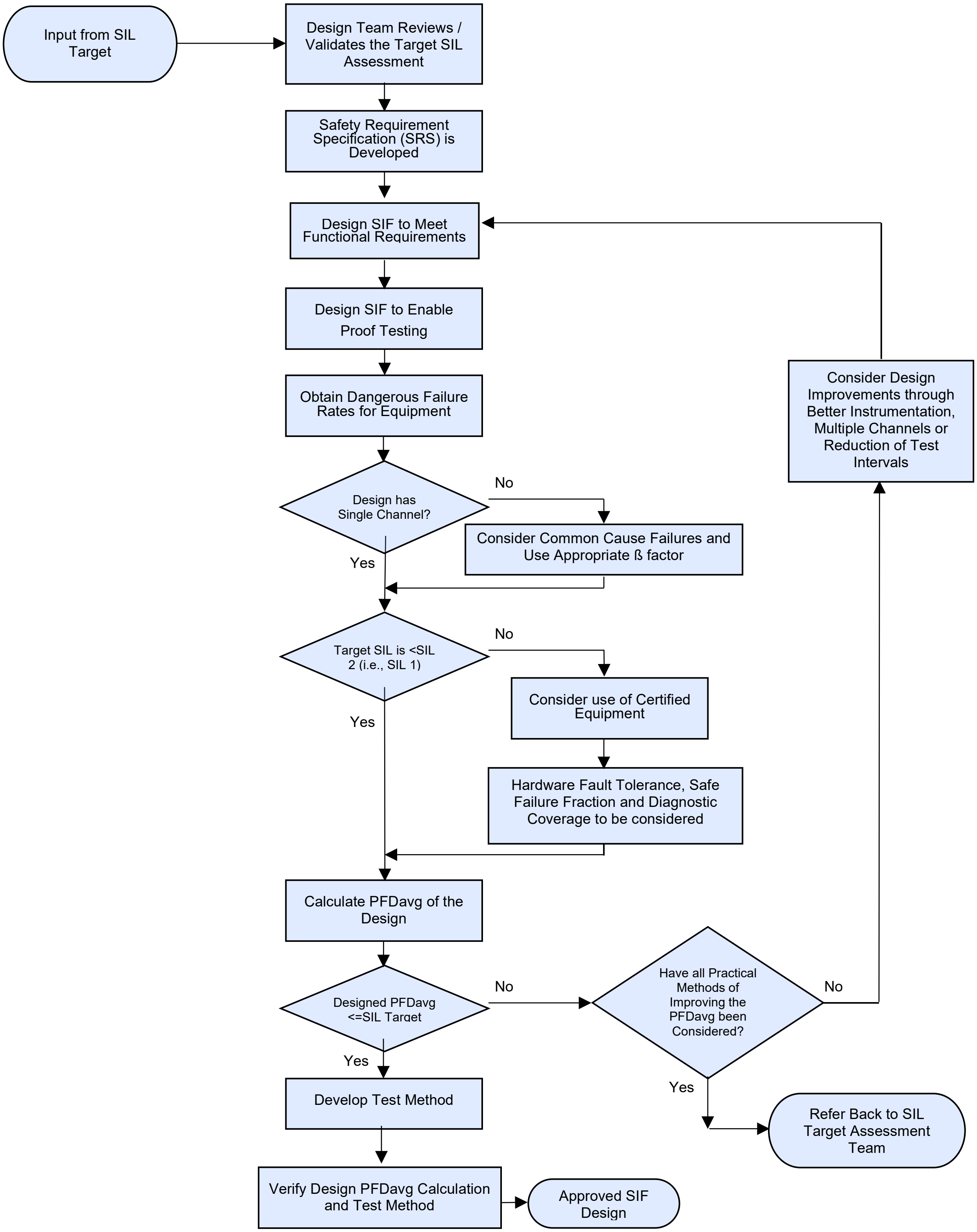
The activity of demonstrating that all safety requirements have been met by the safety instrumented system.

A.37 Verification

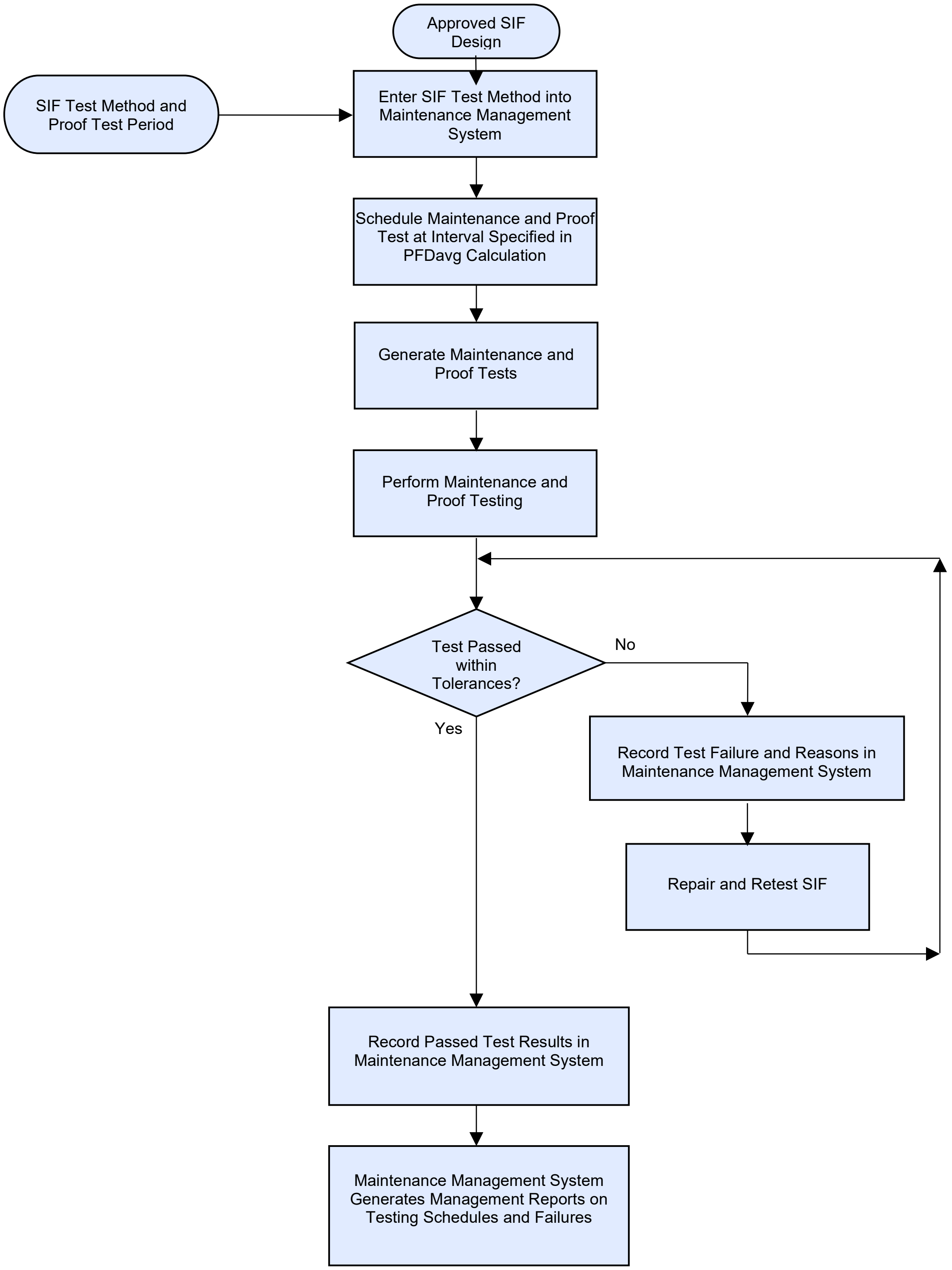
A series of activities to demonstrate that a lifecycle activity has been completed correctly and fully. Examples of verification activities include document reviews, inspections, and testing.

Attachment B: SIF Design, Maintenance, and Review Methodology Flow Charts

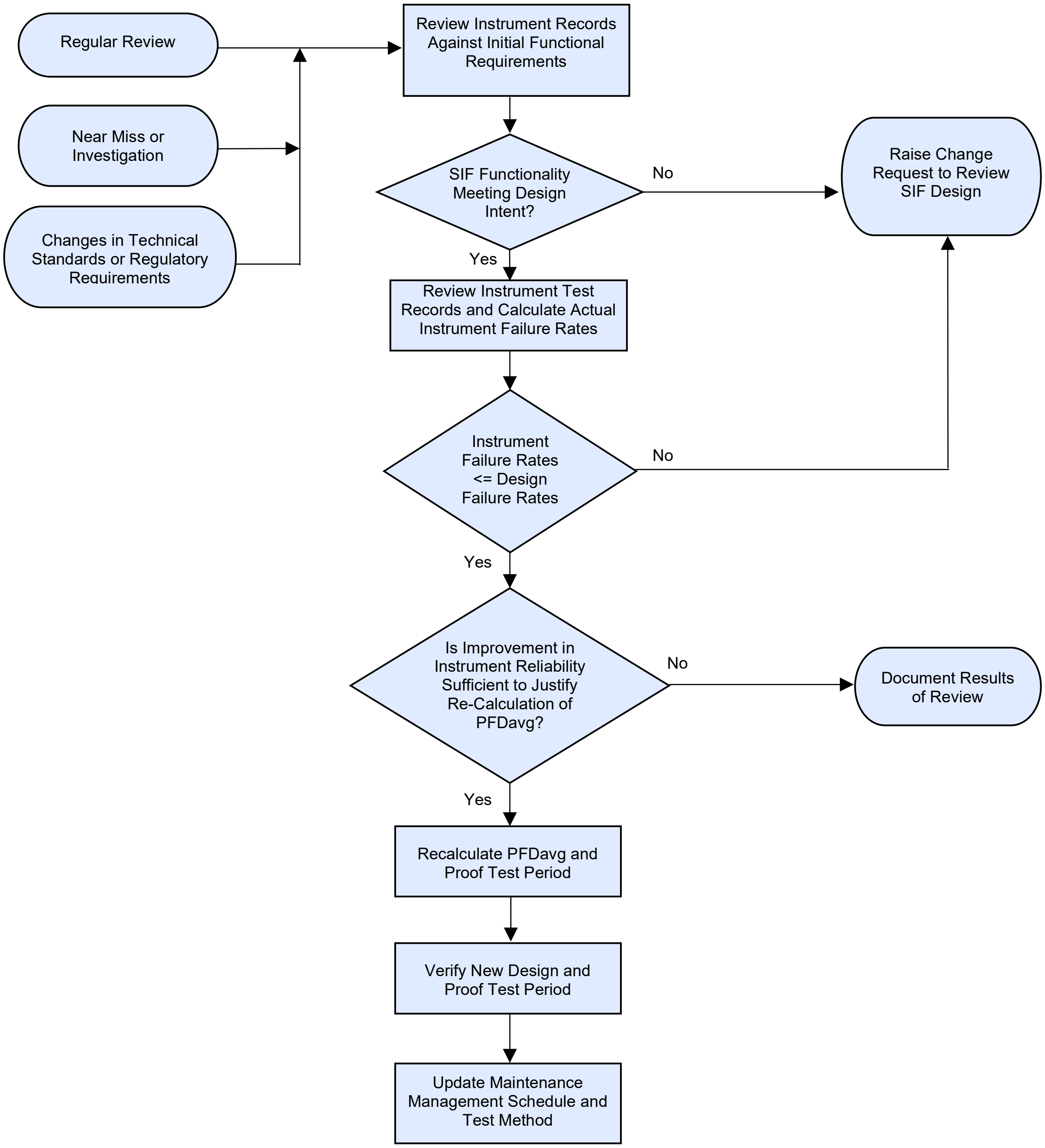
B.1 Calculation of Achieved Safety Integrity Level (SIL) by Safety Instrumented Function (SIF)


Input from SIL Target
Design Team Reviews / Validates the Target SIL Assessment
Safety Requirement Specification (SRS) is Developed
Design SIF to Meet Functional Requirements
Design SIF to Enable Proof Testing
Obtain Dangerous Failure Rates for Equipment
Design has Single Channel?
No
Consider Common Cause Failures and Use Appropriate ß factor
Yes
Target SIL is <SIL 2 (i.e., SIL 1)
No
Consider use of Certified Equipment
Hardware Fault Tolerance, Safe Failure Fraction and Diagnostic Coverage to be considered
Yes
Calculate PFDavg of the Design
Designed PFDavg <=SIL Target
No
Have all Practical Methods of Improving the PFDavg been Considered?
No
Consider Design Improvements through Better Instrumentation, Multiple Channels or Reduction of Test Intervals
Yes
Refer Back to SIL Target Assessment Team
Yes
Develop Test Method
Verify Design PFDavg Calculation and Test Method
Approved SIF Design

B.2 Testing and Maintenance of Safety Instrumented Function (see Attachment K for additional information)


Approved SIF Design
SIF Test Method and Proof Test Period
Enter SIF Test Method into Maintenance Management System
Schedule Maintenance and Proof Test at Interval Specified in PFDavg Calculation
Generate Maintenance and Proof Tests
Perform Maintenance and Proof Testing
Test Passed within Tolerances?
No
Yes
Record Test Failure and Reasons in Maintenance Management System
Repair and Retest SIF
Record Passed Test Results in Maintenance Management System
Maintenance Management System Generates Management Reports on Testing Schedules and Failures

B.3 Regularly Review the Safety Instrumented Function Performance


Regular Review
Near Miss or Investigation
Changes in Technical Standards or Regulatory Requirements
Review Instrument Records Against Initial Functional Requirements
SIF Functionality Meeting Design Intent?
No
Raise Change Request to Review SIF Design
Yes
Review Instrument Test Records and Calculate Actual Instrument Failure Rates
Instrument Failure Rates <= Design Failure Rates
No
Yes
Is Improvement in Instrument Reliability Sufficient to Justify Re-Calculation of PFDavg?
No
Document Results of Review
Yes
Recalculate PFDavg and Proof Test Period
Verify New Design and Proof Test Period
Update Maintenance Management Schedule and Test Method

Attachment C: Key SIF Concepts

C.1 Independent Assessments and Verification

A level of independence for the Functional Safety Assessment (FSA) and verification of Safety Instrumented Functions (SIFs) and alarms shall be established as follows.

The design of each SIF and alarm credited as an Independent Protection Layer (IPL) in a SIL Target Assessment shall be reviewed by a competent person independent of the original design. The reviewer shall determine if each SIF has been designed to meet the functional safety requirements set forth in theSafety Requirements Specification (SRS). The review shall be done per the documented design review described in Attachment H.

C.2 Protective System Failure Modes

C.2.1 Equipment in a protective system can suffer various types of faults.

C.2.1.1 Safe failure – the safety instrumented function performs its safety function without the hazardous condition being present. This is often caused by an equipment fault that causes the safety function to fail safe – for example loss of instrument air or electrical power leading to a trip valve moving to the safe position.

C.2.1.2 Dangerous failure – a failure of equipment stops the safety instrumented function delivering its required functionality when the hazardous condition is making a demand. The equipment failure is not known to the protective function or to the operations staff, for example seizing of a trip valve stem preventing the valve from moving on demand.

C.2.1.3 Detected failure – if the instrument has built in diagnostics, then some failures can be detected, and the device driven to a pre-defined operational state. Detected failures may be discovered through normal operation or through dedicated detection methods.

C.2.2 For a safety instrument with built in diagnostics, there are four failure modes:

C.2.2.1 Safe Undetected failures (SU) – the failure is not detected by the diagnostics, but the failure leads to the process being put in a safe state.

C.2.2.2 Safe Detected failures (SD) – diagnostics detect a failure in the instrument and drives the instrument to a safe state.

C.2.2.3 Dangerous Detected (DD) – a potentially dangerous failure is detected by diagnostics and either; the instrument takes remedial action (for example driving the instrument signal to 0 mA) or a signal is sent to the logic solver where remedial action takes place, or an alarm or warning indication is shown.

C.2.2.4 Dangerous Undetected (DU) - a failure of equipment that has not been detected by the diagnostics and prevents the safety instrumented function from delivering its required functionality when the hazardous condition is making a demand.

C.2.3 A measure of the effectiveness of the diagnostics is called the Safe Failure Fraction (SFF). If the four failure modes are represented by:

λ_{SU} = Safe Undetected failure rate

λ_{SD} = Safe Detected failure rate

λ_{DD} = Dangerous Detected failure rate

λ_{DU} = Dangerous Undetected failure rate

Then the Safe Failure Fraction is:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

C.2.4 For Programmable Logic Controllers (PLC), if TUV Certification is not provided, use the table below to determine the minimum Hardware Fault Tolerance (HFT) necessary for the SIL protection required. Reference IEC 61508 Part 2.

SIL	Minimum Hardware Fault Tolerance for Programmable Logic Controllers		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC61508)		

C.2.5 This tables indicates that a single, standard control PLC, with no special diagnostics (SFF < 60%) could not be used for SIL 1 applications (HFT = 1).

C.2.6 A single, higher specification PLC with higher levels of internal diagnostics (SFF 60% to 90%) could be used for SIL 1 applications (HFT = 0).

C.2.7 A PLC specifically designed for safety applications, sometimes termed a ‘Safety PLC’ will have the highest levels of diagnostics (SFF > 90%) and a single Safety PLC may be used for SIL 2 applications.

C.2.8 Many PLCs will employ multiple, cross checking I/O boards and processors that give a level of hardware fault tolerance.

C.2.9 For the other instrumentation that makes up the SIF (sensors, non-programmable logic solvers and final elements), requirements for hardware fault tolerance is shown in IEC 61508 Part 2 Table 2 for Type A Devices and Table 3 for Type B Devices.

C.2.9.1 IEC 61508 Table 2 : Type A Devices.

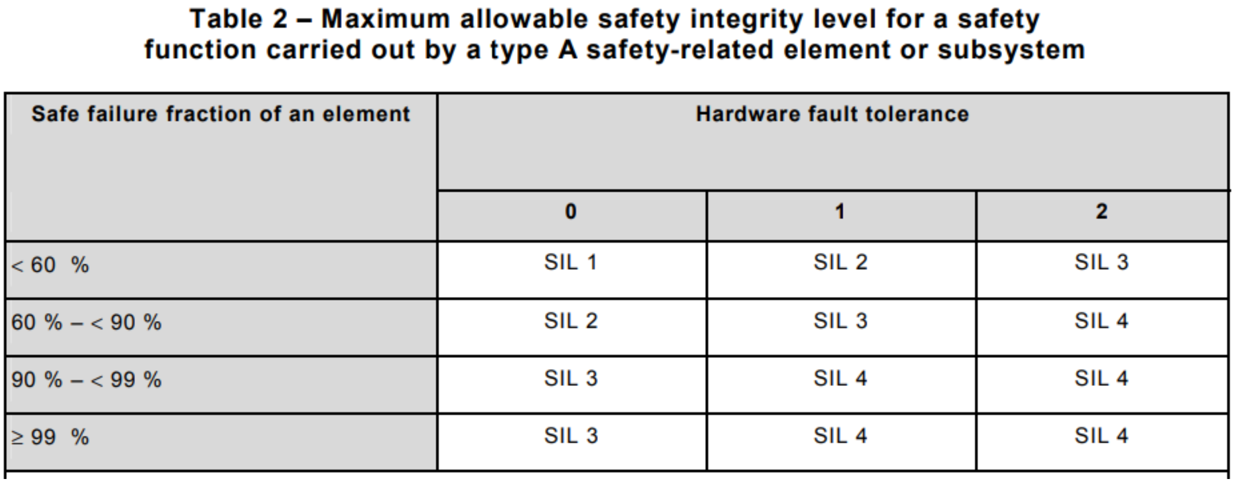


Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

C.2.9.2 IEC 61508 Table 3 : Type B Devices.

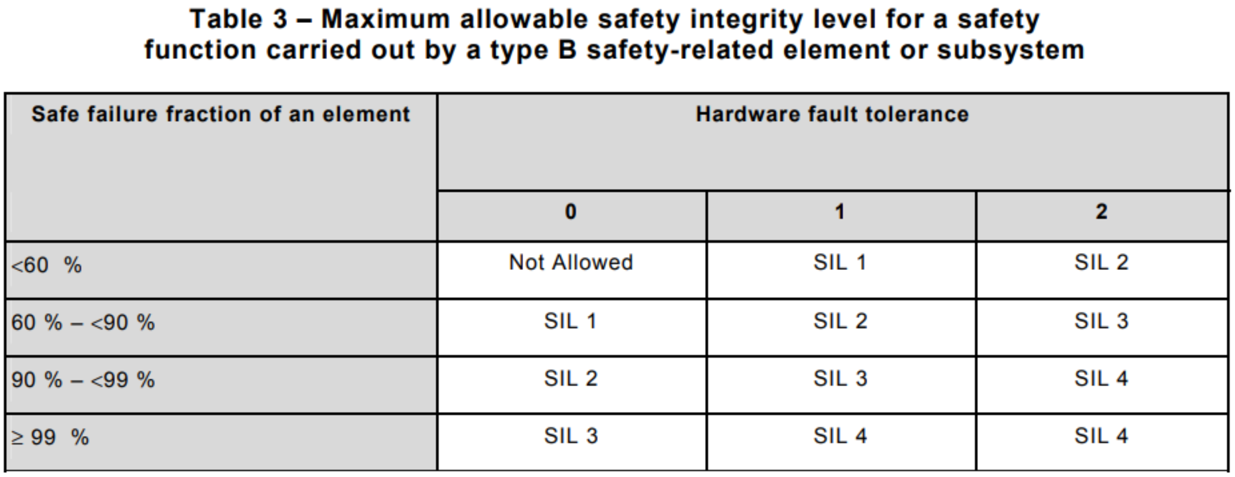


Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

C.2.10 An element is regarded as type A if all of the following criteria are met for the components required to achieve the safety function:

C.2.10.1 The failure modes of all constituent components are well defined; and

C.2.10.2 The behaviour of the element under fault conditions can be completely determined; and

C.2.10.3 There is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

C.2.11 An element shall be regarded as type B if one or more of the following criteria is met for the components required to achieve the safety function:

C.2.11.1 The failure mode of at least one constituent component is not well defined; or

C.2.11.2 The behaviour of the element under fault conditions cannot be completely determined; or

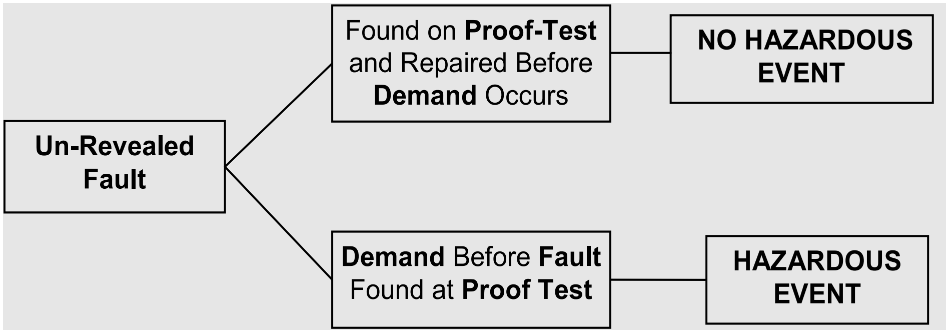
C.2.11.3 There is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

C.2.12 Exceptions to this hardware fault tolerance guidance permitting fault tolerance reduction by one level are detailed in IEC 61511 part 1 section 11.4.4. The exceptions involve having good plant experience and knowledge of the device and being able to minimise the ability to perform uncontrolled modifications to the device.

C.3 Proof testing

C.3.1 Protective systems require proof testing at pre-determined intervals to ensure that faults which could prevent correct function are detected and that equipment is restored to an ‘as new’ condition or as close as is practicable to this condition. If no proof testing is carried out, each un-revealed fault will result in a subsequent hazardous event when the demand occurs.

C.3.2 If proof testing is carried out much more frequently than demands occur, the majority of un-revealed *fail danger* faults will be found and very few of the demands will result in hazardous events.


Un-Revealed Fault
Found on Proof-Test and Repaired Before Demand Occurs
NO HAZARDOUS EVENT
Demand Before Fault Found at Proof Test
HAZARDOUS EVENT

C.3.3 PFDavg is not only affected by the proof test periods, but by the way in which the test is conducted; thus, the probability has to allow for:

a. Un-revealed fault, e.g., a sticking shutdown valve (if it is not included in the test procedure).
b. Time during which a SIF is isolated for maintenance or repair.
c. SIF left isolated after test.
d. Duration under test (with partial or total disablement).
e. SIF incapable of providing protection, e.g.,, design or maintenance fault makes the system response too slow.

C.3.4 The time taken to repair a fault and restore the functionality of a safety instrumented function is the mean time to restoration (MTTR). An allowance for the time that the safety instrumented function can be unavailable and still achieve the target SIL can be built into the PFDavg calculation. The MTTR becomes more significant for higher target SILs.

C.3.5 The contribution from down time for testing will increase with more frequent testing. Some of the other factors such as time isolated for maintenance, SIF left isolated after test or design / maintenance fault will not benefit from increased proof testing. Therefore, testing too frequently may not only be costly, but may actually reduce availability.

C.3.6 Where demands occur very frequently (i.e., tens of times per year) there is no significant value in testing a single channel SIF, although a regular condition inspection is desirable. In such cases the design or operation of the process should be further investigated.

C.3.7 The Safety Instrumented Function shall be regularly inspected to ensure that there are no unauthorised modifications and no observable deterioration to the equipment or process connections. The visual inspection may take place as part of the proof test, or it may be conducted at a different frequency. The results of the inspections shall be recorded.

C.4 Safety Integrity Level (SIL)

C.4.1 Safety instrumented functions (Plant Trips) are designed to meet a specific SIL target which is expressed in terms of the required PFDavg (i.e., the average probability that the system will be in a failed state when a demand occurs). The Process Hazard Analysis (PHA) and associated SIL target assessment will normally specify the target PFDavg value, and it is the task of the design activity to provide a protective system of the required SIL which, with correct use and routine testing and maintenance, will retain this reliability throughout its life. Proof test periods and test methods should be defined as part of the design activity.

C.4.2 There are four quantified SIL grades. The lowest reliability systems are SIL 1 and the highest SIL 4.

C.4.3 The achievement of a SIL 4 safety instrumented function is not considered practicable or desirable in the process industries. SIL 4 safety instrumented functions are not permitted on Indorama Ventures facilities.

C.4.4 The following definitions for SIL levels refer to Demand Mode of Operation (i.e., where the demand placed upon the SIF is not greater than once per year or the failure rate is much lower than the proof test interval):

C.4.4.1 SIL 1

SIL 1 systems have a PFDavg within the following range: 0.01 ≤ PFDavg < 0.1. This performance can be realised by simple systems usually without resorting to redundancy. They use conventional quality materials and good design practices; the majority of safety instrumented functions should be SIL 1.

C.4.4.2 SIL 2

SIL 2 systems have a PFDavg within the following range: 0.001 ≤ PFDavg < 0.01. To achieve this grade of reliability, systems should be very carefully designed. Use may be made of redundancy, e.g., two identical process measurements, or trip mechanisms. Likely sources of common cause failure to danger should be identified and eliminated.

C.4.4.3 SIL 3

SIL 3 systems have a PFDavg within the following range: 0.0001 ≤ PFDavg < 0.001. This grade of reliability is extremely difficult to achieve and maintain. For this reason it should be recognised that the design of such systems requires specialist techniques, which may require the experience and formal training of competent engineers with SIL 3 design experience. Such systems are extremely rare in the process industries.

C.4.5 These failure rates are summarised from the following tables taken from IEC 61511 – Clause 9.2.4. Tables for both Demand Mode and Continuous Demand Mode are shown; Demand Mode is the most commonly found method for the protection of hazards in process industry.

Demand Mode of Operation		
SIL	Target average probability of failure on demand - PFDavg	Required Risk Reduction
1	>= 10^{-2} to < 10^{-1}	>10 to <= 100
2	>= 10^{-3} to < 10^{-2}	>100 to <= 1,000
3	>= 10^{-4} to < 10^{-3}	>1,000 to <= 10,000
4	>= 10^{-5} to < 10^{-4}	>10,000 to <= 100,000

Continuous Mode or Demand Mode of Operation	
SIL	Target frequency of dangerous failures (per hour)
1	>= 10^{-6} to < 10^{-5}
2	>= 10^{-7} to < 10^{-6}
3	>= 10^{-8} to < 10^{-7}
4	>= 10^{-9} to < 10^{-8}

C.5 Guidance when a safety instrumented function is unavailable.

C.5.1 The detection of a dangerous fault in the safety instrumented function (by proof test, diagnostics, inspection or other means) used in demand mode shall result in either of the following actions.

C.5.1.1 A specified action to achieve or maintain the process in a safe state.

C.5.1.2 Continued plant operation while the faulty part is repaired. If the mean time to restoration (MTTR) does not take the PFDavg outside the target SIL, then continued plant operation may take place with the continued safety of the process supplemented by additional measures and constraints. Redundant systems can rely on other functioning devices within the Safety Instrumented System (SIS). Non-redundant systems require additional measures. If the faulty part cannot be repaired within the maximum MTTR allowed by the PFDavg calculation, then a specified action shall be performed to achieve or maintain the process in a safe state.

C.5.2 Continued plant operation may be possible upon detection of a fault by the use of defeats, overrides, bypasses or forces.

C.5.3 Continued plant operation shall be approved by the Management of Change procedure (IVL EHS-204).

C.5.4 More detailed guidance is given in IEC 61511 Clause 11.3.

C.6 Bypasses, overrides, forces and defeats

C.6.1 Overrides and bypass capabilities necessary for testing, maintenance and normal operation, shall be designed and implemented into the system and tested such that logic does not have to be modified or forced by an individual to inhibit the trip or interlock.

C.6.2 There shall be a formal approval process for authorization of any overrides or bypasses. There should also be restricted access as to who can invoke the bypass.

C.6.3 Bypasses of all or part of a SIF shall be logged, preferably automatically. There should be continued visual indication of each specific bypass or override that is activated – this can be via an HMI graphic or other means. Verbal alert or communication is also recommended.

C.6.4 Automatic alerts should occur to the operator once per shift while the bypass or override continues to be activated. Facilities may also establish systems to notify other associates with operational authority, i.e., email notifications.

C.6.5 Direct forcing of logic via programming/monitoring software tools should be avoided, but if it is temporarily deemed necessary, then it shall be done per Management of Change, IVL EHS-204. If determined to be necessary for testing or normal operation, it shall be configured into the system and tested at the first opportunity.

C.6.6 SIFs and SIS Logic shall be designed to minimize the need for temporary start-up bypasses (e.g., low flow trip, etc.). However, if deemed necessary, start-up enable logic shall be designed to temporarily bypass the trip until the process is sufficiently past the trip point. The start-up enable logic would be invoked by the operator, and it shall automatically reset to enable the trip based on time and possibly also by monitoring conditions available to the SIS.

C.6.7 Overrides and bypasses utilized by operating and maintenance personnel shall be registered/logged by the facility to ensure the device is placed back in service to prevent unlimited/indefinite disabling of safety functions. This applies to HMI graphics or other means normally used to interface with the process or safety system.

Attachment D: SIF Standard Calculations

D.1 There are a number of techniques for calculating the PFDavg for a safety instrumented function. A description of the techniques can be found in IEC 61511 Part 2 Annex D.

D.2 In general, the PFDavg is derived from standard calculations. These calculations can be found in IEC 61508 Part 6 Annex B and ISA TR 84.00.02 Part 2.

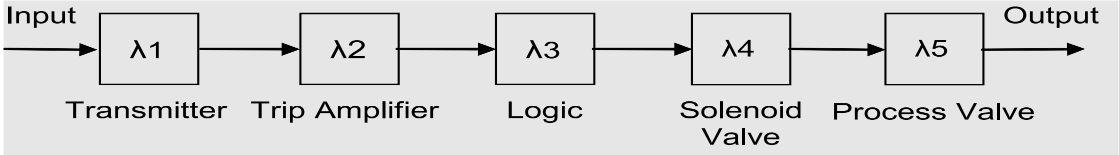
D.3 Simplified and commonly used versions of PFDavg calculations are reproduced below for low demand operation and are valid for the majority of standard applications.

D.4 Where high Safety Integrity Levels (SILs), and consequently very low PFDavg values, are required then the more complex variants of the standard calculations may be considered. These calculations incorporate concepts such as Mean Time to Repair (MTTR), Diagnostic Coverage levels (DC), Dangerous Undetected failure rates (λDU) and Dangerous Detected failure rates (λDD).

D.5 The following calculations are valid for low demand of operation.

D.6 Calculation of PFDavg for a Single Channel (1 out of 1, 1oo1).

D.6.1 This shows a block diagram of a typical trip safety instrumented function (SIF). Each of the components has a failure rate, λ



D.6.2 The failure to danger of any component in a simple single channel system will result in the whole system being rendered incapable of providing protection, and thus the total fail to danger rate is the sum of the failure to danger rates of each individual component.

D.6.3 The system failure to danger rate is the sum of the dangerous failure rates for each component.

$\lambda D = \lambda D1 + \lambda D2 + \lambda D3 + \lambda D4 + \lambda D5$

Where $\lambda D1$, $\lambda D2$, $\lambda D3$ etc. are failure rates/year for individual components in a simple trip system.

D.6.4 The dangerous failure rate is the sum of the dangerous detect, λDD, and dangerous undetect, λDU failure rates.

$\lambda D = \lambda DD + \lambda DU$

The dangerous undetect failure rate, λDU, usually dominates over the dangerous detect failure rate, λDD. For this example, λDD is considered negligible (i.e. $\lambda DD << \lambda DU$ and therefore $\lambda D = \lambda DU$).

PFDavg $= ½ \times \lambda DU \times T$

Where: T = proof test period in years.

D.6.5 The simple calculation can also be expanded to consider each component:

PFDavg = PFD1avg + PFD2avg + PFD3avg + PFD4avg + PFD5avg

Where PFD1avg $= ½ \times \lambda D1 \times T1$

PFD2avg $= ½ \times \lambda DU2 \times T2$, etc.

T1 = Proof test period of the transmitter

T2 = Proof test period of the trip amplifier, etc.

D.6.6 This alternative form of determining PFDavg is useful where different proof test periods are used. This is common when only partial or staggered testing of the elements is possible, e.g., transmitter can be tested every 3 months, but the valve can only be tested every 12 months during the plant shutdown.

D.6.7 The spurious trip rate, also called the safe failure rate, is λS which is normally given as safe failures per year.

$\lambda S = \lambda S1 + \lambda S2 + \lambda S3 + \lambda S4 + \lambda S5$

Where λS1, λS2, λS3 etc. are spurious trip rates/year for individual components in a simple trip system.

D.7 Two Channel System (1 out of 2 voting, 1oo2)

D.7.1 This redundant configuration is used to give a higher level of PFDavg, but the spurious trip frequency is twice that for the non-redundant configuration. Additional detail on this architecture is given in A.2.2.

D.7.2 Consideration of common cause dependant failures results in an extra term being added to the calculation, and so the full calculation is:

PFDavg $= 4/3\ [PFDavg1]2 + \beta[PFDavg1]$ or

PFDavg $= 1/3\ [\lambda_{DU}^2 \times T^2] + \beta[½ \times \lambda_{DU} \times T]$

D.7.3 PFDavg1 is the average probability of failure on demand for a single channel system.

D.7.4 Where two diverse channels are used, then the PFDavg of the ‘worst’ channel should be used for PFDavg1.

D.7.5 The value of the β factor depends upon the amount of diversity used in the redundant channels.

D.7.6 Because a failure of either channel will result in a trip, the spurious trip rate is 2 λS where λS is the safe failure rate.

D.8 Two Channel System (2 out of 2 voting, 2oo2)

D.8.1 Where higher availability is required the configuration should be made 2 out of 2 and the PFDavg is given by:

PFDavg = 2 x PFD_{avg1}

D.8.2 Because both channels need to fail to initiate the trip condition, the spurious trip rate is 2λ2S x TR where λS is the safe failure rate and TR is the mean time to repair.

D.8.3 The 2oo2 architecture should be used with caution as a single dangerous failure will render the safety instrumented function in-operable.

D.9 Three Channel System (1 out of 3 voting, 1oo3)

D.9.1 PFDavg $= 2[PFDavg1]3 + \beta[PFDavg1]$ or

PFDavg $= 1/4\ [\lambda DU3 \times T3] + \beta[½ \times \lambda DU \times T]$

D.9.2 Because a failure of any channel will result in a trip, the spurious trip rate is 3 λS where λS is the safe failure rate.

D.10 Three Channel System (2 out of 3 voting, 2oo3)

D.10.1 This architecture is commonly used because of the reduced spurious trip rate and ability to remove one channel for testing while still retaining a duplex voting safety function.

PFDavg = 4[PFDavg1]2 + β[PFDavg1] or

PFDavg = $[\lambda_{DU}^2 \text{ x } T^2] + \beta[½ \text{ x } \lambda_{DU} \text{ x } T]$

D.10.2 The spurious trip rate is 6λ2S x TR where λS is the safe failure rate and TR is the mean time to repair.

Attachment E: Use of Instrument Data for Dangerous Failure Rates

E.1 Dangerous failure rates for instrumentation are used in calculating the PFDavg. The dangerous failure rates shall be approved by a competent person(s) and are generally obtained from three sources.

E.1.1 Where available, historical facility records of instrument failure rates shall be used for the calculation of the PFDavg. These values reflect the environmental, operational and process conditions on the plant as well as the quality of installation, maintenance and repair activities.

Sufficient data shall be available to statistically justify the facility based failure rates. Guidance is given in IEC 61508 Part 1, 7.4.7.4 a) Note 1 and IEC 61511 Part 1 11.9.2 c) and these standards recommend at least a 70% confidence limit. IEC 61511 Part 2 11.9.2 recommends the 'Chi-square' test for calculating the confidence level, and references the book 'Reliability, maintainability and risk' for a description of the method.

In order to assist in the gathering of a sufficient body of instrument data to enable facility specific data to be calculated, failure rates of the same make / model instrument used in a control application, but operating under the same environmental, operational and process conditions may be used.

Any calculation of facility specific instrument failure rates shall be performed by a competent person.

E.1.2 Where facility records are not available, instrument failure rates obtained from recognised national, industry or *company* publications (often referred to as 'Generic Data') is generally used.

Generic data sets provide limited instrument failure data that has been obtained from a number of installations over a period of time. To reflect the differing process plants from which the data is collected, these values are conservative, and in many cases represent a worst case. Generic data will incorporate failures from associated equipment and interfaces to the instrument, such as junction boxes and impulse lines.

Generic data sets commonly used are the SIS-Tech SIL Solver tool database, the Exida SILver data set or the OREDA data book.

The generic data value shall be adjusted to compensate for known adverse process or environmental conditions. For example, if the process fluid is known to be 'dirty' and often blocks instruments or associated equipment, a Duty Factor of 2 or 4 may be multiplied to the generic data value to reflect this known operational condition.

Credit for extra diagnostics in the instrument may be taken provided that the diagnostics are fully utilised and continued correct operation of the diagnostics and associated safe failure fraction is demonstrated.

Some computer based tools that support PFDavg calculations will be pre-loaded with generic data sets.

E.1.3 Manufacturer supplied failure rates are often supplied with instrumentation, or as part of a safety certificate. These failure rates are predicted failure rates based upon known component failure rates and failure mode analysis.

Manufacturer's failure data is often 10 to 100 times better than equivalent generic data. This may be due to internal diagnostics detecting failures or the failure rate relating only to the instrument, and not considering process or electronic interfaces.

Manufacturer's failure data shall only be used by experienced and competent engineers who fully understand the limitations and constraints detailed in the manufacturers' documentation.

Engineering judgement and plant experience should be used to verify that the diagnostics are fully utilised and can drive the safety function to the safe state and that the scope of the manufacturer’s failure rate relates to the full extent of the instrument and associated equipment. Demonstration of the continued correct operation of the diagnostics and associated safe failure action may be problematical.

Adjustments to the manufacturer’s data may be made to compensate for known adverse process or environmental conditions and for lack of coverage of diagnostics. An order of magnitude difference between manufacturers’ data and generic data values shall be justified.

Attachment F: Use of Programmable Devices

F.1 Programmable systems, generally Programmable Logic Controllers (PLCs), are widely used as the logic solver in safety instrumented functions. These systems offer many advantages such as:

F.1.1 Easy to use monitoring and display facilities.

F.1.2 Software tools for configuration and management of the logic.

F.1.3 Pre-approved software function blocks give standard methods for routine safety functions.

F.1.4 Ease of modification.

F.1.5 Diagnostics for detection of faults in the PLC and its I/O subsystems.

F.1.6 Better detection and location of faults.

F.1.7 Advanced testing facilities.

F.1.8 Cost effective for large number of safety functions.

F.2 Programmable systems also have disadvantages, such as:

F.2.1 High cost for low number of safety functions.

F.2.2 Common cause failure – failure of PLC will render all safety functions inoperable.

F.2.3 Ease of modification.

F.2.4 Reliability of software.

F.3 Several of these disadvantages can be solved by the use of certified or ‘safety’ PLCs. These systems will have:

F.3.1 High levels of in-built diagnostics to detect faults in the PLC or I/O.

F.3.2 Unauthorised access to software is controlled by security measures.

F.3.3 Software will have been designed and programmed using approved methodologies to give high levels of reliability and assurance of performance.

F.4 The programmable logic solver shall meet the highest target Safety Integrity Level (SIL) of the safety instrumented functions implemented within it. For example, if a safety PLC has 101 safety functions implemented in it, 100 are target SIL 1 and 1 is target SIL 2 then the PLC shall meet the requirements of SIL 2.

F.5 The programmable logic solver shall be certified for use in safety applications.

F.6 The programmable logic solver shall be independent from the process control system.

F.7 The programmable logic solver shall have diagnostics that detect internal faults, I/O checks, processor faults and memory checks.

F.8 The programmable logic solver shall utilise limited or fixed variability programming languages for configuring / coding programmable safety systems.

F.9 The Safety Instrumented System (SIS) should be designed to have a manual means of taking the final elements to a fail-safe position. This action may be accomplished by direct actuation of final elements or through a hardwire link to the SIS logic solver. "Soft" keys implemented in the BPCS or SIS HMI are permitted but should not be the only manual means of taking the process to a safe state. Any trip action initiated by manual means should be indicated to the operator. If a manual shutdown is required as part of a SIF, then it will have to be wired and indicated in a manner that meets appropriate SIL design.

Attachment G: Design Activities

G.1 Dangerous failure rates for the instrumentation defined in the design of the safety instrumented function shall be used to calculate the PFDavg achieved by the design. Dangerous failure rates shall be approved by a competent Person.

G.2 Pre-approved standard designs (sometimes termed typical or cookbook designs) may be used; these shall be approved by a competent Person and regularly reviewed.

G.3 Further direction on the use of instrument data is given in Attachment E. Standard calculations to be used for calculating the PFDavg are given in Attachment D.

G.3.1 Where historical facility records of instrument failure rates calculated from safety and control instruments used on similar duty, service and environment are available, then these failure rates shall be used for the calculation of the PFDavg. Sufficient data shall be available to statistically justify the use of historical facility records. Further guidance on the use of statistic methods to derive confidence levels is given in Attachment E.

G.3.2 Where facility records are not available, instrument failure rates used in calculating the PFDavg shall be obtained from recognised national, industry or company publications.

G.3.3 Where manufacturer supplied failure rates are used in calculating the PFDavg, engineering judgement and plant experience shall be used to verify that claimed diagnostics are utilised and the scope of the manufacturer's failure rate relates to the full extent of the instrument as installed.

G.3.4 Instrument failure rates shall be adjusted to compensate for known adverse process or environmental conditions.

G.4 For target Safety Integrity Level (SIL) 1 safety instrumented functions utilising a single sensor and final element, standard good quality instrumentation may be used. This relates to instrumentation that is not specifically designed or sold for a safety duty but has a history of good performance at the facility.

G.5 For multiple (redundant) channel designs, the common cause fault contribution to the PFDavg shall be calculated using an appropriate β factor.

G.6 For target SIL 2 or SIL 3 safety instrumented functions, the following additional guidelines should be considered.

G.6.1 Equipment certified by an independent body as suitable for the target SIL should be considered

G.6.2 Where SIL certified equipment is not available or utilised, historical facility records of the instrument may be used for a justification. The justification shall be performed by a competent Instrument Engineer and documented. Guidance on the use of facility records is given in Attachment E.

G.6.3 Where certified equipment or facility records are not available or utilised a competent Instrument Engineer shall perform an assessment of the instrument to determine that the device has the desired behaviour and reliability. The justification shall be documented and may be derived from recognised national, industry or company publications

G.6.4 Hardware Fault Tolerance (HFT), Safe Failure Fraction (SFF) and Diagnostic Coverage (DC) requirements for the target SIL shall be met.

Attachment H: Example of Design Review Checklist

H.1 This list is an example of the activities to be checked as part of the design review process. It is not considered an all-inclusive list. Refer to Clause 7 of IEC 61511 for more details. Performing the required design reviews during the Safety Instrumented System (SIS) safety life-cycle is mandatory. Additions to this list may be made based on facility experiences.

H.1.1 The SIF design architecture meets the requirements.

H.1.2 The device(s) materials of construction are compatible with the process being measured.

H.1.3 Safety instrumented function speed of response is adequate.

H.1.4 Sensor settings and accuracy will give a reliable safety instrumented function.

H.1.5 Effect of partial operation has been considered.

H.1.6 The need for start-up or shutdown overrides (or bypasses, interlocks or forces) has been considered.

H.1.7 The effect of any start-up or shutdown overrides (or bypasses, interlocks or forces) has been considered.

H.1.8 The operation of the safety instrumented function at start-up, abnormal plant conditions, low plant rates and shutdown has been considered.

H.1.9 Potential common modes between the demand and the safety instrumented function have been investigated.

H.1.10 Where redundancy or diversity is used in a multi-channel safety instrumented function, then common mode failures between the channels have been considered.

H.1.11 The effect of power, instrument air or similar failures, or partial failure, has been considered.

H.1.12 Any maintenance activities, in addition to proof testing, have been considered to ensure that the required availability is achieved (for example calibration of analysers or cleaning of gas detectors).

H.1.13 The proof test procedure specifies a full test of the safety instrumented function, it can be carried out safely with the facilities provided and is clear, concise, unambiguous, defines the recorded responses and checks that the safety instrumented function is put back on-line after testing.

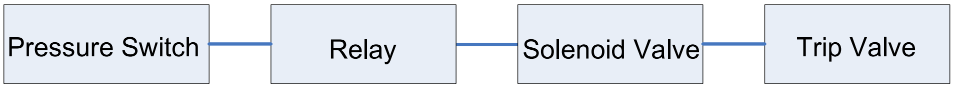
H.1.14 The effects of testing and repairs to the safety instrumented function should be considered with respect to the time that the safety function is unavailable, and the potential for introducing errors.

H.1.15 Any important assumptions in the design have been documented and checked.

H.1.16 Where defeats (or overrides, bypasses or forces) or trip settings are required to be changed for different plant operating conditions, consideration has been given to the effect of these changes and the necessary safeguards have been incorporated into the design.

Attachment I: Worked Examples

I.1 Simple, single channel safety function



Use the following generic failure rates

Component		λ_D
Pressure Switch	1 in 15 years	0.067
Trip Relay	1 in 300 years	0.0033
Solenoid Valve	1 in 30 years	0.033
Trip Valve	1 in 30 years	0.033
	TOTAL	**0.136**

PFDavg = ½ $\Sigma\lambda_D$ * T

λ_D is the dangerous failure rate of the component
T is the proof test period in years (must have consistent units with failure rate).

For a proof test period of 1 year (T = 1)

PFDavg = ½ * 0.136 * 1 = 0.068 = SIL 1

For a proof test period of 6 months (T = 0.5)

PFDavg = ½ * 0.136 * 0.5 = 0.034 = SIL 1

I.2 Example from Layer of Protection Analysis (LOPA) in IVL EHS-406

I.2.1 Safety Instrumented System (SIS) function is defined as 'Bottoms pressure PT-2617 or Overhead pressure PT-2604 will trip 8 # Steam HV-2631A/B to 1st IC4 Recycle Column Reboilers E-F5-009A/B.

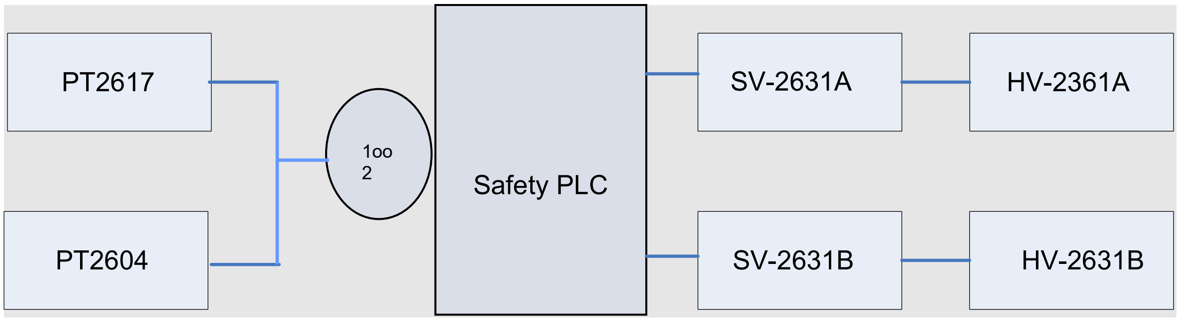
I.2.2 Target PFDavg = 0.0048, we will calculate the test interval required to achieve this PFDavg.

I.2.3 This description implies the following architecture;

I.2.3.1 1oo2 voting on the two pressure sensors (PT-2617 or PT-2604).

I.2.3.2 No information on the logic solver, for this example assume a safety Programmable Logic Controllers (PLC).

I.2.3.3 Both steam valves (HV-2631A and HV-2631B) must shut. Assume trip valves and solenoid valves.



I.2.4 The following failure data is taken from example ranges of dangerous failure rates for field equipment using the SIS-Tech SIL Solver tool as published in Guidelines for the Safe and Reliable Instrumented Protective Functions by CCPS.

Component			λ_D
Pressure switch	1 in 45 years	Generic data	0.022
Safety PLC	1 in 10,000 years	Certified for SIL 2 applications, configured with certified tool in accordance with supplied safety manual, failure data from manufacturer's certificate. Safe Failure Fraction (SFF) is given as 90%	0.0001
Solenoid Valve	1 in 60 years	Generic data	0.0167
Trip Valve	1 in 60 years	Generic data	0.0167

I.2.5 For the input channels in a 1oo2 voting, with identical instruments, λDU = 0.022. For this example, a value for β has been taken as 0.10 (10%).

PFD_{avg_input} = 1/3 [λDU2 x T2] + β[½ x λDU x T]

PFD_{avg_input} = $1/3(0.022^2 \times T^2) + 0.1(½ \times 0.022\ T) = 0.00016\ T^2 + 0.0011\ T$

I.2.6 For the logic solver (LS), λDU = 0.0001

PFD_{avg_LS} = ½ x 0.0001 T = 0.00005 T

I.2.7 For the output channel (Solenoid Valve + Trip Valve), both must close, so consider the valves in series

PFD_{avg}_output = ½ x λ_{DU} x T

PFD_{avg_output} = ½ x (0.0167 + 0.0167 + 0.0167 + 0.0167)T = 0.0334 T

I.2.8 For the total safety function, the PFDavg is given by:-

PFD_{avg_total} = PFDavg_input + PFDavg_LS + PFDavg_output

PFDavg_total = 0.00016 T2 + 0.0011 T + 0.00005 T + 0.0334 T

= 0.00016 T2 + 0.03455 T

For T = 1 month (1/12),

PFDavg_total = 0.00289

which meets the target of 0.0048, however hardware fault tolerance and Mean Time to Repair (MTTR) should also be considered.

I.2.9 The input channels meet the hardware fault tolerance (HFT) requirements for SIL 2 (HFT = 1) because the 1oo2 voting will tolerate a single hardware failure.

I.2.10 The logic solver meets the hardware fault tolerance requirements for SIL 2 with SFF of 90% and certified for use up to SIL 2.

I.2.11 The final elements DO NOT meet the hardware fault tolerance requirements for SIL 2 (HFT = 1). They may be used for this safety function if the requirements of IEC 61511 part 1 section 11.4.4 are met, this will generally rely upon the facility having a record of good performance of the device and the failure modes are well known. This decision should be made by a Responsible Instrument Engineer.

I.2.12 The contribution of MTTR to the PFD calculation can be estimated as follows.

I.2.12.1 A proof test or repair takes 2 hours to complete and is conducted 12 times per year. The time the safety function is unavailable is given by:

2 * 12 / 8760 = 0.0027

I.2.13 The total PFDavg can now be given as

0.00289 + 0.0027 = 0.0056

Which does not meet the target PFDavg

Upon inspection, the two valves dominate the calculations. In reality, the use of a control valve or second trip valve would be used to provide a second means of process isolation to each Recycle Column Reboiler. The control valve would have to be configured with a solenoid valve to control the instrument air to the control valve actuator. An alternate method is to utilise a high performance trip valve, with possible diagnostics that may detect some of the potential failure modes by methods such as automated partial stoking of the valve. Such equipment and methods should be assessed by a competent Instrument Engineer.

Attachment J: Testing Activities

J.1 A proof test method, procedure or check list shall be created to demonstrate that the Safety Instrumented Function (SIF) operates correctly.

J.2 The proof test shall ensure that all elements of the safety instrumented function are tested; sensor, logic solver and final element, although different elements may have differing proof test periods.

J.3 The proof test shall be performed on the equipment ‘as found’.

J.4 The proof test method shall include step-by-step instructions on performing the test including:

J.4.1 Any necessary constraints to be in place before the test may be executed.

J.4.2 Any necessary inspection, cleaning or maintenance activities to be done after the ‘as found’ test.

J.4.3 Verification that trip set points and values, measurement tolerances are in accordance with the Safety Requirements Specification (SRS).

J.4.4 Validation that the field sensor and associated instrument process tie points and tie lines are free and clear so that the equipment is operable.

J.5 Proof test records shall be retained for the life of the process.

J.6 If a proof test fails, the failure shall be recorded on the proof test record sheet, appropriate measures are to be taken for operation to continue, and the performance of the SIF is to be evaluated for possible design changes.

J.7 Safety instrumented systems designed and installed to National Codes (for example Gas Burner Management systems) shall be tested and inspected in line with the National Codes.

J.8 Actual demands on the safety instrumented function may be used in place of a proof test if sufficient feedback on the performance of the components that make up the safety instrumented function is available (for example valve limit switches, transmitter trends and flow rates). The actions required to use information from a demand shall be specified in a procedure and the results shall be recorded.

J.9 Additional guidance on testing methods may be found in the ISA-TR84.00.03 (Ref 7.13) document for Automation Asset Integrity of Safety Instrumented Systems.

Attachment K: Maintenance and Modifications

K.1 A maintenance program shall be established for preventative maintenance, repair and proof testing of the Safety Instrumented Function SIF and related alarms.

K.2 The maintenance programme shall schedule proof testing of the safety instrumented function based upon the calculated proof test period required to meet the SIL of the SIF.

K.3 Faults detected during maintenance activities shall be recorded as specified by the proof test method, repaired and retested before the SIF is put back into service.

Note: When a SIF is found to be in a degraded state, the event shall be recorded as a near miss process safety event and the appropriate action shall be taken. This may be an immediate repair or the implementation of a bypass/override until a repair can be made.

K.4 Maintenance activities, proof testing and repairs shall be performed by competent persons trained and experienced in the technologies used and the methods used for testing. Approved proof test procedures shall exist for each SIF and they shall be followed for testing.

K.5 Repairs to SIF devices shall be addressed within the Mean Time To Repair (MTTR) timing requirements set in the SIF Safety Requirement Specification (SRS) documentation.

K.6 Management reports shall be generated as required, at least annually, produced detailing the status of the proof testing schedule, highlighting any overdue tests and SIFs not in service, such as those bypassed or overridden, while awaiting repair.

K.7 Any modifications required to the SIF shall be performed according to the Management of Change Standard, IVL EHS-204. This includes modifications, bypasses, and overrides.

Attachment L: Reasons for Safety Instrumented Function Reviews

L.1 When changes to the process or when modification requirements are identified during a PHA/LOPA revalidation, which may have an impact on the Safety Instrumented Function (SIF), occur after the SIF installation.

L.2 When multiple actual demands on a safety instrumented function occur, the SIF shall be reviewed and appropriate actions taken to either reduce the demands to the level assumed in the Safety Requirement Specification (SRS) document or change the SRS design to add the extra risk reduction required due to the higher demand rate.

L.2.1 The PFDavg calculation for the SIFs is typically based on low demand mode. The low demand mode equations are no longer valid when the demand exceeds once per year and a more rigorous set of equations must be used to determine the hazard rate.

L.2.2 When a SIF activates, the activation shall be subject to an incident investigation (IVL EHS-106). One of the required outcomes from the investigation is the determination and documentation of whether there has been an actual demand or a spurious failure of a trip system component.

L.2.3 NOTE: Following a SIF activation, other than those resultant from proof testing activities, the process shall NOT be restarted until the cause of the operation has been determined and it is safe to restart.

L.3 When maintenance and proof test records indicate failures. These records shall be assessed to verify that the failure rates used for PFDavg calculations are still appropriate. Actions shall be defined to improve equipment reliability; otherwise, the PFDavg shall be recalculated.

L.4 When new information shows that the achieved PFDavg no longer meets the target PFDavg, then changes to the instrumentation, architecture or proof test period are required. These changes shall be performed according to the Management of Change Standard, IVL EHS-204.

L.5 When improved instrument failure rates result in the achieved PFDavg exceeding the target PFDavg, then opportunities to extend the proof test period may be considered. A suitable body of operating evidence is required to give a degree of confidence in the improved instrument failure rates. Any changes to the proof test period shall be performed according to the Management of Change Standard, IVL EHS-204.

L.6 When requested by the Site Manager following a process related incident, excessive demands, high rates of instrument failures, or changes in technical standards or regulatory requirements.

Attachment M: Example Safety Requirement Specification Form

See IVL EHSF-409-01