

DEP SPECIFICATION

INSTRUMENTED PROTECTIVE FUNCTIONS (IPF)

DEP 32.80.10.10-Gen.

February 2014

ECCN EAR99

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2014 Shell Group of companies
All rights reserved. No part of this document 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. Part 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. Part 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 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	10
1.5	SUMMARY OF MAIN CHANGES	11
1.6	COMMENTS ON THIS DEP	12
1.7	DUAL UNITS.....	12
1.8	NON NORMATIVE TEXT (COMMENTARY).....	12
2.	COMPLIANCE WITH INTERNATIONAL/LOCAL STANDARDS.....	13
3.	IPF MANAGEMENT PLANNING	13
3.1	COMPLIANCE TO INTERNATIONAL STANDARD	13
4.	RISK ANALYSIS AND ALLOCATION OF PROTECTION LAYERS	14
4.1	PROCESS HAZARD AND RISK ASSESSMENT (SIL ASSESSMENT).....	14
4.2	ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS.....	15
4.3	IMPLEMENTATION	17
5.	IPF REQUIREMENTS SPECIFICATION	18
5.1	COMPLIANCE TO INTERNATIONAL STANDARD	18
6.	DESIGN - HARDWARE.....	19
6.1	IPF REQUIREMENT SPECIFICATION	19
6.2	GENERAL DESIGN REQUIREMENTS.....	19
6.3	PROCEDURES/DOCUMENTATION.....	20
6.4	IPF OWNER DURING DETAILED DESIGN	22
6.5	PFD/ λ_{DU} CALCULATIONS	22
6.6	FAULT TOLERANCE.....	26
6.7	IMPLEMENTATION OF IPFS.....	28
7.	DESIGN - APPLICATION SOFTWARE.....	49
7.1	SOFTWARE CLASSIFICATION.....	49
7.2	APPLICATION SOFTWARE REQUIREMENT SPECIFICATION	49
7.3	APPLICATION SOFTWARE DESIGN AND CONFIGURATION.....	50
7.4	HUMAN-MACHINE INTERFACE.....	52
7.5	ALARM SIGNAL HANDLING.....	53
7.6	RESETTING.....	53
7.7	MAINTENANCE OVERRIDES.....	54
7.8	OPERATIONAL OVERRIDES	55
7.9	START-UP PERMISSIVES.....	56
7.10	IPS DATA CAPTURE	56
8	OTHER INSTRUMENTED PROTECTION LAYERS – HSSE CRITICAL INSTRUMENTS.....	59
8.1	CLASSIFICATION OF HSSE CRITICAL INSTRUMENTATION	59
8.2	IMPLEMENTATION REQUIREMENTS.....	60
9	INSTALLATION, COMMISSIONING AND VALIDATION	61
9.1	INSTALLATION AND COMMISSIONING.....	61
9.2	VALIDATION.....	62
10.	OPERATION AND MAINTENANCE	67
10.1	COMPLIANCE TO INTERNATIONAL STANDARDS	67
10.2	PROJECT RESPONSIBILITIES FOR OPERATE AND MAINTAIN	67
11.	MODIFICATION.....	69
11.1	COMPLIANCE TO INTERNATIONAL STANDARDS	69
11.2	RISK ANALYSIS	69
11.3	DESIGN AND DEVELOPMENT	69
11.4	INSTALLATION, COMMISSIONING AND VALIDATION	69

12.	DECOMMISSIONING	70
12.1	GENERAL REQUIREMENTS.....	70
12.2	RISK ANALYSIS	70
12.3	DESIGN AND DEVELOPMENT	70
12.4	INSTALLATION, COMMISSIONING AND VALIDATION	70
13.	VERIFICATION.....	71
13.1	GENERAL	71
13.2	LEVEL OF INDEPENDENCE	71
13.3	VERIFICATION PLAN	71
13.4	REPORTING.....	73
14	REFERENCES	74

APPENDICES

APPENDIX 1	HIGH INTEGRITY PRESSURE PROTECTION SYSTEMS.....	75
-------------------	--	-----------

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements and gives recommendations for designing new instrumented protective functions (IPFs) and for confirming the suitability of existing IPFs.

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 IPFs 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 February 2011; 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 shall 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: arrangement of instrumented protective system (IPS) subsystems; internal structure of an IPS subsystem; arrangement of software programs.
Availability	Fraction of time that a system or plant is able to perform its designated service.
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 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.
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.

Term	Definition
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.
Failure (also fault)	An abnormal condition that may cause a reduction or loss of capability of the IPF to perform its intended function.
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 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.
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.
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.

Term	Definition
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.
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.
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	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 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.
Safety Integrity Level (SIL)	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 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 consequences (H&S, Environment, and Economic Loss) on a grid. The grid contains the (ALARP) SIL requirement.
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.

Term	Definition
Virtual Demand Rate	The demand rate on the IPF when all barriers before and after the IPF are “virtually” placed before the IPF.

1.3.3 Abbreviations

Term	Definition
1oo2	1 out of 2 voting (Fail Dangerous Tolerant)
2oo2	2 out of 2 voting (Fail Spurious Tolerant)
2oo3	2 out of 3 voting (Fail Dangerous and Spurious Tolerant)
ALARP	As Low As Reasonably Practicable
BPCS	Basic Process Control System
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.
ESD	Emergency shutdown
EWS	Engineering Work Station
FE	Final Element
FGS	Fire gas and smoke detection and protection system
FMEA	Failure mode effects analysis
FPL	Fixed program language
H&S	Health and Safety
HAZOP	Hazard and operability study
HEMP	Hazards and Effect Management Process
HSE	Health, safety and environment
HSSE	Health, Safety, Security, and Environment
I/O	Input/output
IEC	International Electrotechnical Commission
IPF	Instrumented protective function
IPF-RS	IPF Requirements Specification
IPS	Instrumented protective system
LOPA	Layers of Protection Analysis
LS	Logic Solver
MOC	Management of Change
MOS	Maintenance override switch
MVC	Measurement validation and comparison
NDE	Normally de-energised

Term	Definition
NE	Normally energised
NTP	Network Time Protocol
OOS	Operational override switch
PAS	Process Automation System (consisting of BPCS, IPS and FGS)
PE	Programmable Electronic
PFD	Probability of failure on demand
PLC	Programmable logic controller
RS	Requirement Specification
SER	Sequence of events recorder
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
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
UZ	Tag numbering system to indicate IPF group

1.4 CROSS-REFERENCES

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

1.5 SUMMARY OF MAIN CHANGES

This DEP is full a revision of the DEP of the same number dated February 2011. The following are the main, non-editorial changes.

Section/Clause	Change
1.3.2	Removed "manual switches" from the generic definition of "sensors".
4.2.1	Minor modifications to Table 1, SIL decision matrix for personal safety risks
4.3.2	Added requirement that "The membership of the assessment team shall include at least one senior competent person not involved in the project design team."
6.6.1	Removed DACA references for IPF field devices connected to the PCD.
6.7.3.2	Removed sentence "Modbus and OPC communications shall not be used for sharing a sensor for IPF and BPCS".
6.7.4.1	Changed wording to "The adjustment to configurable transmitter parameters shall be either be write-protected to prevent inadvertent modifications of program parameters or protected by passwords which are part of the maintenance management system and are auditable to comply with DACA requirements."
6.7.4.5.	Changed Table 10 to reflect the AUTO MOS function with Transmitter failure failing towards tripping point and if Auto MOS is allowed in the function a maximum of 1 hour before enabling the function and trip action will occur (if not repaired or a MOS is in place)
6.7.4.6	Change the minimum sensor architecture requirements in Tables 11, 12, 13 to be in line with risk analyses
6.7.4.11	Changed wording to Normal practice is that the manual trip function is hardwired to the IPS. Documentation of the rationale for not installing the manual trip function, independent of the IPS which satisfies requirements of IEC-61511-1, should be noted in the IPF narrative that the manual trip function will not be independent of the logic solver but is deemed to provide sufficient risk reduction as the predominant failure mode is human error.
6.7.5.2	Reworded "IPS to IPS communication (if "black channel") shall be recognized in the certification of the IPSs."
6.7.5.3.1	Remove section 6.7.5.3.1 (PCD security); it will be covered in a PCD DEP
6.7.5.6.3	Removed Section 6.7.5.6.3 System connectivity); it will be covered in a PCD DEP
6.7.5.6.5.2	Changed wording to "The IPS may be a node on the Control Bus and shall use PAS vendor proprietary peer-to-peer communication. As an alternative to this proprietary communication, the IPS shall communicate via individual, galvanically isolated point-to-point links with the PAS using a secure communications protocol. Event time stamps should be preserved.
6.7.5.9.1	Cabinet requirements to be less prescriptive.
6.7.5.10	Removed requirement that the power supply to the input and output circuits be floating (non-earthed).

Section/Clause	Change
6.7.6.1	Removed limitations on hydraulically actuated valves and electrically operated valves in IPF service. Power failure rate to be included in PFD calculation for electrically operated valves.
8.8.2	Eliminated 6 year maximum interval between IPF testing and made maximum interval subject to the specified time from the safety analysis.
9.2.1	Relaxed requirement to fully test IPS with DCS at FAT, if a virtual DCS configuration is used, until the SAT.
A1.7	Removed the sentence "minimum effective diameter shall be 25 mm" from the section as technically limiting and less prescriptive.

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be submitted to the Administrator using one of the following options:

Shell DEPs Online (Users with access to Shell DEPs Online)	Enter the Shell DEPs Online system at https://www.shelldeps.com Select a DEP and then go to the details screen for that DEP. Click on the "Give feedback" link, fill in the online form and submit.
DEP Feedback System (Users with access to Shell Wide Web)	Enter comments directly in the DEP Feedback System which is accessible from the Technical Standards Portal http://www.shell.com/standards . Select "Submit DEP Feedback", fill in the online form and submit.
DEP Standard Form (Other users)	Use DEP Standard Form 00.00.05.80-Gen. to record feedback and email the form to the Administrator at standards@shell.com .

Feedback that has been registered in the DEP Feedback System by using one of the above options will be reviewed by the DEP Custodian for potential improvements to the DEP.

1.7 DUAL UNITS

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.

1.8 NON NORMATIVE TEXT (COMMENTARY)

Text shown in italic style in this DEP indicates text that is non-normative and is provided as explanation or background information only.

Non-normative text is normally indented slightly to the right of the relevant DEP clause.

2. COMPLIANCE WITH INTERNATIONAL/LOCAL STANDARDS

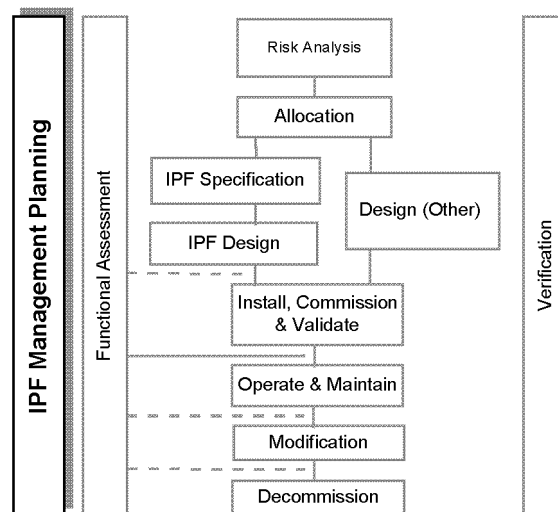
1. IPFs shall comply with IEC 61511-1, Clause 4.

Clause 4 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.”

2. The Life Cycle Management of IPFs, which includes analysis, design, installation and testing, and operation and maintenance of IPFs SHALL [PS] comply with IEC 61511-1, clauses 5 through 19.
3. Surface Safety Systems for all fixed offshore structures, floating production, storage and off-take systems shall also comply with DEP 37.01.10.10-Gen. Section 2.
4. SIL 4 IPFs shall be designed and implemented in full compliance with IEC 61508.

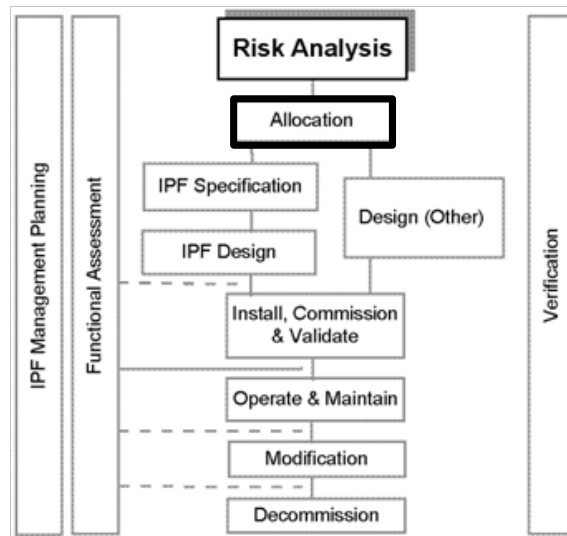
3. IPF MANAGEMENT PLANNING



3.1 COMPLIANCE TO INTERNATIONAL STANDARD

1. IPF life cycle management planning is a design requirement and SHALL [PS] comply with requirements of IEC 61511-1 Section 6.2. The IPF life cycle management plan is to be audited against IEC 61511-1 Section 6.2 before/ during the pre-startup safety review.

4. RISK ANALYSIS AND ALLOCATION OF PROTECTION LAYERS



4.1 PROCESS HAZARD AND RISK ASSESSMENT (SIL ASSESSMENT)

4.1.1 Objectives

1. The hazard and risk assessment shall achieve the following objectives:
 - a. determine the hazardous events which could affect the process and associated equipment;
 - b. determine the sequence of events leading to the hazardous event;
 - c. determine the process consequences and likelihoods associated with the hazardous event;
 - d. determine the safety functions required to achieve the necessary risk reduction and if any of the safety functions are instrumented

4.1.2 Requirements

1. A hazard and risk assessment, SIL assessment, SHALL [PS] be carried out on hazardous processes and its associated equipment and shall result in the following.
 - a. a description of each identified hazardous event and the factors that contribute to it;
 - b. a description of the consequences and likelihood of the event;
 - c. consideration of conditions such as normal operation, start-up, shutdown, etc.;
 - d. the determination of requirements for additional risk reduction necessary to achieve the required safety;
 - e. a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
 - f. a detailed description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates, and
 - g. 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

1. Allocation shall achieve the following objectives:
 - a. allocate protection layers to prevent a hazard;
 - b. determine the required IPFs;
 - c. 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

1. The allocation process shall result in identification of all protective layers, including IPF, that prevent a potential H&S, environment or economic consequence
2. For ultimate over-pressure protection by IPF, excluding reactive processes, refer to Appendix A.
3. 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.
4. Layers of Protection Analysis (LOPA) shall be used for potential H&S, environment or economic consequence of severity 3 or greater.
5. Valid protection layers shall have all of the following three attributes:
 - a. Independent from initiating event, cause of hazard or threat, and other protection layers
 - b. Effectiveness of action, action prevents or mitigates the hazard
 - c. Dependability, 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 (> 90% probability of success on demand).

4.2.3 Identification of HSSE critical instruments

1. The following instruments identified through the allocation process shall be classified as HSSE critical instruments:
 - a. Safety Critical Instrument is an Instrument that is used in a barrier (including IPF) that prevents or mitigates a RAM RED or YELLOW 5A and 5B on Tables 1 or 2.
 - b. Any non-IPF instrumented protection layer, alarm or control, that "is part of a HEMP barrier or recovery measure" and prevents or mitigates a severity 4 or 5 H&S or environment consequence on Tables 1 or 2. see (8.0).

4.2.4 Other functions of the risk assessment team

1. For each risk reduction requirement greater than or equal to SIL 1, the risk assessment team shall:
 - a. Define the process safety time

- b. Define IPF success criteria for sensor subsystems that detect the hazard and final element subsystems that prevent/mitigate the hazard when activated
- c. Identify valves that have a leakage requirement and define maximum allowable leak rate to prevent hazard

4.3 IMPLEMENTATION

4.3.1 Timing

1. 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.
2. 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.
3. 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.

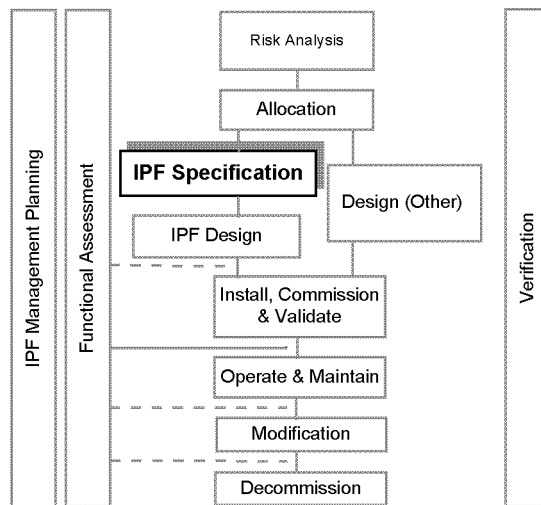
4.3.2 Classification team

1. As a minimum a classification team shall consist of representatives from:
 - a. process technology
 - b. operations
 - c. competent facilitator
 - d. technical safety
 - e. specialist from PACO is optional but recommended to be part of the review team
2. The classification team shall include at least one senior competent, independent person not involved in the project design team.
3. 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.
4. Process safety specialist should be consulted for all severity 4 and 5 H&S or environment consequence.
5. The process technology and operations team members should be the same as those who participated in the DSR /HAZOP review.
6. 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

1. The Principal should maintain a catalogue of IPF analysis for typical process equipment conducted by senior level facilitator, process technologist, operations, and equipment engineers.
2. 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.

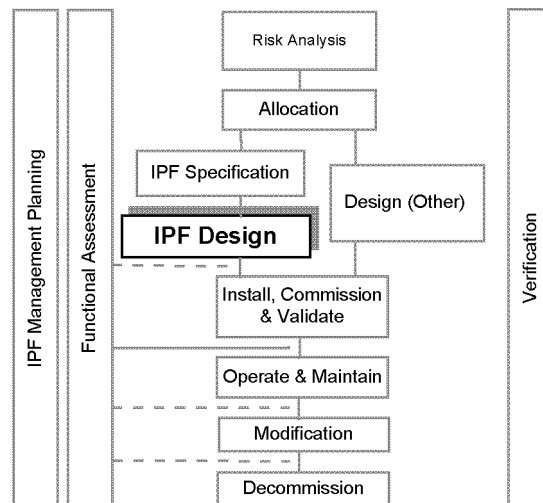
5. IPF REQUIREMENTS SPECIFICATION



5.1 COMPLIANCE TO INTERNATIONAL STANDARD

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

6. DESIGN - HARDWARE



6.1 IPF REQUIREMENT SPECIFICATION

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

6.2 GENERAL DESIGN REQUIREMENTS

1. Each IPF, $\geq$ SIL 1, SHALL [PS] comply with the following 3 requirements:
 - a. 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).
 - b. 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.

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

Safety Integrity Level (SIL)	Required PFD (demand mode)	Required λ_{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.			

c. Performance Requirements:

i. 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.

- ii. Moment of action. When establishing the moment the action shall be initiated, the process safety time and the accuracy of the sensor(s) shall be taken into account.
- iii. Final element leakage rate requirement, If the IPF final element is one or more valves, each valve shall comply with the leakage rate requirements, as applicable.

6.3 PROCEDURES/DOCUMENTATION

6.3.1 General

- 1. For Greenfield projects, the contractor shall produce the IPF life cycle procedures/documentation specified in (6.3.1-6.3.3) to satisfy IEC 61511 requirements. For brown field projects, the contractor shall integrate new procedures/documentation into the existing site document management system and identify any gaps in satisfying IEC 61511 documentation requirements.

6.3.2 Operate and maintain procedures:

- 1. IPF Site Management Procedure, The IPF Site Management Procedure shall include the following:
 - a. Identification of site owner(s) for the management of IPFs
 - b. Roles and Responsibilities, including competence and training requirements
 - c. IPF change control process, could be integrated into the site change control process
 - d. Requirements for performing routine test/inspection per the IPF SRS.
 - e. Requirements for testing after repairs or change (such as transmitter configuration change)
 - f. Requirements for monitoring/validating IPF performance including tracking of the following indicators:
 - i. IPF component failures, to assure components perform per design and identify bad actors. If statistically worse than assumed in the PFD calculation, then the design shall be updated based on actual failure rates.
 - ii. Demand rates, to assure IPF risk analysis is correct and identify bad actors
 - iii. Testing according to schedule
 - g. Requirements around management of obsolete equipment
 - h. Requirements around investigating IPF incidents; including failure on demands, testing failures, and nuisance (spurious) trips
 - i. Requirements for managing non-IPF instrument barriers (Safety Critical Instruments), this could be part of a separate procedure

- j. Requirements for operational response to abnormal situations, such as response to trips and requirements to respond IPF component failures
 - k. Requirement for managing of test deferrals, including approval authority
 - l. Requirements for operations to manage MOS and OOS including specification of maximum allowable time IPFs can be in over-ride (MOS or OOS) and subsequent required action should that time be exceeded.
 - m. Requirements for verification activities, including internal and external reviews and frequency of reviews
 - n. Requirements for maintaining IPF RS and operate and maintain documentation
 - o. Requirements for maintaining validation and verification records including:
 - i. project documentation such as FAT, Loop Test, SAT, and project verification audits
 - ii. run and maintain documentation such as test/inspection records, internal, and external audits.
 - p. Security requirements to prevent uncontrolled or inadvertent changes
 - q. Requirements for periodic revalidation of IPF Risk Analysis and Design
 - r. Requirements to repair IPF deficiencies identified through testing, diagnostics, or failure on demand in a timely manner, should be less than Mean Time to Repair Assumed in the PFD calculation.
2. IPF Mitigation Procedures, Each IPF sensor and final element shall have pre-approved step-by-step operating procedures to identify operating precautions including alternative means of providing controls/barriers required when an IPF is out of service (such as when the IPF is being overridden for testing or repairs).
3. Proof Test/Inspection Procedures,
- a. Proof test/inspection procedures shall be written to test each IPF component
 - b. Proof test/inspection procedures shall include pass/fail requirements per the IPF Requirement Specification; including the following:
 - i. Trip set point pass/fail criteria, dangerous and safe, for sensor elements and logic solver
 - ii. Valve stroke time (based on process safety time)
 - iii. Valve leak test requirements (if applicable).
 - iv. Correct logic action
 - c. In addition to above performance requirements, proof test/inspection procedures shall include the following:
 - i. Description of the tests and inspections performed
 - ii. Dates of the tests and inspections
 - iii. Name of the person(s) who performed the test and inspection
 - iv. Serial number or other unique identifier of the system tested (for example, loop number, tag number, equipment number, and/or SIF number);
 - v. Results of the tests and inspection (for example, "as-found" and "as-left" conditions).
 - vi. Validation of correct alarm and indication
 - d. Proof test procedures shall include method to verify test equipment is traceable to a national standard.

- 4 Time based maintenance/replacement, Time based maintenance and replacement of IPF components shall be identified to assure IPF component failure rates remain constant.

6.3.3 QA procedures

1. Project shall develop procedures per the QA plan as described in DEP 62.10.08.11-Gen. section 2; including FAT, Loop Testing/Inspection, and SAT procedures.

6.3.4 IPF safety requirement specification

See (5.1.)

6.4 IPF OWNER DURING DETAILED DESIGN

- 1 The Contractor shall appoint an 'IPF lead'.
 - a. The 'IPF lead' shall assume overall responsibility for the creation of the IPF SRS as well as assure the conceptualisation engineering, design, specification, procurement, installation testing, commissioning and documentation, MoC and hand-over of the SIS satisfy the IPF SRS.
 - b. The IPF lead shall be competent, i.e. shall have a Shell SIFpro Certification or be a TÜV Certified Functional Safety Expert.
 - c. The Principal shall approve the nomination of the IPF lead.
2. The Principal shall appoint an 'IPF owner' to verify all phases of the IPF life cycle comply with this DEP.

6.5 PFD/ λ_{DU} CALCULATIONS

6.5.1 General

1. The PFD of an IPF shall be calculated by the following methods:
 - a. IEC 61508 part 6 Annex B;
 - b. ISA TR 84.0.02 Parts 1, 2, 3 or 4;
2. PFD calculation shall take the minimum requirements as specified in the following Sections into account.

6.5.2 Assumptions

1. The probabilistic calculations SHALL [PS] take account of all failures that may occur during the Mission Time of the IPF. Early and late life failures that are likely to occur outside the mission time of an IPF do not need to be taken into account.
2. All the failure rates used in the calculation methodology shall be assumed to be constant over time. Failures that are expressed as failures per million operations and (operating) time based failures, shall be converted to failure rates constant over time. Testing does not change the failure rates.
3. For normally de-energised (NDE) output circuits the failure rate of cables and connections, power supply, instrument air supply, etc. shall be included in the dangerous failure rate of the final element. If the instrument air supply and/or the output circuit of NDE final elements is supervised, this shall be taken into account as diagnostics provided they comply with the requirements of (6.5.3.3).
4. For normally energised (NE) outputs, the entire output circuit including output card, wiring, and final elements shall be included in the safe failure rate.

6.5.3 Inputs into PFD/ λ_{du} calculations

6.5.3.1 Sensor, logic solver and final element architecture

1. The success criteria that form the basis of the PFD/ λ_{du} calculation SHALL [PS] reflect the IPF architecture.

6.5.3.2 Reliability data

1. Both dangerous and safe failure rates for the following components shall be taken into account by the PFD/ λ_{du} calculations
2. Data shall be obtained from the Principal's standard data set.
3. Data shall cover:
 - a. The sensor, excluding the IPS input.
 - b. The IPS input. For a PLC type IPS, this is the (robust) input card. For other IPSs this is the trip amplifier and the first relay, solid-state module or magnetic-core.
 - c. The Logic solver common parts excluding the IPS input and IPS output but including racks and power supply.
 - d. The IPS output. For a PLC type IPS, this is the (robust) output card. For other IPS this is the last relay or solid-state output module.
 - e. The final element, including interposing relays, solenoid valves etc. however excluding the IPS output.
4. The failure rates of the sensor and IPS input shall be added to give the total sensor failure rate because it is assumed that both the sensor and the IPS input are tested during the regular manual or automatic proof test. For similar reasons, the failure rates of the IPS output and final element shall be added to give the total final element failure rate.

6.5.3.3 Diagnostic coverage factor

1. The PFD/ λ_{du} calculations shall also take diagnostic coverage for the sensor or final element into account. The detection may be done by the instrument itself or by the IPS or by the DCS.
2. Diagnostic credit shall only be taken when the process is brought to the safe state if a fault is detected or if safety is maintained by different means, such as activating MOS, implementing high priority correction, and implementing mitigation procedure. The allowable coverage factor that may be assumed in the calculation of the PFD/ λ_{du} shall be established in accordance with Figure 1.
3. The diagnostic coverage factor shall be estimated by means of analysis techniques such as Failure Modes Effects Analysis (FMEA).
4. The claimed coverage for diagnostics carried out in the DCS shall be limited to 90 % because the maximum claimed risk reduction from a system that does not comply with IEC 61508 and IEC 61511 is a factor 10 (corresponding to 90% coverage).
5. For sensor diagnostics that are based on the comparison of two or more measurements (such as MVC), coverage may only be claimed if the comparison algorithm complies with all of the following requirements:
 - a. Validation comparison activates an alarm monitored by full time operations staff who are trained on required corrective action
 - b. The two transmitters are active, between 10-90% of max. calibrated range, under normal operating conditions.
 - c. The comparison algorithm is tuned so that any unacceptable deviation is detected. That is to say, an unacceptable deviation is detected when the