

DEP SPECIFICATION

INSTRUMENTED PROTECTIVE FUNCTIONS (IPF)

DEP 32.80.10.10-Gen.

February 2011
(DEP Circular 72/11 has been incorporated)
ECCN EAR99

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2011 Shell Group of companies

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, published or transmitted, in any form or by any means, without the prior written permission of the copyright owner or Shell Global Solutions International BV.

This document contains information that is classified as EAR99 and, as a consequence, can neither be exported nor re-exported to any country which is under an embargo of the U.S. government pursuant to Part 746 of the Export Administration Regulations (15 C.F.R. Parts 746) nor can be made available to any national of such country. In addition, the information in this document cannot be exported nor re-exported to an end-user or for an end-use that is prohibited by Part 744 of the Export Administration Regulations (15 C.F.R. Parts 744).

PREFACE

DEP (Design and Engineering Practice) publications reflect the views, at the time of publication, of Shell Global Solutions International B.V. (Shell GSI) and, in some cases, of other Shell Companies.

These views are based on the experience acquired during involvement with the design, construction, operation and maintenance of processing units and facilities. Where deemed appropriate DEPs are based on, or reference international, regional, national and industry standards.

The objective is to set the recommended standard for good design and engineering practice to be applied by Shell companies in oil and gas production, oil refining, gas handling, gasification, chemical processing, or any other such facility, and thereby to help achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to Shell companies for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual Operating Units to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs, they shall be solely responsible for such use, including the quality of their work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will typically expect them to follow those design and engineering practices that will achieve at least the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal.

The right to obtain and to use DEPs is restricted, and is typically granted by Shell GSI (and in some cases by other Shell Companies) under a Service Agreement or a License Agreement. This right is granted primarily to Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or another Shell Company. The use of DEPs by these Operating Units is subject in all respects to the terms and conditions of the relevant Service Agreement.
- 2) Other parties who are authorised to use DEPs subject to appropriate contractual arrangements (whether as part of a Service Agreement or otherwise).
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, Shell GSI disclaims any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof, even if it is wholly or partly caused by negligence on the part of Shell GSI or other Shell Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Company, or companies affiliated to these companies, that may issue DEPs or advise or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of Shell GSI, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of Shell GSI. The copyright of DEPs vests in Shell Group of companies. Users shall arrange for DEPs to be held in safe custody and Shell GSI may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in Shell GSI.

TABLE OF CONTENTS

1.	INTRODUCTION	5
1.1	SCOPE.....	5
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	5
1.3	DEFINITIONS	5
1.4	CROSS-REFERENCES	12
1.5	SUMMARY OF MAIN CHANGES.....	12
1.6	COMMENTS ON THIS DEP	17
1.7	DUAL UNITS.....	17
2.	COMPLIANCE WITH INTERNATIONAL/LOCAL STANDARDS.....	18
3.	IPF MANAGEMENT PLANNING	19
3.1	COMPLIANCE TO INTERNATIONAL STANDARD	19
4.	RISK ANALYSIS AND ALLOCATION OF PROTECTION LAYERS	20
4.1	PROCESS HAZARD AND RISK ASSESSMENT (SIL ASSESSMENT)	20
4.2	ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS.....	21
4.3	IMPLEMENTATION	23
5.	IPF REQUIREMENTS SPECIFICATION	24
5.1	COMPLIANCE TO INTERNATIONAL STANDARD	24
6.	DESIGN - HARDWARE.....	25
6.1	IPF REQUIREMENT SPECIFICATION	25
6.2	GENERAL DESIGN REQUIREMENTS.....	25
6.3	PROCEDURES/DOCUMENTATION.....	26
6.4	IPF OWNER DURING DETAILED DESIGN.....	27
6.5	PFD/ λ_{DU} CALCULATIONS.....	28
6.6	FAULT TOLERANCE.....	31
6.7	IMPLEMENTATION OF IPFS.....	33
7.	DESIGN - APPLICATION SOFTWARE.....	55
7.1	SOFTWARE CLASSIFICATION	55
7.2	APPLICATION SOFTWARE REQUIREMENT SPECIFICATION	55
7.3	APPLICATION SOFTWARE DESIGN AND CONFIGURATION.....	56
7.4	HUMAN-MACHINE INTERFACE	58
7.5	ALARM SIGNAL HANDLING.....	58
7.6	RESETTING	59
7.7	MAINTENANCE OVERRIDES.....	59
7.8	OPERATIONAL OVERRIDES	62
7.9	START-UP PERMISSIVES.....	62
7.10	IPS DATA CAPTURE	62
8	OTHER INSTRUMENTED PROTECTION LAYERS - HSSE CRITICAL INSTRUMENTS	65
8.1	CLASSIFICATION OF HSSE CRITICAL INSTRUMENTATION	65
8.2	IMPLEMENTATION REQUIREMENTS.....	65
9.	INSTALLATION, COMMISSIONING AND VALIDATION	67
9.1	INSTALLATION AND COMMISSIONING.....	67
9.2	VALIDATION.....	68
10.	OPERATION AND MAINTENANCE	73
10.1	COMPLIANCE TO INTERNATIONAL STANDARDS.....	73
10.2	PROJECT RESPONSIBILITIES FOR OPERATE AND MAINTAIN	73
11.	MODIFICATION.....	75
11.1	COMPLIANCE TO INTERNATIONAL STANDARDS.....	75
11.2	RISK ANALYSIS	75
11.3	DESIGN AND DEVELOPMENT	75
11.4	INSTALLATION, COMMISSIONING AND VALIDATION	75
12.	DECOMMISSIONING	76

12.1	GENERAL REQUIREMENTS.....	76
12.2	RISK ANALYSIS	76
12.3	DESIGN AND DEVELOPMENT	76
12.4	INSTALLATION, COMMISSIONING AND VALIDATION	76
13.	VERIFICATION	77
13.1	LEVEL OF INDEPENDENCE	77
13.2	VERIFICATION PLAN	77
13.3	REPORTING.....	79
14.	REFERENCES	80

APPENDICES

APPENDIX 1	HIGH INTEGRITY PRESSURE PROTECTION SYSTEMS.....	81
------------	---	----

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements to comply with IEC 61511-1, Clause 6, which states “To conform to this International Standard, it shall be shown that each of the requirements outlined in Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has(have) been met.” This DEP covers the IPF Life Cycle management of IPFs as it pertains to projects. It does not cover all the aspects of operation and maintenance of IPFs, just requirements and deliverables related to projects.

This DEP is intended for use for both new projects and existing installations. For existing installations, the objective is not to design IPFs but rather to confirm the suitability of the existing IPF implementations and to bring the required documentation up to a minimum standard. An added benefit of applying this DEP to existing installations is the optimisation of maintenance and inspection efforts.

This DEP applies to all automated instrument protective functions greater than or equal to SIL 1.

This DEP contains mandatory requirements to mitigate process safety risks in accordance with Design Engineering Manual DEM 1 – Application of Technical Standards.

This is a revision of the DEP of the same number dated January 2010; see (1.5) regarding the changes.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them. Any authorised access to DEPs does not for that reason constitute an authorization to any documents, data or information to which the DEPs may refer.

This DEP is intended for use in facilities related to oil and gas production, gas handling, oil refining, chemical processing, gasification, distribution and supply/marketing. This DEP may also be applied in other similar facilities.

When DEPs are applied, a Management of Change (MOC) process should be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements could be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable with regards to the safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for it. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The capitalised term **SHALL [PS]** indicates a process safety requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

The following definitions have been used in this DEP. Where IEC 61511 uses different terminology, these terms are also provided for reference.

Term	Definition
Architecture	Arrangement of hardware and/or software elements in a system, for example: 1) arrangement of instrumented protective system (IPS) subsystems; 2) internal structure of an IPS subsystem; 3) arrangement of software programs.
Availability	Fraction of time that a system or plant is able to perform its designated service.
Basic Process Control System (BPCS)	The system that responds to input signals from the process and generates output signals to maintain operation of the process in a desired state. The system does not perform functions assessed as SIL 1 or higher.
Beta Factor	The number of Common Mode Failures (of fault tolerant Sensors or Final Elements), expressed as a fraction of all possible Failures.
Constraints	The process parameter value at which a hazard or concern arises. This could be a relief valve setting, an IPF trip setting, an equipment design limit, a catalyst temperature limit, the pH at which corrosion accelerates, the temperature at which coke formation in heater tubes accelerates, etc.
Continuous mode	Mode of the IPF whereby in the event of a dangerous failure of the IPF a potential hazard will occur without further failure unless action is taken to prevent it. NOTE: In demand mode applications where the demand rate is more frequent than once per year, the hazard rate will not be higher than the dangerous failure rate of the IPF. In such a case, it will normally be appropriate to use the continuous mode criteria.
Common Mode Failure	A Failure having the potential to affect all duplicated components in a fault tolerant configuration by virtue of their common or shared characteristics.
Demand mode	Mode of the IPF whereby a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the IPF a potential hazard only occurs in the event of a failure in the process or the BPCS.
Dangerous Failure	A Failure that has the potential to place the IPF in a state in which it will fail to perform its function. Dangerous Failures are usually only revealed when the system has to perform a certain action or through testing. Formerly known as unrevealed failure.
Dangerous Failure Rate	The number of Dangerous Failures per unit time.
Dangerous Fault Tolerance	A configuration in which plant integrity is not jeopardised by the Dangerous Failure of a single IPF component. Formerly known as unrevealed failure robustness. In IEC 61508 and IEC 61511 Dangerous Fault Tolerance is referred to as Fault Tolerance. De-energized-to-trip (DTT) / Normally Energized - IPF circuits where the

Term	Definition
	outputs and devices are energized under normal operation. Removal of the source of power (e.g., electricity or air) will cause a trip action.
Demand	A process or equipment condition or event which requires an Instrumented Protective Function to take action to prevent a Hazardous Situation.
Demand Rate	The frequency at which a Demand occurs, i.e. the number of Demands per unit time.
Diagnostic Coverage Factor	The number of Dangerous Failures that diagnostic features are capable of detecting, expressed as a fraction of all possible dangerous failures. NOTE: Diagnostic features may only be recognised as such if they can trip the process to a safe state or maintain safety by different means.
DCS Trip to Manual Function (DTTM)	Non-IPF function initiated by the IPF interlock that causes one or more DCS controllers to change mode from automatic to manual and to drive their outputs to a predetermined position. Normally the function is used to match the controller output to the position of a control valve tripped by an IPF solenoid.
De-energized-to-trip (DTT) / Normally Energized	IPF circuits in which the outputs and devices are energized under normal operation. Removal of power (e.g., electricity or air) causes a trip action.
Energized-to-trip (ETT) / Normally De-Energized	IPF circuits in which the outputs and devices are de-energized under normal operation. Application of power (e.g., electricity or air) causes a trip action
External risk reduction facilities	Measures to reduce or mitigate the risks, which are separate and distinct from the IPF. Examples include a drain system, fire wall, bund (dike).
Failure (also fault)	An abnormal condition that may cause a reduction or loss of capability of the IPF to perform its intended function.
Failure Mode Effects Analysis (FMEA)	A qualitative reliability analysis identifying failure modes of components and the associated impact on functionality. See IEC 60812.
Fail Safe	A concept that defines the failure direction of a component or system as a result of specific malfunctions. That failure direction is towards a safer or less hazardous condition.
Fault avoidance	Use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle of the instrumented protection system.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults.
Final Element	A device, or combination of devices, that manipulate a process variable or attract the attention of the operator to achieve risk reduction. The Final Element includes output cards or output relays, solenoid valves and cabling. Examples are valves, switchgear (rotating equipment stop circuits) and alarms.

Term	Definition
Hardwired signal	Single signal between the switching device (on-off) or transmitting device (analog) that is carried by a dedicated set of wires. This excludes signals communicated serially using protocols such as HART, Foundation FieldBus, ModBus, etc.
Hazard or Hazardous Situation	A situation with the potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.
Hazard Rate	The frequency at which Hazardous Situations occur per unit time. In Demand Mode: Hazard Rate = Demand rate x Probability of Failure on Demand.
Instrumented Protective Function (IPF)	A function comprising one or more sensors, a Logic Solver and one or more Final Elements whose purpose is to prevent or mitigate hazardous situations and that have SIL 1, SIL 2, SIL 3 or SIL 4. An IPF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event. In IEC 61508 and IEC 61511 an IPF is referred to as a Safety Instrumented Function (SIF).
Instrumented Protective System (IPS)	The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment. In IEC 61508 and IEC 61511 an IPS is referred to as a 'Logic Solver'.
IPF Requirements Specification (IPF-RS)	A document describing the detailed functional and technical requirements of IPFs. The IPF Requirements Specification is an input to the detailed design of IPFs. In IEC 61508 and IEC 61511 the IPF Requirements Specification is referred to as the Safety Requirements Specification (SRS).
Logic Solver	The portion of an Instrumented Protective Function that performs the application logic function. The Logic Solver excludes trip amplifiers, input cards and output cards. Examples are electromechanical relays, solid-state/magnetic-core logic and the Central Processing Unit (CPU) section of programmable electronic systems.
Mission time	The time interval between maintenance shutdowns.
Mitigation	The action of making a consequence less severe or relieving consequences.
Mode of operation	Way in which an instrumented protective function operates
MooN	Instrumented protective function, or part thereof, made up of "N" independent channels, which are so connected that "M" channels are sufficient to perform the safety function.
Necessary risk reduction	Risk reduction required to ensure that the risk is reduced to a tolerable level.
Permissive	The result of a check on whether or not a combination of conditions is healthy, to allow the Logic Solver to proceed with the next step in a sequence.
Probability of Failure on Demand	The probability (dimensionless) of the Instrumented Protective Function failing to respond to a Demand. Because the PFD changes over time, this DEP assumes the PFD to be the average PFD over the mission time.

Term	Definition
Process Safety Time	The period of time in which the process can be operated without protection and with a Demand present without entering a dangerous condition. The Process Safety Time determines the dynamic response requirements of the IPF.
Proof Test	A test carried out on IPF components against an approved procedure to confirm that all requirements of the IPF are met.
Proof Test Coverage Factor	The number of Dangerous Failures detected by the Proof Test expressed as a fraction of all possible dangerous failures.
Prior use	When a documented assessment has shown that there is appropriate evidence, based upon the previous use of the component, that the component is suitable for use in an instrumented protective function.
Risk Assessment Matrix (RAM)	A tool used to assess the Consequences and Risks of Hazards to HSSE. The results are referred to as a RAM Severity rating and a RAM Risk rating. Whenever this DEP refers to RAM it is to the Shell HSSE RAM, not the SIL Decision Matrix.
Redundancy	Use of multiple elements or systems to perform the same function; redundancy can be implemented by means of identical elements (identical redundancy) or by diverse elements (diverse redundancy). Redundancy can be implemented as Safe Fault Tolerant or Dangerous Fault Tolerant or a combination of the two.
Risk	The frequency at which a Hazardous Situation occurs multiplied by the consequence of the Hazardous Situation.
Safe Failure	A Failure whose occurrence does not have the potential to place an IPF in a dangerous state. Formerly known as revealed failure.
Safe-failure Rate	The number of Safe Failures per unit time.
Safe-failure Fraction	The fraction of all Failures that drive the sub-system (e.g. Sensor or Final Element) to the safe state. $SFF = \frac{\lambda_{safe} + (\lambda_{dangerous} \times DCF)}{\lambda_{safe} + \lambda_{dangerous}}$ where: SFF is the safe-failure fraction λ_{safe} is the safe-failure rate (year⁻¹); $\lambda_{dangerous}$ is the dangerous failure rate (year⁻¹); DCF is the diagnostic coverage factor. For this formula it is assumed that the diagnostic test interval is small compared to the mean time between dangerous failures.
Safe Fault Tolerance	A configuration in which plant availability is not jeopardised by the safe failure of a single IPF component. Formerly known as Revealed Failure Robustness.

Term	Definition
Safety Integrity Level (SIL)	Dangerous failure class 1, 2, 3 or 4, derived from the consequences of failure on demand and the Demand Rate. Formerly known as IPF Class. The definition in IEC 61511: discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions (IPF in this DEP) to be allocated to the safety instrumented systems (trip systems). Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.
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). [IEC 61511]. In summary, an SIS is a collection of IPFs (including sensors and final elements) that together protect a process unit or major piece of equipment.
Sensor	A device, or combination of devices, that indicates whether a process or equipment item is operating outside the operating envelope. The sensor typically includes input cards and input relays. Examples are manual switches, position switches and measurement systems (including process connections, sensors, transmitters, cabling, trip amplifiers or input cards etc.).
SIL Decision Matrix	Plot of virtual demand rate and consequence; H&S, Environment, and Economic Loss on a grid. Virtual demand rate plotted without IPF barrier. The grid contains the ALARP SIL requirement based on the risk, virtual demand rate and consequence.
Tolerable risk	Risk which is accepted in the given context based upon current corporate HSE philosophy. The risk in this area can be tolerated but one should demonstrate that the risk is reduced to level that is ALARP, i.e. further risk reduction would be impractical and involve a disproportioned effort and capital.
Trip	An Instrumented Protective Function action to bring the Final Element to a safe state.
UZ Group (IPF Group)	A group of IPFs dedicated to a specific piece of equipment (e.g. a compressor, a furnace); a functional grouping of interlocks.
Virtual Demand Rate	The demand rate on the IPF when all barriers before and after the IPF are "virtually" placed before the IPF. Those before the IPF reduce the real demand rate on the IPF and those after the IPF virtually reduce the demand rate on the IPF. The reduced demand rate (which real and virtual demand reductions) sets the SIL requirement of the IPF.

1.3.3 Abbreviations

1oo2	1 out of 2 voting (Fail Safe)
2oo2	2 out of 2 voting (Fault Tolerant)
2oo3	2 out of 3 voting (Fail Safe and Fault Tolerant)
AIPS	Asset Integrity Process Safety
AK	Anforderungsklasse (requirement class)
ALARP	As Low As Reasonably Practicable
BDEP	Basic Design and Engineering Package
BOD	Basis of Design
BPCS	Basic Process Control System
C&E	Cause and Effect Diagram (Shutdown Matrix)

CAPEX	Capital expenditure
CEM	Cause and Effect Matrix
CCF	Common Cause Failures
CPU	Central processing unit
DCF	Diagnostic Coverage Factor
DCS	Distributed control system
DSR	Desktop Safety Review (also referred to as 'Technical Desk HSE review')
DTTM	DCS trip to manual.
DIN	Deutsche Industrie Norm (German industrial standard)
EPC	Engineering, Procurement, Construction project phase
ESD	Emergency shutdown
EWS	Engineering Work Station
FE	Final Element
FGS	Fire gas and smoke detection and protection system
FLD	Functional logic diagram
FMEA	Failure mode effects analysis
FPL	Fixed program language
FVL	Full variable language
H&S	Health and Safety
HAZOP	Hazard and operability study
HEMP	Hazards and Effect Management Process
HSE	Health, safety and environment
HR	Hazard Rate
HSSE	Health, Safety, Security, and Environment
I/O	Input/output
IEC	International Electrotechnical Commission
IPF	Instrumented protective function
IPL	Independent Protection Layer
IPF-RS	IPF Requirements Specification
IPS	Instrumented protective system
LOPA	Layers of Protection Analysis
LS	Logic Solver
MOC	Management of Change
MoonN	"M" components out of "N" total components
MOS	Maintenance override switch
MVC	Measurement validation and comparison
NDE	Normally de-energised
NE	Normally energised
NTP	Network Time Protocol
OOS	Operational override switch
OPEX	Operational expenditure
PAS	Process Automation System
PCN	Process Control Network
PE	Programmable Electronic
PEFS	Process engineering flow scheme (also known as P&ID - Piping and Instrument Diagram)
PFD	Probability of failure on demand
PFS	Process Flow Scheme
PLC	Programmable logic controller
QRA	Quantified Risk Assessment
RS	Requirement Specification

SER	Sequence of events recorder
SFC	Safe-Failure cluster
SFF	Safe-Failure Fraction
SIF	Safety Instrumented Function (IEC 61508/61511 equivalent of IPF)
SIL	Safety integrity level
SIS	Safety Instrumented System
SOV	Solenoid valve
SRS	Safety Requirement Specification
TSO	Tight shut off
TÜV	Technischer Überwachungsverein (German body, translates to Technical Inspection Agency).
NOTE: Throughout this DEP, reference to TÜV means either TÜV Bayern or TÜV Rheinland.	
UPS	Uninterruptible Power Supply
USD	United States Dollars
UZ	Tag numbering system to indicate IPF group
VDU	Visual display unit

1.4 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets. Other documents referenced by this DEP are listed in (14).

1.5 SUMMARY OF MAIN CHANGES

This DEP is a revision of the DEP of the same number dated January 2010. The following are the main, non-editorial changes.

This revision combines 3 IPF DEPs, listed as follows, into a single DEP:

- DEP 32.80.10.10-Gen., Classification and implementation of instrumented protective functions. January 2010
- DEP 32.80.10.12-Gen, Management of instrumented protective functions. October 2001 (now retired)
- DEP 32.80.10.30-Gen., Instrumented protective systems, December 2008 (now retired)

Rationale for combining IPF DEPs:

- Provides better alignment with IEC 61511-1
- Reduces risk of conflicts between multiple standards
- Eliminates redundancy

Old DEP #	Old section	New section	Change
All	All	All	Split in Specification and Informative DEP.
All	All	All	Combined 3 IPF DEPs; DEP 32.80.10.10-Gen. (Classification and Implementation of Instrumented Protective Functions), DEP 32.80.10.12-Gen. (Management of Instrumented Protective Functions), and DEP 32.80.10.30-Gen. (Instrumented Protective Systems), into single IPF DEP. New DEP is DEP 32.80.10.10-Gen., Instrumented Protective Functions (IPF).
All	All	N/A	Deleted reference to “SILa”

Old DEP #	Old section	New section	Change
32.80.10.12	All	N/A	Each chapter had a section on Objective, Scope and Timing, Inputs, and Success Factors. Deleted these sections because didn't have actionable requirements or measurable success factors.
32.80.10.12	3	3	Deleted content around IPF Management Planning, replaced with requirement to follow IEC 61511 Section 6.2. In the Information DEP list typical procedures/documents used to comply with international standard.
32.80.10.10	3.1	N/A	Removed the Shell Bow-tie figure
32.80.10.10	3.3.5	N/A	Removed all references to Primary, Collateral, Half-, and Synergetic IPFs
32.80.10.10	3.3.6	N/A	Removed section on IPFs and Alarms
32.80.10.10	3.3.7.2	4.2.1	Removed references to D0...D43 and Table 1 (Demand Rate Categories) from the Demand Rate Section
32.80.10.10	3.3.7.3.2	N/A	Removed Figure 6 on multiple LOPAs for same scenario.
32.80.10.10	3.3.7.1	4.2.1	Updated SIL Decision Matrices and removed references to safety, environmental and economics consequence categories
32.80.10.10	3.3.7.9	N/A	Remove notes from section on Tight Shutoff
32.80.10.10	3.3.7.11	N/A	Remove note from section on SIL 4
32.80.10.12	6	5	Deleted content around IPF Requirement Specification, replaced with requirement to follow IEC 61511 Section 10.3. In the Information DEP list typical procedures/documents used to comply with international standard.
32.80.10.10	4.1	6.2	Added more definition around IPF response time requirements.
N/A	N/A	6.3	Added requirement in design phase to create specific procedures/documentation and required content. In most cases the documentation is required to satisfy IEC 61511 requirements for the Operation and Maintenance part of IPF Life Cycle Management.
32.80.10.12	7.5	6.4	Added responsibility requirement of IPF owner during design.
32.80.10.10	4.2.3.2	6.5.3.2	Added requirement around use of maintenance history to derive failure rates.
32.80.10.10	4.2.3.2	6.5.3.3	Added clarification on required response to detected fault.
32.80.10.10	4.2.3.2	6.5.3.3	Added requirement for transmitter to be within range during normal operation to take credit for sensor diagnostic test.
32.80.10.10	4.3.1	6.6.1	Added requirements from IEC 61511-1 to take credit for the prior use modifier.

Old DEP #	Old section	New section	Change
32.80.10.10	4.3.1	6.6.1	Added fault tolerance requirement from IEC 61511-1 for PE IPS.
32.80.10.10	4.4.1	6.7.1	Deleted exception that allowed using human as one leg of an IPF.
32.80.10.10	4.4.3	6.7.3	Deleted reference to SIL 4 design, as this DEP does not cover design of SIL 4 IPFs.
32.80.10.10	4.4.3	6.7.3.1	Deleted exception that permitted use of control valve as an IPF valve in a DFT configuration, even if control valve failure can cause hazard.
32.80.10.10	4.4.3	6.7.3.2	Deleted exception that permitted sharing of BPCS/IPF sensor in a 1oo2 configuration.
32.80.10.10	4.4.3	6.7.3.2	Limited sharing of BPCS/IPF transmitter using a middle of 3 select algorithm to SIL 2, changed from SIL 3.
32.80.10.10	4.4.3	6.7.3.2	Allow use of signal splitter on input, least preferred option with restrictions, when sharing DCS/IPS via a middle of 3 select algorithm.
32.80.10.10	4.4.4.1	6.7.4.1	Allow use of car seals in addition to valve locks for administrative controls.
32.80.10.10	4.4.4.1	6.7.4.1	Allow use of process connected tuning fork type level point detectors in certain applications up to SIL 2.
32.80.10.10	4.4.4.1	6.7.4.1	Deleted statement allowing use of digital communication for analogue transmitters.
32.80.10.10	4.4.4.1	6.7.4.1	Changed requirement to connect analogue transmitters directly to IPF input from a shall to a should.
32.80.10.10	4.4.4.1	6.7.4.1	In addition to write protect jumpers, allow use of password write protect in the transmitter with restrictions.
32.80.10.10	4.4.4.11	6.7.4.2	Exclude storage tank levels from trip setting range requirement.
32.80.10.10	4.4.4.3	6.7.4.3	Removed requirement to install filter on transmitters. Added requirement not to install filters on transmitters with fast process safety times.
32.80.10.10	4.4.4.5	6.7.4.5	Allow transmitter to fail away from trip with auto MOS.
32.80.10.10	4.4.4.6	6.7.4.6	Changed some of the voting requirements when sharing HH and LL trip, removed 1oo1 option,
32.80.10.10	4.4.4.9	6.7.4.9	Removed requirement for level displacers to have vessel connections at 80 and 100% of control range.
32.80.10.10	4.4.4.9	6.7.4.9	Removed the restriction for small density variations in order to make the control and IPF level transmitters the same range.
32.80.10.10	4.4.4.10	6.7.4.10	Added restriction on sharing of IPF TE and indicating only TE in a common thermowell.

Old DEP #	Old section	New section	Change
N/A		6.7.5.3.1	Added requirement around safety related communications over long distances, such as pipe line applications.
32.80.10.30	2.3.4	N/A	Deleted section, covered in 6.7.5.3.1 or DACA DEP.
32.80.10.30	2.3.5	N/A	Deleted section, covered in 6.7.5.3.1 or DACA DEP.
32.80.10.30	2.4	6.7.5.5	Changed IPS response time requirement.
32.80.10.30	2.5.1	6.7.5.6.1	Deleted requirement around using proven software/hardware, changed to products shall be technically qualified to the satisfaction of the Principal and shall be sourced from Manufacturers acceptable to the Principal.
32.80.10.30	2.5.1	6.7.5.6.1	Deleted requirement to install major equipment in separate IPS, changed to separate I/O.
32.80.10.30	2.5.7	6.7.5.6.6	Deleted requirement to trip after 72 hours run time with IPS fault, change to action based on requirements to maintain SIL.
32.80.10.30	2.5.7	6.7.5.6.6	Changed requirement to wire fault tolerant sensors and final elements to separate IPS I/O cards from a shall to a should.
32.80.10.30	2.7.1	6.7.5.7.1	Deleted requirement to base spare parts on FMEA analysis using theoretical failure rates from ML HDBK 217.
32.80.10.30	2.7.2	6.7.5.7.2	Deleted requirement for IPS to support RTD, TC and pulse analogue inputs.
32.80.10.30	2.7.3	6.7.5.7.3	Deleted requirement for IPF Class VI trip functions to be connected to a watchdog or secondary power disconnection device.
32.80.10.30	3.1	6.5.5.8.1	Changed most of the requirements around cabinet construction from shall to should, didn't list all. Most suppliers have different good practices, not safety related issue.
32.80.10.30	3.1	6.5.5.8.1	Changed the requirement to install common cabinet trouble alarm to individual diagnostic DCS alarms.
32.80.10.30	3.2	6.5.5.8.2	Changed most of the requirements around internal wiring in IPS cabinets from shall to should, didn't list separately. Most suppliers have different good practices, not safety related issue.
32.80.10.10	4.4.6.1	6.7.6.1	Excluded turbine trip and throttle valves from type hydraulic valves not suitable for higher SILs.
32.80.10.10	4.4.6.4	6.7.6.4.1	Added requirement for identifying valves that require leak test and setting leak test requirement.
32.80.10.10	4.5	N/A	Deleted section on Fire, Gas, and Smoke Detection. Covered in F&G DEP.
N/A	N/A	7.1	Added requirement around classification and use of application software, per IEC 61511-1.

Old DEP #	Old section	New section	Change
N/A	N/A	7.2	Added section setting requirements around Application Software Specification, per IEC 61511-1
N/A	N/A	7.3	Added section on application software design; including use/management of standard function blocks, general requirements (per IEC 61511-1), and software auditing.
N/A	N/A	7.4.1	Added more details on IPF HMI requirements.
32.80.10.30	2.9	7.5	Deleted requirements around F&G alarm handling, covered in F&G DEP.
32.80.10.30	2.9	7.5	Added requirement for first up alarm be reset by a trip reset, not first up reset.
32.80.10.30	2.9	7.5	Deleted requirement for first up alarm to flash.
32.80.10.10	4.4.12	7.5	Added recommendation to require DCS reset when filed reset is required.
32.80.10.10	4.4.13.1	7.7.1	Changed requirement for repeated MOS alarm from a shall to a should.
32.80.10.10	4.4.13.3	7.7.3	Added requirement not to over-ride outputs.
32.80.10.10	4.4.13.3	7.7.3	Added requirement to use 2 soft DCS outputs to activate MOS.
32.80.10.10	4.4.13.3	7.7.3	Allow mounting of MOS enable switch on IPS cabinet.
32.80.10.10	4.4.13	7.8	Requirement to install automated operation over-ride when feasible.
32.80.10.10	4.4.13	7.8	Requirement to have step by step procedures for use of manual operational over-ride.
32.80.10.30	2.10	7.10	Changed name from SER to Post Event analysis to focus on functionality as opposed to hardware.
32.80.10.30	2.10.1	7.10	Deleted the following SER requirements: - Capable of storing 100,000 time stamped events - Store 100 events in IPS on power failure - SER tag shall be 12 characters, service description 30 characters - The time stamp shall be equal to the IPS clock speed
32.80.10.30	2.10.1	7.10	Changed many SER requirements from shall to should as most were not related to safety or an ability to meet safety requirement.
32.80.10.30	2.10.1	7.10	If it can be shown to satisfy functional requirements, allow use of DCS alarm/logging functionality
32.80.10.30	2.10.1	7.10	Added requirement to evaluate rotating equipment post event analysis needs.
N/A	N/A	8	Added section 8, Other Instrumented Protection Layers – HSSE Critical Instruments

Old DEP #	Old section	New section	Change
32.80.10.30	6.1	9.0	Deleted following requirement to split IPS FAT into 2 phases, 1 at IPF supplier and 2 nd at PAS supplier.
32.80.10.30	6.2	9.0	Deleted section on hardware FAT, covered in DEP 63.10.08.11-Gen.
32.80.10.30	6.3	9.0	Change 25% I/O check to 100%.
32.80.10.12	10	9	Complete re-write of validation section to align with recent large project experience and IEC 61511-1
32.80.10.12	11	10.2	Complete re-write of operation and maintenance section to align with IEC 61511-1
32.80.10.12	12	11	Added requirement for IPF Modification to follow all requirements of IEC 61511-1 Section 17.2.
32.80.10.10	N/A	13	Added new section on requirements for Verification.
32.80.10.10	N/A	Appendix A	Added new appendix on requirements for HIPPS systems.

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the Administrator at standards@shell.com, using the DEP Feedback Form. The DEP Feedback Form can be found on the main page of "DEPs on the Web", available through the Global Technical Standards web portal <http://www.shell.com/standards> and on the main page of the DEPs DVD-ROM.

1.7 DUAL UNITS

**Amended per
Circular 72/11**

Dual units have been incorporated throughout this DEP.

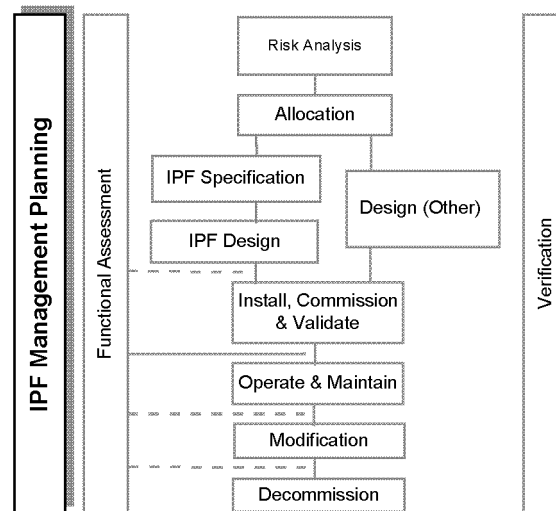
This DEP contains both the International System (SI) units, as well as the corresponding US Customary (USC) units, which are given following the SI units in brackets. When agreed by the Principal, the indicated USC values/units may be used.

2. COMPLIANCE WITH INTERNATIONAL/LOCAL STANDARDS

Surface Safety Systems for all fixed offshore structures, floating production, storage and off-take systems SHALL [PS] also comply with DEP 37.01.10.10-Gen. Section 2.

SIL 4 IPFs SHALL [PS] be designed and implemented in full compliance with IEC 61508, SIL 4 designs are not covered by this DEP.

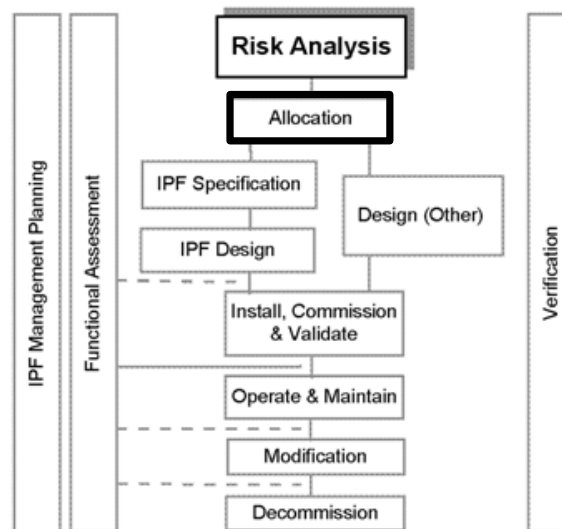
3. IPF MANAGEMENT PLANNING



3.1 COMPLIANCE TO INTERNATIONAL STANDARD

IPF life cycle management SHALL [PS] comply with requirements of IEC 61511-1 Section 6.2.

4. RISK ANALYSIS AND ALLOCATION OF PROTECTION LAYERS



4.1 PROCESS HAZARD AND RISK ASSESSMENT (SIL ASSESSMENT)

4.1.1 Objectives

The hazard and risk assessment shall achieve the following objectives:

- determine the hazardous events which could affect the process and associated equipment;
- determine the sequence of events leading to the hazardous event;
- determine the process consequences and likelihoods associated with the hazardous event;
- determine the safety functions required to achieve the necessary risk reduction and if any of the safety functions are instrumented

4.1.2 Requirements

A hazard and risk assessment, SIL assessment, SHALL [PS] be carried out on hazardous processes and its associated equipment. It shall result in

- 1) a description of each identified hazardous event and the factors that contribute to it;
- 2) a description of the consequences and likelihood of the event;
- 3) consideration of conditions such as normal operation, start-up, shutdown, etc.;
- 4) the determination of requirements for additional risk reduction necessary to achieve the required safety;
- 5) a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- 6) a detailed description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates, and
- 7) allocation of the safety functions to layers of protection taking account of potential reduction in effective protection due to common cause failure between the different layers.

4.2 ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS

4.2.1 Objectives

Allocation shall achieve the following objectives:

- allocate protection layers to prevent a hazard;
- determine the required IPFs;
- determine, for each IPF, the associated safety integrity level. The decision matrixes in Tables 1, 2, and 3 shall be used to determine the SIL.

Table 1 SIL decision matrix for personal safety risks

Inverse Virtual Demand rate (years per demand) on IPF	Health/Safety (Requisite SILs)						Notes for demand rate selection
<1	-	SIL 1 ©	SIL 2 ©	SIL 3 ©	SIL 4 ©	X	Continuous mode
1-10	-	SIL 1	SIL 2	SIL 3 ©	SIL 4	SIL 4	Difficult/complex controls; happens between shutdowns Unspared machinery (pumps, compressors)
10-100	-	-	SIL 1	SIL 2	SIL 3	SIL 3	Control loop failure with operator intervention as a safeguard Spared machinery (pumps, compressors)
100-1000	-	-	-	SIL 1	SIL 2	SIL 2	Single effective barrier (omit IPF or operator intervention in the count)
>1000	-	-	-	-	SIL 1	SIL 1	Two or more effective barriers present (omit IPF or operator intervention in the count)
Personnel Safety	No injury or health effect	Slight injury or health effect	Minor injury or health effect	Major injury or health effect	PDT or 1-3 casualties	> 3 casualties	All independent layers of protection, conditional modifiers, exposure, possibilities for aversion etc. will need to be separately considered, documented and taken into account in LOPA for severity 3 and higher.
Severity (Numeric)	0	1	2	3	4	5	

Table 2 SIL decision matrix for environmental risk

Inverse Virtual Demand rate (years per demand) on IPF	Environmental Risks (Requisite SILs)						Notes for demand rate selection
<1	-	-	SIL 1 ©	SIL 2 ©	SIL 3 ©	X	Continuous mode
1-10	-	-	SIL 1	SIL 2	SIL 3	SIL 4	Difficult/complex controls; happens between shutdowns Unspared machinery (pumps, compressors)
10-100	-	-	-	SIL 1	SIL 2	SIL 3	Control loop failure with operator intervention as a safeguard Spared machinery (pumps, compressors)
100-1000	-	-	-	-	SIL 1	SIL 2	Single effective barrier (omit IPF or operator intervention in the count)
>1000	-	-	-	-	-	SIL 1	Two or more effective barriers present (omit IPF or operator intervention in the count)
Environment	No effect	Slight effect	Minor effect	Moderate effect	Major effect	Massive effect	
Severity (Numeric)	0	1	2	3	4	5	

Table 3 SIL decision matrix for production losses and equipment damage risks

Inverse Virtual Demand rate (years per demand) on IPF	Production Losses/Equipment Damage Risks ("Tolerable" and "Broadly Acceptable" SILs)						Notes for demand rate selection
<1	- / -	- / -	- / -	- / SIL 1 ©	- / SIL 2 ©	SIL 1 / SIL 3 ©	Continuous mode
1-10	- / -	- / -	- / -	- / SIL 1	- / SIL 2	SIL 1 / SIL 3	Difficult/complex controls, happens between shutdowns Unspared machinery (pumps, compressors)
10-100	- / -	- / -	- / -	- / -	- / SIL 1	- / SIL 2	Control loop failure with operator intervention as a safeguard Spared machinery (pumps, compressors)
100-1000	- / -	- / -	- / -	- / -	- / -	- / SIL 1	Single effective barrier (omit IPF or operator intervention in the count)
>1000	- / -	- / -	- / -	- / -	- / -	- / -	Two or more effective barriers present (omit IPF or operator intervention in the count)
Economic	< 1K\$	1-10K\$	10-100K\$	100K-1M\$	1-10M\$	>10M\$	
Severity (Numeric)	0	1	2	3	4	5	

4.2.2 Requirements of the allocation process

- The allocation process shall result in identification of all protective layers, including IPF, that prevent a potential H&S, environment or economic consequence
- For ultimate over-pressure protection by IPF - excluding reactive processes - refer to Appendix A.
- SIL SHALL [PS] be determined by plotting the frequency (Inverse Virtual Demand Rate) and consequence on Tables 1, 2, and 3 with all the allocated protection layers in place except for the potential IPF.
- Layers of Protection Analysis, LOPA, shall be used for potential H&S, environment or economic consequence of severity 3 or greater.
- Valid protection layers shall have all of the following 3 attributes:
 - Independent from initiating event, cause of hazard or threat, and other protection layers
 - Effectiveness of action, high probability that action prevents or mitigates the hazard
 - Dependability, How reliable is the protective layer; e.g. operator has time to recognize and take corrective action. The protective layer shall be properly maintained, tested or inspected to be considered reliable.

4.2.3 Identification of HSSE critical instruments

The following instruments identified through the allocation process shall be classified as HSSE critical instruments:

- Instruments that form an IPF that prevents or mitigates a severity 4 or 5 H&S or environment consequence on Tables 1 or 2
- Any non-IPF instrumented protection layer, alarm or control, that "is part of a HEMP barrier or recovery measure" prevents or mitigates a severity 4 or 5 H&S or environment consequence on Tables 1 or 2 (8.0).

4.2.4 Other functions of the risk assessment team

For each risk reduction requirement greater than or equal to SIL 1, the risk assessment team shall:

Define the process safety time

Define IPF success criteria for sensor subsystems that detect the hazard and final element subsystems that prevent/mitigate the hazard when activated

Identify valves that have a leakage requirement and define maximum allowable leak rate to prevent hazard

4.3 IMPLEMENTATION

4.3.1 Timing

The IPF classification and implementation methodology shall be applied during conceptual design for those IPFs that have the potential to significantly impact project decisions, not all IPFs are analysed in this phase.

The IPF study shall be conducted after the DSR or HAZOP study to minimise re-work and ensure that the process design has sufficiently matured before the study commences.

During detailed engineering all potential IPFs including those forming part of packaged units shall be reviewed. Potential IPFs already analysed during the conceptual design shall be revisited to ensure their validity, for instance in case the process design has changed.

4.3.2 Classification team

As a minimum the team shall consist of representatives from:

- process technology
- operations
- competent facilitator

Other disciplines shall be consulted when the IPFs of a particular engineering specialty are classified, e.g. rotating equipment specialists should be consulted for compressor IPFs.

Process safety specialist should be consulted for all severity 4 and 5 H&S or environment consequence.

The process technology and operations team members should be the same as those who participated in the DSR /HAZOP review.

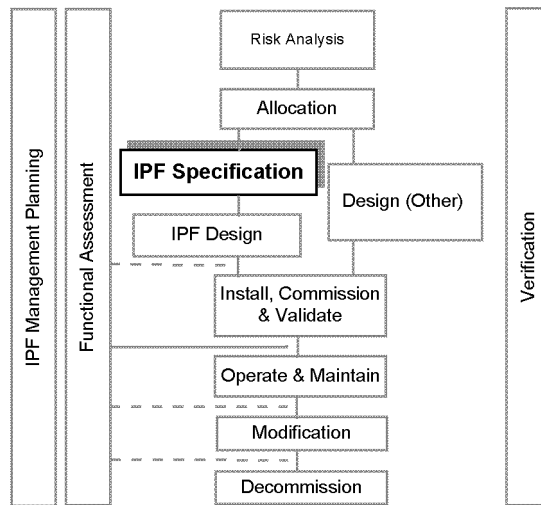
The facilitator shall be an expert in the use of the classification methodology and tools for the assessment. The facilitator shall be certified, with certification approved by Principal.

4.3.3 Templates, process/equipment IPF DEPs, and previous analysis

The Principal should maintain a catalogue of IPF analysis for typical process equipment conducted by senior level facilitator, process technologist, operations, and equipment engineers.

If the Principal has an IPF standard for a particular process or type of equipment, it shall be used as the starting point to conduct the IPF SIL assessment.

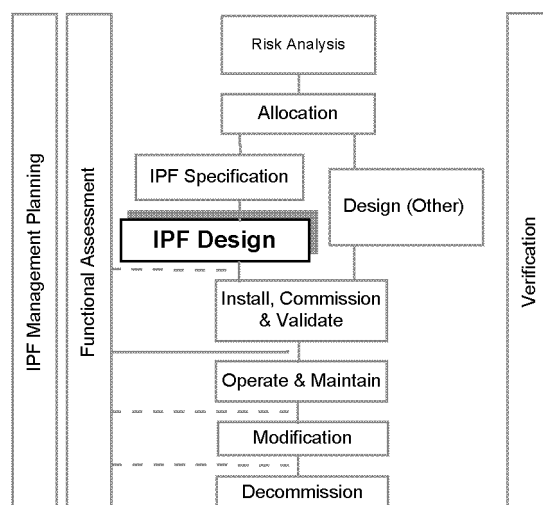
5. IPF REQUIREMENTS SPECIFICATION



5.1 COMPLIANCE TO INTERNATIONAL STANDARD

IPF requirement specification documents SHALL [PS] be prepared that satisfy requirements of IEC 61511-1 Section 10.3.

6. DESIGN - HARDWARE



6.1 IPF REQUIREMENT SPECIFICATION

Design and procurement SHALL [PS] be in accordance with the IPF Requirement Specification.

6.2 GENERAL DESIGN REQUIREMENTS

Each IPF, $\geq$ SIL 1, SHALL [PS] comply with the following 3 requirements:

1. SIL PFD Requirement, IPF satisfies minimum requirements for the probability of failure on demand (PFD: IPF in demand mode) or dangerous undetected failure rate (λ_{du} : IPF in continuous mode). See (6.5).
2. Fault Tolerance Requirement, Hardware architecture, (sensors, logic solver, and final elements) satisfies minimum fault tolerance. See (6.6). The relationship between the SIL of the IPF, the required PFD and the required minimum dangerous fault tolerance is given in Table 4 Relation between SIL, required PFD and base fault tolerance.

Table 4 Relation between SIL, required PFD and base fault tolerance

Safety Integrity Level (SIL)	Required PFD (demand mode)	Requière $\lambda_{du} [y^{-1}]$ * (Continuous mode)	Base dangerous fault tolerance
<SIL 1	No requirements	No requirements	0
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 8.76 \cdot 10^{-3}$ to $< 8.76 \cdot 10^{-2}$	0
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 8.76 \cdot 10^{-4}$ to $< 8.76 \cdot 10^{-3}$	1
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 8.76 \cdot 10^{-5}$ to $< 8.76 \cdot 10^{-4}$	2
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 8.76 \cdot 10^{-6}$ to $< 8.76 \cdot 10^{-5}$	3
X	Intolerable	Intolerable	

* The target IPF undetected dangerous failure rates (λ_{du}) are derived from IEC 61511-1 where the frequency is expressed as failures per hour.

3. Performance Requirements:

a) IPF Response Time < Process Safety Time

IPF Responses Time =

(Sensor Response Time (Including Filters) + IPS Response Time (input to output) + Programmed Time Delays + (Final Element Response Time + Margin))

If final element is a valve, should add a margin to required valve response time, 10-30%, because the valve stroke time can degrade over time.