

PETRONAS TECHNICAL STANDARDS

DESIGN AND ENGINEERING PRACTICE

MANUAL

MANAGEMENT OF INSTRUMENTED PROTECTIVE FUNCTIONS

PTS 32.80.10.12
OCTOBER 2001



© 2010 PETROLIAM NASIONAL BERHAD (PETRONAS)

All rights reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the permission of the copyright owner



Documents

Document Sharing Hub

PREFACE

PETRONAS Technical Standards (PTS) publications reflect the views, at the time of publication, of PETRONAS OPU/Divisions.

They are based on the experience acquired during the involvement with the design, construction, operation and maintenance of processing units and facilities. Where appropriate they are based on, or reference is made to, national and international standards and codes of practice.

The objective is to set the recommended standard for good technical practice to be applied by PETRONAS' OPU/Divisions in oil and gas production facilities, refineries, gas processing plants, chemical plants, marketing facilities or any other such facility, and thereby to achieve maximum technical and economic benefit from standardisation.

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

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

The right to use PTS rests with three categories of users :

- 1) PETRONAS and its affiliates.
- 2) Other parties who are authorised to use PTS subject to appropriate contractual arrangements.
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) and 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, PETRONAS 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 PTS, combination of PTS or any part thereof. The benefit of this disclaimer shall inure in all respects to PETRONAS and/or any company affiliated to PETRONAS that may issue PTS or require the use of PTS.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, PTS shall not, without the prior written consent of PETRONAS, be disclosed by users to any company or person whomsoever and the PTS shall be used exclusively for the purpose 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 PETRONAS. The copyright of PTS vests in PETRONAS. Users shall arrange for PTS to be held in safe custody and PETRONAS may at any time require information satisfactory to PETRONAS in order to ascertain how users implement this requirement.

TABLE OF CONTENTS

1.	INTRODUCTION	6
1.1	SCOPE	6
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS.....	6
1.3	DEFINITIONS	6
1.4	ABBREVIATIONS	9
1.5	CROSS-REFERENCES	10
2.	GENERAL	11
2.1	IPF MANAGEMENT PHILOSOPHY	11
2.2	IEC STANDARDS	12
2.3	THE IPF LIFE-CYCLE MODEL.....	13
2.4	STRUCTURE OF THIS PTS.....	14
2.5	RELATIONSHIP WITH OTHER PROCESSES	17
3.	IPF MANAGEMENT PLANNING	19
3.1	OBJECTIVE	19
3.2	SCOPE AND TIMING.....	19
3.3	INPUTS.....	19
3.4	ACTIVITIES	19
3.5	CUSTODIANS AND CONTRIBUTORS	20
3.6	DELIVERABLES	20
3.7	SUCCESS FACTORS.....	20
4.	RISK ANALYSIS	22
4.1	OBJECTIVE	22
4.2	SCOPE AND TIMING.....	22
4.3	INPUTS.....	22
4.4	ACTIVITIES	23
4.5	CUSTODIANS AND CONTRIBUTORS	23
4.6	DELIVERABLES	23
4.7	SUCCESS FACTORS.....	23
5.	HSE REQUIREMENTS ALLOCATION	24
5.1	OBJECTIVE	24
5.2	SCOPE AND TIMING.....	24
5.3	INPUTS.....	24
5.4	ACTIVITIES	25
5.5	CUSTODIANS AND CONTRIBUTORS	26
5.6	DELIVERABLES	26
5.7	SUCCESS FACTORS.....	26
6.	IPF REQUIREMENTS SPECIFICATION	28
6.1	OBJECTIVE	28
6.2	SCOPE AND TIMING.....	28
6.3	INPUTS.....	28
6.4	ACTIVITIES	28
6.5	CUSTODIANS AND CONTRIBUTORS	29
6.6	DELIVERABLES	29
6.7	SUCCESS FACTORS.....	31
7.	DESIGN AND DEVELOPMENT - HARDWARE	32
7.1	OBJECTIVE	32
7.2	SCOPE AND TIMING.....	32
7.3	INPUTS.....	32
7.4	ACTIVITIES	32
7.5	CUSTODIANS AND CONTRIBUTORS	33
7.6	DELIVERABLES	33
7.7	SUCCESS FACTORS.....	33
8.	DESIGN AND DEVELOPMENT - APPLICATION SOFTWARE	35

8.1	OBJECTIVE	35
8.2	SCOPE AND TIMING.....	35
8.3	INPUTS.....	35
8.4	ACTIVITIES	35
8.5	CUSTODIANS AND CONTRIBUTORS	37
8.6	DELIVERABLES	37
8.7	SUCCESS FACTORS	37
9.	DESIGN AND DEVELOPMENT: OTHER RISK REDUCTION	38
9.1	OBJECTIVE	38
9.2	SCOPE AND TIMING.....	38
10.	INSTALLATION, COMMISSIONING AND VALIDATION	39
10.1	OBJECTIVE	39
10.2	SCOPE AND TIMING.....	39
10.3	INPUTS.....	39
10.4	ACTIVITIES	39
10.5	CUSTODIANS AND CONTRIBUTORS	41
10.6	DELIVERABLES	41
10.7	SUCCESS FACTORS	41
11.	OPERATION AND MAINTENANCE	42
11.1	OBJECTIVE	42
11.2	SCOPE AND TIMING.....	42
11.3	INPUTS.....	42
11.4	ACTIVITIES	42
11.5	CUSTODIANS AND CONTRIBUTORS	44
11.6	DELIVERABLES	45
11.7	SUCCESS FACTORS	45
12.	MODIFICATION	46
12.1	OBJECTIVE	46
12.2	SCOPE AND TIMING.....	46
12.3	INPUTS.....	46
12.4	ACTIVITIES	46
12.5	CUSTODIANS AND CONTRIBUTORS	47
12.6	DELIVERABLES	47
12.7	SUCCESS FACTORS	47
13.	DECOMMISSIONING	48
13.1	OBJECTIVE	48
13.2	SCOPE AND TIMING.....	48
13.3	INPUTS.....	48
13.4	ACTIVITIES	48
13.5	CUSTODIANS AND CONTRIBUTORS	49
13.6	DELIVERABLES	49
13.7	SUCCESS FACTORS	49
14.	FUNCTIONAL ASSESSMENT	50
14.1	OBJECTIVE	50
14.2	SCOPE AND TIMING.....	50
14.3	INPUTS.....	50
14.4	ACTIVITIES	50
14.5	CUSTODIANS AND CONTRIBUTORS	51
14.6	DELIVERABLES	51
14.7	SUCCESS FACTORS	51
15.	VERIFICATION	52
15.1	OBJECTIVE	52
15.2	SCOPE AND TIMING.....	52
15.3	INPUTS.....	52
15.4	ACTIVITIES	52
15.5	CUSTODIANS AND CONTRIBUTORS	53

15.6	DELIVERABLES	53
15.7	SUCCESS FACTORS	53
16.	REFERENCES	54

APPENDICES

APPENDIX 1	DOCUMENTATION.....	56
APPENDIX 2	WORKED EXAMPLE: IPF MANAGEMENT PLAN	59
APPENDIX 3	GENERAL GUIDELINES FOR PROOF TESTING	89
APPENDIX 4	FAILURE RATES AND FAILURE RATE COLLECTION.....	99
APPENDIX 5	IPF REQUIREMENTS SPECIFICATION FOR LARGE PROJECTS	104

1. INTRODUCTION

1.1 SCOPE

This new PTS specifies requirements and gives recommendations for the management of Instrumented Protective Functions (IPFs).

It aims to provide:

- a structured and practical approach to achieving and maintaining compliance with the relevant IEC standards;
- additional practical tools to continuously improve management of IPFs.

Much of the detailed technical information relating to the IPF classification methodology, IPF implementation rules and IPF calculations can be found in PTS 32.80.10.10

This PTS 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 PTS to existing installations is the optimisation of maintenance and inspection efforts.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by PETRONAS, the distribution of this PTS is confined to companies forming part of PETRONAS or managed by a Group company, and to Contractors and Manufacturers/Suppliers nominated by them.

This PTS is intended for use in oil refineries, chemical plants, gas plants, exploration and production facilities and supply/marketing installations.

If national and/or local regulations exist in which some of the requirements are more stringent than in this manual, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable as regards safety, economic and legal aspects. In all cases, the Contractor shall inform the Principal of any deviation from the requirements of this document 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 with the objective of obtaining agreement to follow this document 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 or maintenance of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier/Vendor** 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 its design and construction. The Principal will generally specify the technical requirements. 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 word **should** indicates a recommendation.

1.3.2 Specific definitions

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

Basic Process Control System

The system which 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 robust initiators or final elements), expressed as a fraction of all possible failures.

Common Mode Failure

A Failure having the potential to affect all duplicated components in a robust configuration by virtue of common or shared characteristics.

Dangerous Failure

A Failure which 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 Failure Robustness

IEC: 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.

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. Also known as frequency of demand.

Diagnostic Coverage Factor

The number of Dangerous Failures that diagnostic features are capable of detecting expressed as a fraction of all possible 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

An abnormal condition that may cause a reduction in, or loss of the 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.

Fault

See Failure.

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.

Hazard or Hazardous Situation

The potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

Initiator

IEC: Sensor

A device or combination of devices that indicates whether a process or equipment item is operating outside the operating envelope. The Initiator includes input cards and input

relays. Examples are manual switches, position switches and measurement systems (including process connections, sensors, transmitters, cabling, trip amplifiers, input cards, etc.).

Instrumented Protective Function (IPF)

IEC: Safety Instrumented Function (SIF)

A function comprising the initiator function, logic solver function and final element function for the purposes of early warning, prevention or mitigation of hazardous situations.

Instrumented Protective System (IPS)

IEC: Logic Solver

The electromechanical, electronic and/or programmable electronic logic solver component of the IPF, including the input and output cards.

IPF Management Plan

A documented management plan that demonstrates how the objective of each phase of the IPF life-cycle will be achieved in practice.

IPF Requirements Specification

IEC: Safety Requirements Specification

A document describing the detailed functional and technical requirements of IPFs. The IPF Requirements Specification is an input to the detailed design of IPFs.

Logic Solver

The portion of an IPF which 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.

Probability of Failure on Demand (PFD)

The probability of the IPF failing to respond to a demand.

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. 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 detailed in the IPF Requirements Specification are met.

Proof Test Coverage Factor

The number of dangerous failures detected by the proof test expressed as a fraction of all possible failures.

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 the IPF in a dangerous state. Formerly known as revealed failure.

Safe Failure Rate

The number of safe failures per unit time.

Safe Failure Class

A class (N or F) derived from the cost benefit of providing safe failure robustness. Where robustness can be justified, the safe failure class is F. Where robustness cannot be justified, the safe failure class is N. Formerly known as revealed failure class.

Safe Failure Fraction

The fraction of all failures that drive the sub-system (e.g. initiator or final element) to the safe state.

(fraction safe failures + [fraction dangerous failures * diagnostic coverage factor]).

Safe Failure Robustness

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 Instrumented System (SIS)

IEC Term Only

The collective term for a group of IPFs, including initiators, the IPS and the final elements.

Safety Integrity Level (SIL)

Dangerous failure class 1, 2, 3 or 4 derived from the consequences of failure on demand and the frequency of demand. Formerly known as the 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) 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.

Trip

The IPF action to bring the final element(s) to a safe state.

Validation

Confirmation that the system under consideration fully meets the integrity requirements set forth in the associated IPF Requirements Specification.

Verification

Demonstration for a particular life-cycle phase that all deliverables (documents, software, hardware) meet the objectives set for that phase.

1.4 ABBREVIATIONS

AK	Anforderungsklasse (IPS requirement class)
BDEP	Basic Design and Engineering Package
BDP	Basic Design Package
BPCS	Basic Process Control System. See (1.3.2) .
BOD	Basis of Design
DCS	Distributed Control System (a form of BPCS)
EDRS	Equipment Data Requisition Sheet
EPC	Engineering, Procurement, Construction project phase
FMEA	Failure Mode Effects Analysis
HAZOP	Hazard and Operability Study
HMI	Human Machine Interface
HSE	Health, Safety and Environment
IEC	International Electrotechnical Commission
IPF	Instrumented Protective Function
IPS	Instrumented Protective System
MOS	Maintenance Override Switch
MVC	Measurement Validation and Comparison (see report OP-98 30219).
OOS	Operational Override Switch
PEFS	Process Engineering Flow Scheme
PFD	Probability of Failure On Demand
PFS	Process Flow Scheme
PLC	Programmable Logic Controller

PRENSAP	Process Engineering and Safeguarding Manual
PS	Project Specification
PSFS	Process Safeguarding Flow Scheme
RRM	Risk and Reliability Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TSO	Tight Shut Off
TUV	Technischer Überwachungsverein (German technical inspection agency)

1.5 CROSS-REFERENCES

Where cross-references to other parts of this PTS are made, the referenced section number is shown in brackets.

Other documents referenced in this PTS are listed in [\(16\)](#).

2. GENERAL

2.1 IPF MANAGEMENT PHILOSOPHY

IPFs have traditionally been designed and managed on the basis of:

- the results of HAZOP studies and Technical Desk HSE Reviews;
- experience;
- perceived good engineering practice.

IEC 61508 and the draft IEC 61511, together with this PTS, present a more structured approach to full life-cycle management of an IPF that:

- removes uncertainty regarding the safety integrity, cost effectiveness and availability requirements;
- provides traceability in IPF design;
- reduces over-engineering;
- prevents under-engineering and therefore increases integrity;
- provides a basis for maintenance and operating strategies;
- achieves a high level of consistency (e.g., of underlying principles, terminology, information, etc.) within the various phases of the project and amongst the different teams that are involved. This will have both safety and economic benefits;
- is owned by different teams and people in different phases during the life-cycle of the IPFs. This requires careful planning, identification of custodians and delegated responsibilities, definition of requirements, deliverables of various phases, etc. to eliminate the possibility of human error during design and maintenance of the IPFs.

NOTE: This PTS is aimed solely at the achievement and maintenance of the functional safety of IPFs and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

2.2 IEC STANDARDS

The two key IEC standards that apply to IPFs and their associated component parts are IEC 61508 - Parts 1 through 7, and Draft IEC 61511 - Parts 1 through 3.

IEC 61508 is relevant primarily for manufacturers and suppliers of IPF components.

Draft IEC 61511 is relevant for designers, integrators and users of IPFs and is therefore the standard most relevant for the Principal.

Should there be conflict between the requirements of the latest versions of IEC 61508, the draft IEC 61511 and this PTS, this PTS shall take precedence.

2.3 THE IPF LIFE-CYCLE MODEL

Figure 1 presents a model for the complete life-cycle of an IPF. The model is a simplified representation of many interdependent activities and does not attempt to fully depict the iterative nature of some of them. For example:

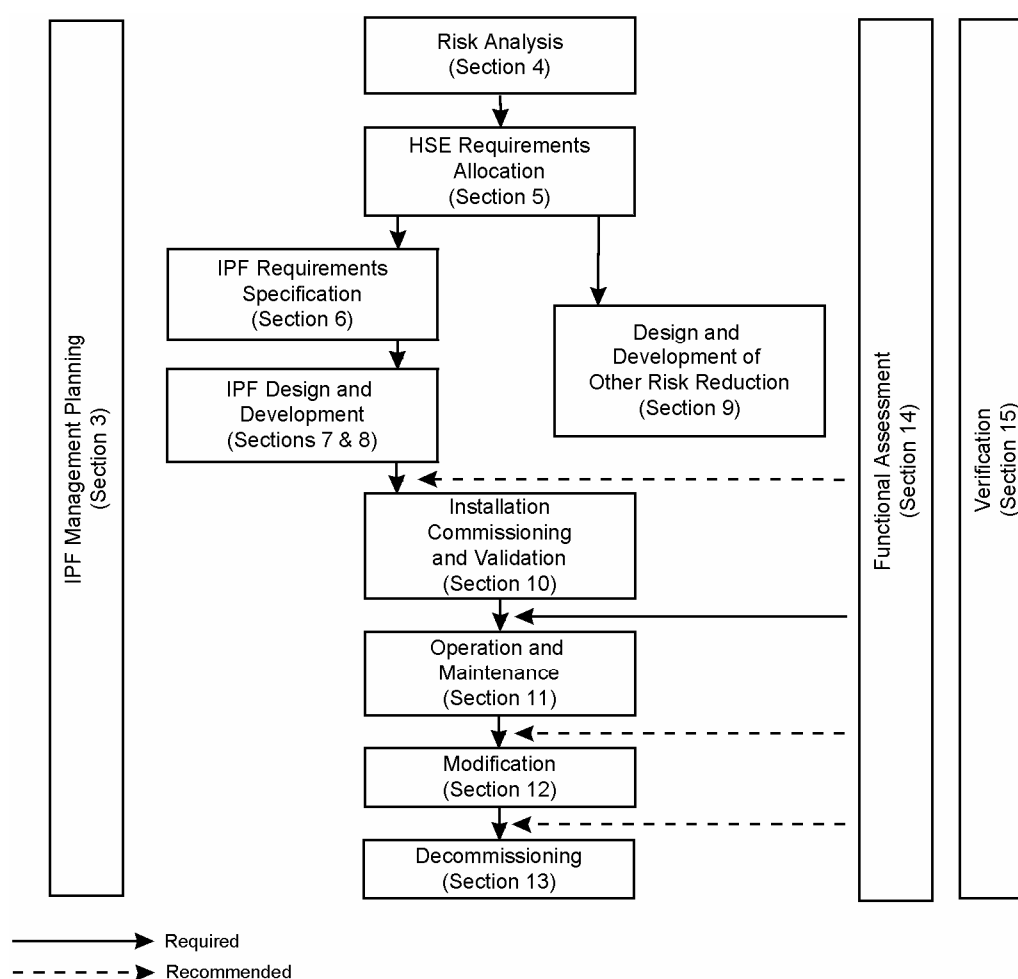
- each phase of the life-cycle will be executed within the modification phase;
- changes in one phase may require a return to one or more previous phases.

Further, activities such as planning and verification are shown as overall processes but apply also to each phase at a more detailed level.

The guidelines and the structure of this PTS are based on the IPF life-cycle model.

Table 1 summarises the key aspects of this PTS.

Figure 1 IPF Life-cycle Management



- NOTES
- 1) There are iteration loops between the activities that are not shown in the figure.
 - 2) To save time in some projects where a standard process and a standard safeguarding design are applied, it is acceptable to carry out the initial HSE requirements specification phase before the Risk Analysis phase. Results of the Risk Analysis shall be reviewed again to determine their possible impact on the HSE requirements specification, e.g., IPF classification, and the extent of further IPF re-identification and re-classification required. However in that case, the HSE requirements allocation shall be preceded by a 'Basic Design & Engineering' phase that produces the documents required to execute the HSE requirements allocation phase.

2.4 STRUCTURE OF THIS PTS

The sections that follow provide practical guidelines on how to meet the objectives of each of the life-cycle phases. The guidelines are structured around the IPF life-cycle model and provide the following for each phase of the life-cycle:

- the *objective* of the phase. This is essentially a re-statement of the objectives presented in Table 1;
- the *scope and timing* of the phase. The scope provides the boundaries of the phase and is stated in organisational, discipline or geographical terms. Recommended timing is generally given in the context of project phases;
- the typical *inputs* required. These are generally in the form of information but may be formal acceptance of the outputs of previous phases;
- the practical *activities* required. These are the tasks required to ensure that the objectives of the phase are met;
- the *custodian and contributors* for the phase. The custodian is accountable for the objective of the phase being met. He may delegate responsibility for activities to other individuals but still remains accountable for the outcome. Contributors will act as enablers, supplying information or services to enable the objectives to be met;
- the minimum *deliverables* of the phase. These represent the physical evidence that the phase has been effectively implemented and may include reports, databases, etc;
- the *success factors* critical to meeting the objective of the phase. These will generally be less tangible issues relating to environment and culture.

Table 1 IPF life-cycle objectives and activities

Amended per
Circular 64/03

LIFE-CYCLE PHASE	OBJECTIVE/DELIVERABLES	ACTIVITIES	DOCUMENTS
IPF Management Planning	A detailed IPF Management Plan is in place to manage the implementation of each life-cycle phase and to demonstrate how the objective of each phase will be practically met.	Preparation of IPF Management Plan	This PTS, Section (3) Report OP 03-30302
Risk Analysis	All hazards and hazardous events associated with the process and processing equipment are known, the associated risks and the required risk reductions have been determined and the risk reduction measures have been identified.	Technical Desk HSE Review/HAZOP	This PTS, Section (4) Report OP 99-30010 EP 95-0313 EP 95-0300 EP 95-0314 PTS 80.47.10.30
HSE Requirements Allocation	The systems (including IPFs) required to implement the risk reduction measures have been identified and the level of integrity required of those systems has been determined.	IPF Identification IPF Classification Study (including calculation of proof test intervals)	This PTS, Section (5)
IPF Requirements Specification	The detailed functional and technical requirements of the IPF to meet the required level of integrity (SIL) have been identified.	Preparation of the IPF Requirements Specification Development of Maintenance Strategy	This PTS, Section (6)
IPF Design and Development	IPF hardware and application software and other risk reduction measures have been designed in order to fully meet the detailed requirements of the IPF Requirements Specification.	Detailed Hardware Design Procurement Procedure Preparation Application Software Design, Configuration and Testing Software Auditing Factory Acceptance and Integration Testing	In principle, all PTSs but more specifically: This PTS, Sections (7), (8), (9) PTS 32.80.10.30 PTS 32.31.00.10 PTS 32.30.20.11 PTS 32.45.10.10 PTS 80.47.10.31 PTS 32.31.00.34
Design and Development - Other Risk Reduction	Other systems have been designed in order to fully meet the required integrity level.	Detailed design of other systems	PRENSAP

Installation, Commissioning and Validation	The design of the IPF is realised and is proven to meet the required SIL.	Planning Installation Function Commissioning Testing	This PTS, Section (10) PTS 62.10.08.11
Operation and Maintenance	The IPF meets the required SIL throughout its operational life.	Competence Management Proof Testing Preventative/Predictive Maintenance Corrective Maintenance Trip Reporting Incident Investigation Failure Rate Data Collection IPF Requirements Specification Review	This PTS, Section (11) EP 95-0120 EP 95-0321 HSE-001
Modification	The IPF meets the required SIL both during and after modification.	Risk Analysis Design and Development Installation, Commissioning and Validation Documentation and Close-out	This PTS, Section (12) EP 95-0313
Decommissioning	The IPF meets the required SIL both during and after decommissioning.	Risk Analysis Design and Development Installation, Commissioning and Validation Documentation and Close-out	This PTS, Section (13) EP 95-0313
Functional Assessment	The level of integrity achieved by the IPF is known throughout its life-cycle.	Formal IPF Assessment	This PTS, Section (14)
Verification	The degree to which the IPF Management Plan has been executed is known.	Progress Review Meetings Auditing	This PTS, Section (15)

2.5 RELATIONSHIP WITH OTHER PROCESSES

2.5.1 General

This PTS should not be implemented in isolation but integrated with the following processes that should be operating on the facility.

2.5.2 The HSE Management Process

The management of IPFs is one part of the overall HSE management of the processing facility. As such, the implementation of processes described here should be clearly connected with the HSE management system/HSE case for the facility.

Note: Further information regarding HSE management systems can be found in EP 95-0100 and in the Shell HSE Committee document "HSE Management System - Integrating HSE into the Business".

2.5.3 The Human Resources Management Process

The management of IPFs requires organisational capability and organisational definition. The implementation of the processes in this PTS, particularly IPF Management Planning, shall at least identify requirements for competence and define roles, responsibilities and accountabilities in conjunction with the Human Resources Management System.

When assessing the competence of individuals, departments or organisations involved with any of the IPF life-cycle phases, the following issues should be taken into consideration:

- the leadership and management qualities available to effectively manage IPFs;
- the skills and knowledge of personnel and the abilities they have to apply those skills and knowledge effectively in a particular organisational context;
- the skills and knowledge in the process being protected, including dynamic behaviour and consequence analysis;
- the skills and knowledge in safety/risk engineering;
- the skills and knowledge in operation and maintenance of all IPF components, including software and hardware;
- the knowledge of safety regulations;
- the novelty and complexity of the process and the IPF components;
- the means available to establish and maintain competence, including prior experience, on the job training, on site class room training and vendor supplied training;
- the systems in place to maintain competence through leave, sickness, relocation or retirement of personnel;
- the systems in place to continually assess competence against agreed standards.

NOTE: Further guidance on competence assurance can be found in EP 95-0120.

2.5.4 Information Management Process

The management of IPFs will generate a great deal of information, ([Appendix 1, Table 7](#)), that must be adequately controlled in terms of approval, formatting, filing and retrieval.

Information generated for IPFs shall be managed by the facility's asset information management system and related software tools. The system should at least provide the tools and guidelines to:

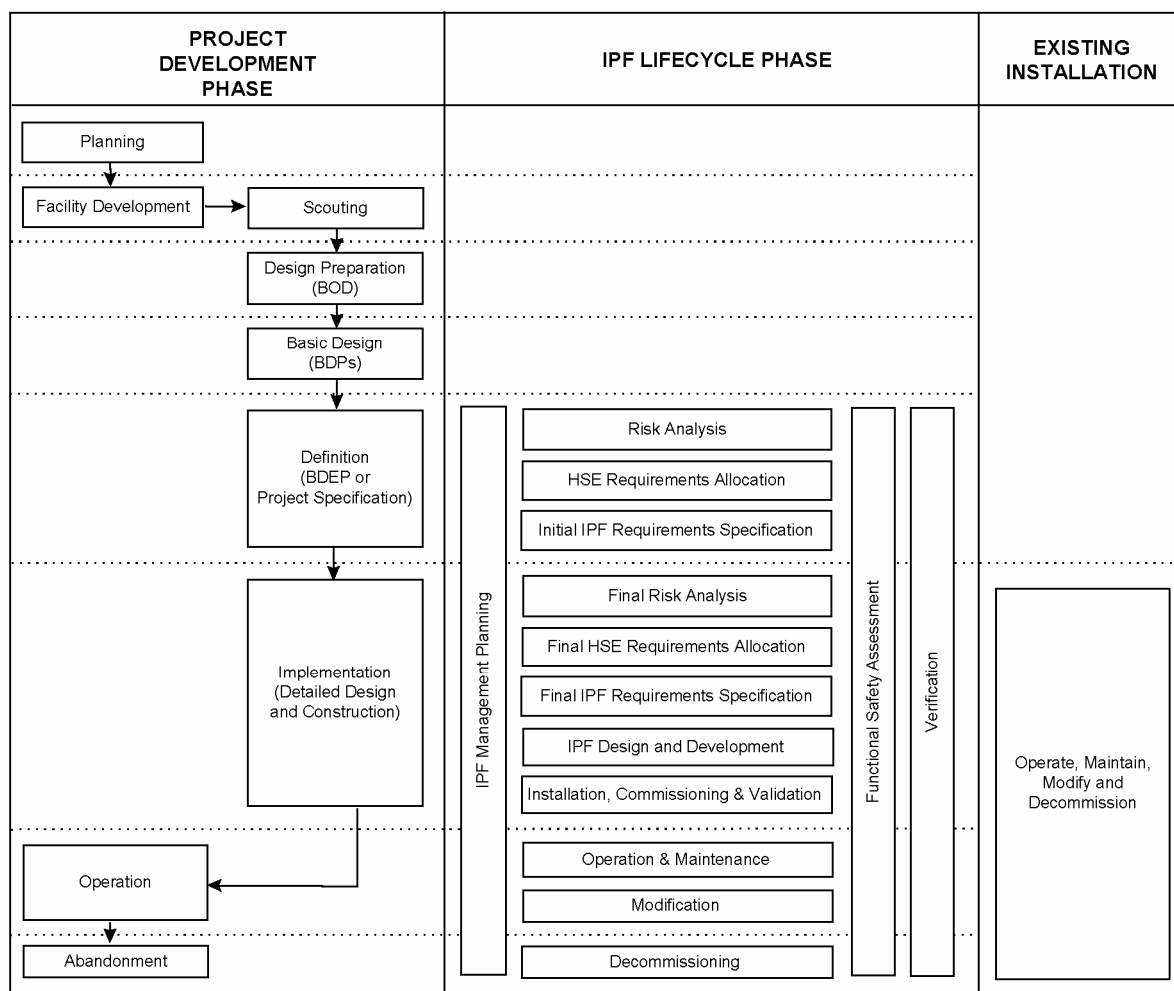
- register the information;
- record the information revision and date;
- register the information custodian;

- provide reference to the location of the information;
- indicate the relative importance of the information to the business;
- indicate whether the information is to be managed as live or non-live, see [\(Appendix 1\)](#);
- indicate the minimum review cycle for live information.

2.5.5 Project Development Process

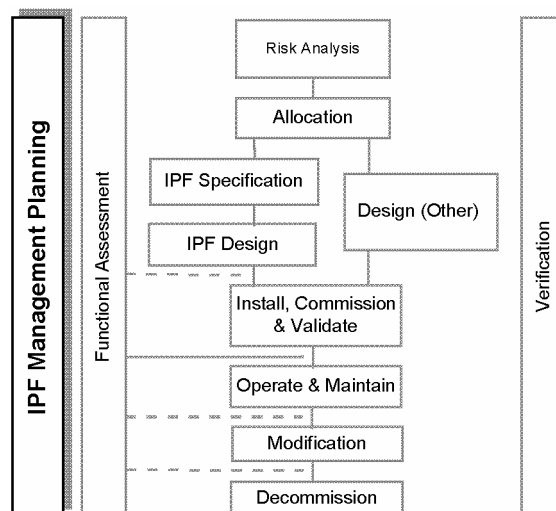
For new developments, the IPF life-cycle has a direct relationship with the project life-cycle and broader business process as shown in Figure 2.

Figure 2 Relationship with Project Process



NOTE: Each life-cycle phase applies equally to projects and to existing installations. For existing installations, the objective is not to design IPFs, but rather to confirm the suitability of the existing IPF installation and to bring the required documentation up to a minimum standard. An added benefit of applying this PTS to existing installations is the optimisation of maintenance and inspection efforts.

3. IPF MANAGEMENT PLANNING



3.1 OBJECTIVE

A detailed IPF Management Plan is in place to manage the implementation of each life-cycle phase and to demonstrate how the objective of each phase will be met in practice.

3.2 SCOPE AND TIMING

The requirements of IPF planning pertain to each phase in the life-cycle and apply equally to new developments and to existing installations.

For new developments, IPF Management Planning shall commence in the definition phase of the project, and agreed components of the IPF Management Plan shall be defined as a deliverable from the Project Specification or BDEP to the Implementation/EPC phase. After further development, the Plan shall be defined as a deliverable from the project organisation to the operating/maintaining organisation.

For new developments, the IPF Management Plan should be integrated into the overall execution plan. For existing facilities, the IPF Management Plan should be aligned with normal business planning processes and should be reviewed at a suitable frequency determined by the Principal (typically once per year) to provide input to budget preparation, personnel establishment, competence assessment, etc.

3.3 INPUTS

Basis of Design/Basic Design Packages
Project Implementation Plan
Overall project schedule

3.4 ACTIVITIES

A documented **IPF Management Plan** shall be prepared that demonstrates how the objective of each phase of the life-cycle will be practically achieved.

This Management Plan may be part of the project or overall site quality plan.

The Plan shall clearly identify all interfaces and demonstrate how they will be managed. As a minimum, interfaces between project phases, between project and operations phases and between disciplines should be addressed.

Contributions should be sought from other discipline engineers (process, HSE, mechanical, etc.), contractors and maintenance and operational personnel.

Concurrence from integrity and operational custodians shall be sought.

The expected form and content of the IPF Management Plan is described in (3.6) below.

3.5 CUSTODIANS AND CONTRIBUTORS

The custodian(s) for activities conducted in this phase shall be clearly identified.

For new developments, the custodian of the IPF Management Plan should be the Project Manager. For existing facilities the custodian should be the person accountable for technical integrity of the facility, delegating responsibility for carrying out activities to engineering, or maintenance personnel.

3.6 DELIVERABLES

An approved IPF Management Plan.

The Plan shall be structured around the IPF life-cycle model and, as a minimum, should contain:

IPF MANAGEMENT PLAN	
Introduction	
Overall Objectives	
Roles and Responsibilities	
Statement of Business Environment	
For each life-cycle phase:	
the objective to be met;	
the scope;	
the roles and responsibilities;	
the required inputs;	
the specific actions to be undertaken. Each action should be clear and unambiguous. Progress of the action should be measurable and if necessary, the means of measuring progress should be described. Each action should be accompanied by an action party, intermediate milestones (if appropriate) and a realistic target completion date or target frequency for cyclic actions;	
the procedures and methods to be used;	
the resources required. These may be personnel, equipment, financial, etc.;	
the expected physical deliverables.	

(Appendix 2) provides a worked example showing one possible format for the IPF Management Plan.

3.7 SUCCESS FACTORS

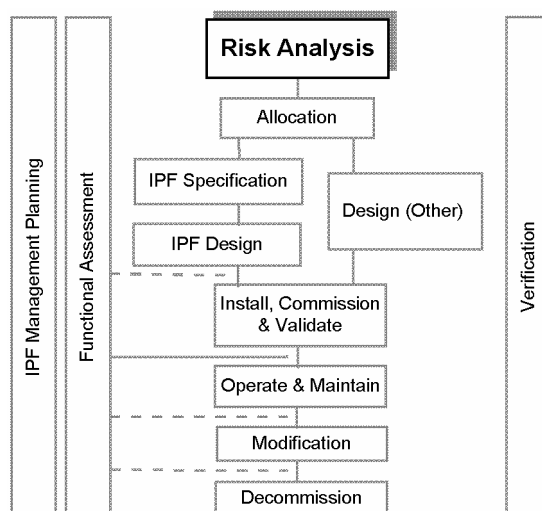
Ownership - Custodians and contributors should have a sense of ownership of the Plan. Ownership can be achieved in practice by appropriate involvement in preparation of the Plan and effective communication of its objectives and content. Typically, this involvement and communication should be with shop floor operational and maintenance personnel, supervisory staff, discipline engineers and management.

Accountability - A single individual should be personally accountable for the plan being produced and achieving its stated objectives. To further strengthen the commitment, this accountability should be formally written into a job statement.

Practicality - The actions defined in the Plan should be practical and achievable.

Interfaces - The Plan should identify the many interfaces between and within project and operating organisations. Successful management of these interfaces by clear procedures and protocols underpinned by effective communication is essential.

4. RISK ANALYSIS



4.1 OBJECTIVE

All hazards and hazardous events associated with the process and processing equipment are known, the associated risks and the required risk reductions have been determined and the risk reduction measures have been identified.

4.2 SCOPE AND TIMING

The scope is limited to risk analyses leading to instrumented risk reduction methods, typically limited to process and utility equipment.

Risk analysis studies shall be conducted during the project definition phase with results incorporated into the Project Specification or BDEP. The studies should be included in the project schedule. The availability and quality of the necessary drawings, documents and personnel will determine the timing.

- NOTES:
- 1) In the context of this document, this phase does not cover conceptual risk-based design studies that optimise issues like plot layout, mechanical integrity, etc.
 - 2) To save time in some projects where a standard process and a standard safeguarding design are applied, it is acceptable to carry out the initial HSE requirements specification phase before the Risk Analysis phase. Results of the Risk Analysis shall be reviewed again to determine their possible impact on the HSE requirements specification, e.g., IPF classification, and the extent of further IPF re-identification and re-classification required. However in that case, the HSE requirements allocation shall be preceded by a 'Basic Design & Engineering' phase that produces the documents required to execute the HSE requirements allocation phase.

4.3 INPUTS

Corporate Risk Tolerability Criteria, e.g., HSE-029
HSE Assumptions
Process/Utility Flow Schemes (PFS/UFS)
Preliminary Process/Utility Engineering Flow Schemes (PEFS/UEFS)
Preliminary Safeguarding Memoranda
Preliminary Equipment Data Requisition Sheets (EDRS)
Preliminary Plant Plot Layouts
Results of Technical Desk HSE Review/HAZOP and other risk analyses for the facility
Operating and Maintenance Philosophies

4.4 ACTIVITIES

A **Technical Desk HSE Review or HAZOP** shall be conducted.

The study shall review the PEFS after they have had at least one round of comments from relevant specialists. As a minimum, the review shall:

- identify the hazards and hazardous events of the process and associated equipment;
- determine the sequence of events leading up to the hazardous events;
- identify the causes of each hazardous event (including fault conditions and any foreseeable misuse);
- identify the consequences of each hazardous event;
- determine the likelihood and hence risk associated with the hazardous events;
- determine the requirement for additional risk reduction;
- establish what risk reduction measures should be taken;
- record the assumptions used during the analysis, including demand rates, failure rates, human intervention and operating conditions.

Detailed guidance on the conduct of Technical Desk HSE Reviews and HAZOPs can be found in OP 99-30010 and EP 95-0313.

NOTE: If decisions are made in later phases of the IPF life-cycle which change the basis on which this risk analysis is carried out, then the risk analysis shall be reviewed and revised as necessary.

4.5 CUSTODIANS AND CONTRIBUTORS

The custodian(s) for activities conducted in this phase shall be clearly identified.

For new developments, the custodian should be the Project Manager. For existing facilities, the custodian should be the Process Engineering discipline.

Contributions to the Technical Desk HSE Review/HAZOP should be sought from other discipline specialists, e.g., instrument, process control, operations, HSE, etc., and from vendors, depending on the particular facility.

4.6 DELIVERABLES

An approved Technical Desk HSE Review or HAZOP report describing the additional risk reduction measures required shall be prepared. The recommendations from the report shall be converted into an action list, complete with action parties and target completion dates.

4.7 SUCCESS FACTORS

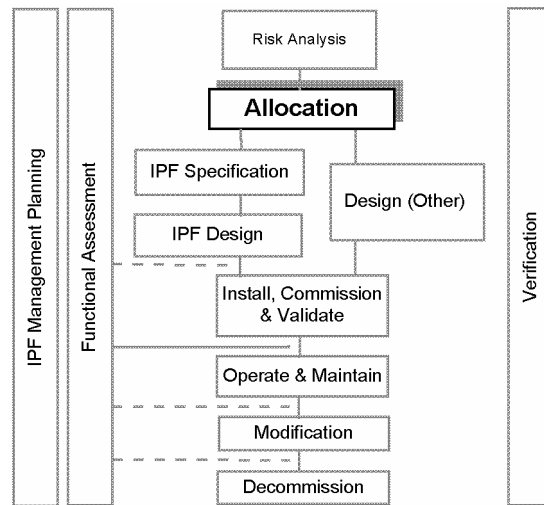
Traceability - Activities carried out in later phases of the IPF life-cycle will directly or indirectly address hazards identified in this Risk Analysis phase, e.g., Allocation and IPF Classification. Traceability of these activities to hazards will enhance their consistency (shared assumptions) and coverage (no gaps, no duplication). Traceability could be achieved in practice by indexing and cross referencing hazards.

Experience - The value of the time spent on the review will be enhanced by maximising the collective experience of the team members in all aspects of the facility under review, particularly regarding the consequence of failures.

Reporting - Accurate and thorough reporting will ensure all issues are addressed and incorporated into the design and will greatly increase the value of the review should it be re-visited during the life of the facility.

Follow-up - To minimise loss of value by incomplete or neglected implementation, an action item co-ordinator should be appointed to track all actions to completion.

5. HSE REQUIREMENTS ALLOCATION



5.1 OBJECTIVE

The systems (including IPFs) required to implement the risk reduction measures have been identified and the level of integrity required of those systems has been determined.

5.2 SCOPE AND TIMING

The scope is limited to the allocation of instrument engineering solutions to the risk reduction measures identified in the Technical Desk HSE Review/HAZOP and the determination of the integrity level required of those solutions.

The allocation shall be carried out during the project definition phase and incorporated into the Project Specification or BDEP. The allocation will likely require the involvement of a number of disciplines and should be done as soon as possible after the Technical Desk HSE Review/HAZOP report is finalised. In reality, some aspects of safety requirements allocation will be done in parallel with or during the Technical Desk HSE Review/HAZOP.

NOTE: To save time in some projects where a standard process and a standard safeguarding design are applied, it is acceptable to carry out the initial HSE requirements specification phase before the Risk Analysis phase. Results of the Risk Analysis shall be reviewed again to determine their possible impact on the HSE requirements specification, e.g., IPF classification, and the extent of further IPF re-identification and re-classification required. However in that case, the HSE requirements allocation shall be preceded by a 'Basic Design & Engineering' phase that produces the documents required to execute the HSE requirements allocation phase.

5.3 INPUTS

Technical Desk HSE Review/HAZOP report
Process/Utility Flow Schemes (PFS/UFS)
Preliminary Process/Utility Engineering Flow Schemes (PEFS/UEFS)
Preliminary Process Safeguarding Flow Schemes (PSFS)
Preliminary Safeguarding Memoranda
Preliminary Cause and Effect diagrams
HSE assumptions
Economic assumptions
Engineering design standards

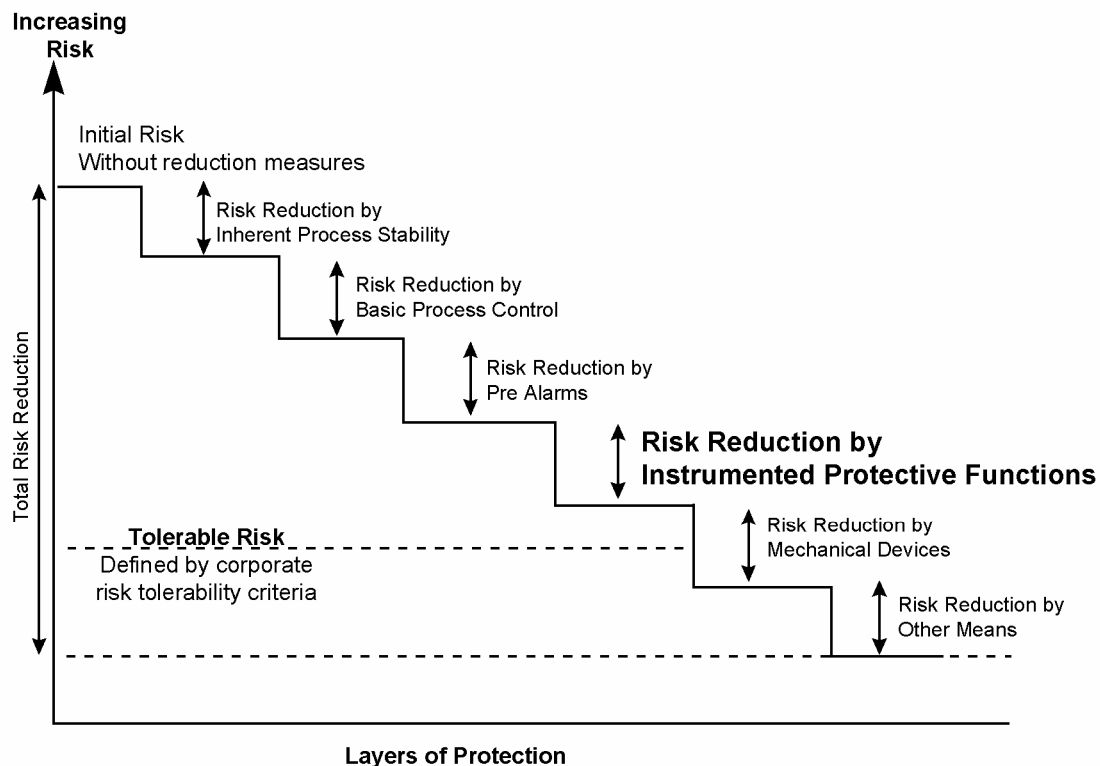
5.4 ACTIVITIES

5.4.1 IPF identification

An engineering solution will have been allocated to each risk reduction measure identified in the Risk Analysis. Solutions may take the form of mechanical/structural protections, instrumented protections (providing automated action or prompting manual action, e.g., alarms), procedural protections, external facilities, etc.

Figure 3 demonstrates how the summed contribution of risk reductions from both IPFs and other risk reduction methods reduces the residual risk to below the tolerable level.

Figure 3 Risk Reduction by Layers of Protection



The sub-set of the solutions that are instrumented, i.e., IPFs, shall be identified. This will enable preparation of preliminary Cause and Effect Diagrams and IPF content of PEFS.

5.4.2 IPF classification study

An IPF classification study shall be conducted. The study shall determine for each IPF:

- the required SIL;
- the requirement for dangerous failure robustness, taking into account the level of complexity of the IPF sub-system, the SIL and the safe failure fraction, see PTS 32.80.10.10;
- the proof test interval required to meet the PFD target for the SIL.

Additionally the study should establish the cost-benefit of applying safe failure robustness.

The methodology chosen to determine the SIL shall use HSE risk tolerability criteria that are consistent with applicable corporate guidelines (typically based on the Risk Assessment Matrix issued by the Shell HSE Advisers Panel, April 1999 (HSE-029).

The calculation of proof test interval shall take into account:

- the highest SIL applicable to the function;
- the probability of failure on demand required by the SIL;

- the chosen logic solver technology, e.g., electromechanical relays, PLC, solid state;
- the minimum implementation architecture, e.g., 1oo1, 1oo2, etc.;
- the dangerous failure rates for the initiator, logic solver and final element;
- the safe failure rates for the initiator, logic solver and final element;
- where robustness has been used, the susceptibility of the IPF to common mode failures, i.e., the Beta factor;
- the coverage factor of any diagnostic features, i.e., the diagnostic coverage factor;
- the coverage factor of the proof test, i.e., the proof test coverage factor;
- the repair time to correct a detected failure;
- the human error rate;
- the duration for which the proof test defeats the protection;
- the maintenance shutdown interval.

Typical methods for calculating proof test intervals include simulation, cause consequence analysis, fault tree analysis, Markov models, simplified formulae and reliability block diagrams.

The average probability of failure on demand targets and IPS approval (AK class) for each SIL shall be according to Table 2. Functions classified as lower than SIL 1 have no special PFD requirement.

Table 2 Relationship between SIL, PFD and AK Class

Safety Integrity Level (SIL)	Average probability of failure on demand	IPS approval (AK Class)
1	10^{-2} to 10^{-1}	3
2	10^{-3} to 10^{-2}	4
3	10^{-4} to 10^{-3}	5, 6
4	10^{-5} to 10^{-4}	7

If the classification determines that an IPF of SIL 4 is required, additional safety and reliability assessments should be considered. The use of an IPF in such cases may require the approval of local authorities.

5.5 CUSTODIANS AND CONTRIBUTORS

The custodian(s) for activities conducted in this phase shall be clearly identified.

For new developments, the custodian should be the Project Manager. For existing facilities, the custodian could be the Instrument Engineering, Process Engineering or Operations discipline.

Contributions to the IPF classification study should be sought from other discipline specialists, e.g., instrument, process control, operations, HSE, etc., and from vendors, depending on the particular facility.

5.6 DELIVERABLES

Updated Cause and Effects Diagrams
IPF Narratives
IPF Classification Study report

5.7 SUCCESS FACTORS

Buy-in - The chosen IPF classification methodology and the potential implications for the final design, i.e., reduced IPF protection, should be understood and accepted by all

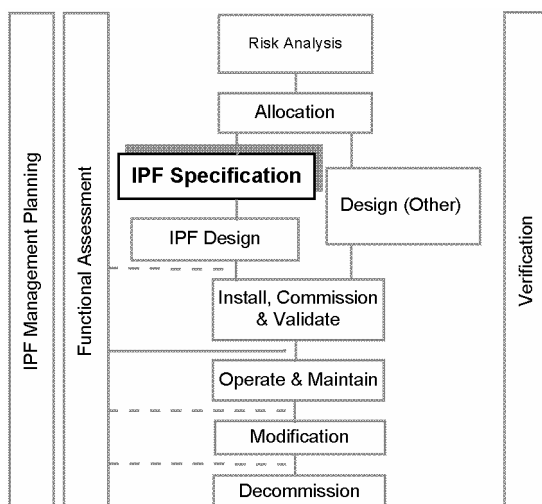
stakeholders, e.g., management, other disciplines, vendors and external bodies, before a classification exercise is begun.

Competence - The facilitator of the IPF classification study shall be competent by virtue of training and suitable experience with the chosen method.

Experience - The value of the time spent on the IPF classification will be enhanced by maximising the collective experience of the team members in all aspects of the facility under review, particularly consequence of failures.

Consistency - Consistency in the interpretation of risk and the response to it can be achieved by traceability to hazards as mentioned in (4.7). Consistency can be further enhanced if team members contributing to the IPF classification study are the same as those who conducted the Technical Desk HSE Review/HAZOP. However, care should be taken to address potential “common mode” problems this approach may introduce, e.g., by inexperienced team members making incorrect assumptions, etc.

6. IPF REQUIREMENTS SPECIFICATION



6.1 OBJECTIVE

The detailed functional and technical requirements of the IPF to meet the required level of integrity (SIL) have been identified.

6.2 SCOPE AND TIMING

The scope of this phase is limited to hardware and software elements of the IPF (initiator, logic solver and final element). The deliverable of the phase is an IPF Requirements Specification that provides the detailed specification for the IPF. At the discretion of the Principal, the IPF Requirements Specification may be prepared for the entire site or broken down into separate Specifications for each process plant/unit.

Development of the IPF Requirements Specification should commence during project definition and shall be included in the Project Specification or BDEP. Work should commence as soon as the HSE Requirements Allocation is complete. The IPF Requirements Specification should be completed during project implementation.

6.3 INPUTS

Cause and Effect Diagrams
Safeguarding Memoranda
Process Safeguarding Flow Schemes (PSFS)
Process Engineering Flow Schemes (PEFS)
IPF Classification Study report
IPF Narratives

6.4 ACTIVITIES

6.4.1 Preparation of the IPF Requirements Specification

An IPF Requirements Specification shall be prepared. The specification shall provide a single point of reference for IPF technical and functional requirements. It shall contain the information described in (6.6) below.

6.4.2 Development of a maintenance strategy

A strategy for proof testing and maintenance of the IPF shall be developed during this specification stage so that necessary allowances can be made in the design of hardware and software.

The maintenance strategy may influence the following decisions:

- requirement for additional robustness in initiators and final elements where operational opportunities to proof test and maintain are limited. Robustness will improve access to components for testing or allow test intervals to be increased to allow access;
- requirement for additional access to instruments, e.g., ladders, platforms, etc., or allowance for reduced access;
- use of automated testing using software algorithms and/or hardware, e.g., Measurement Validation and Comparison (MVC), automated valve stroking, partial valve stroking;
- operational and maintenance manning levels for the facility.

6.5 CUSTODIANS AND CONTRIBUTORS

The custodian(s) for activities conducted in this phase shall be clearly identified.

For new developments, the custodian should be the Project Manager. For existing facilities, the custodian should be the Instrument Engineering discipline.

Contributions to the IPF Requirements Specification should be sought from other discipline specialists, e.g., instrument, process control, operations, HSE, etc., and from vendors, depending on the particular facility.

6.6 DELIVERABLES

The IPF Requirements Specification document shall provide a single point of reference for all information listed in [Table 3](#). Depending on the plant, the specification may be:

- One document for the entire plant containing all information required by [Table 3](#);
This option might be used for relatively small plants.
- An independent document for each processing unit, each containing the information required by [Table 3](#);
This option might be used for larger plants with smaller processing units that operate autonomously from a process, instrument or management perspective or otherwise have little in common.
- A manual containing a common document and separate documents for each processing unit. The common document would describe general issues that apply to all process units, e.g., issues from the Design Requirements section of Table 3 dealing with more general design philosophies such as MOS handling. The process unit documents would hold the detailed information for each unit.

This option would be used for larger integrated sites such as an LNG plant.

Table 3 IPF Requirements Specification contents

Section 1) IPF Narrative: A functional description of the IPFs, including: * The safe state of the process, e.g., venting by valve opening, rundown shutoff by valve closure. * An overview of the IPFs required to achieve the required risk reduction. * The process inputs to the IPFs. – Settings for process input trips and alarms and their required accuracy. * The process outputs from the IPFs and their actions. – The process safety time for process outputs and other requirements, e.g., TSO. * The functional relationship between the inputs and outputs. This should include logical, mathematical and permissive relationships. NOTE: In practice, this will be the cause and effect diagrams together with narrative descriptions as required. * Requirements for manual reset, maintenance override, operational override, start-up override and manual shutdown per function. – The maximum allowable spurious trip rate (or safe failure rate). * The modes of operation of the facility, e.g., start-up, shutdown, automatic, manual, foreseeable abnormal conditions and the IPFs required to operate in each mode.
Section 2) IPF Specification Sheets: An IPF specification sheet for each IPF defining: * The assumed demand rate and description of demand scenarios. * The Safety Integrity Level (SIL). NOTE: The response time will influence design aspects such as valve stroking time and IPS loading and cycle time. The response time will also be important in determining whether operator response to alarms can be relied upon.
Section 3) IPF Component Specification Sheets: * The system architecture, including robustness of initiators and final elements and methods of voting, e.g., 2oo3. – The minimum proof test interval. – Proof test procedures. – Documented source of failure rates, proof test coverage factor, diagnostic coverage factor and Beta factor for common mode failures.

Continued on next page.

Section 4) Design Requirements:

The general requirements for design of IPFs, including:

- * The architecture, interfaces between subsystems, performance and integrity requirements (including the interfaces) for, e.g., IPS, DCS, PLC, machinery control system, etc. See PTS 32.80.10.30
- * Interfaces, including HMIs required for operation, maintenance and communication.
 - The maximum allowable cycle time for the logic solver (taking into account the most stringent response time requirement of all IPFs).
 - The failure modes of the IPF and the associated desired responses.
 - The specific requirements with respect to procedures for starting and re-starting the IPF.
 - Diagnostics and automatic tests required in the operating system and application software.
 - Specific configurations for handling MOS/OOS facilities in hardware and software.
 - Software security requirements, e.g., for protection of modifiable parameters in intelligent transmitters and the IPS.
 - The physical environment likely to be encountered by all components in the IPF during all phases of its life-cycle, e.g., temperature, humidity, contaminants, vibration, shock, electromagnetic interference, radio frequency interference, lightning, etc.

Legend:

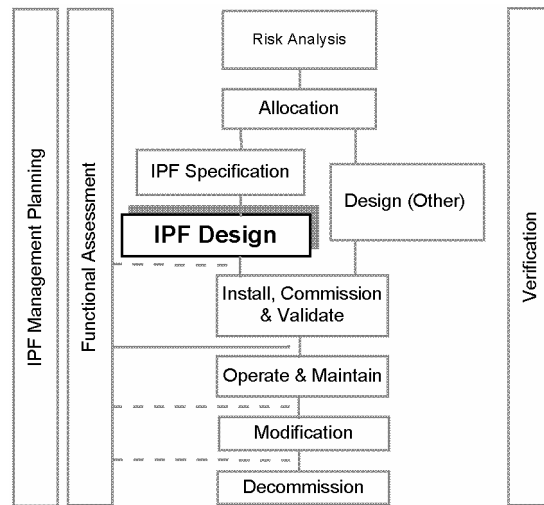
- * Information to be completed during the definition phase and documented in the Project Specification or the BDEP;
- Information to be completed during the implementation phase.

See [\(Appendix 5\)](#) for guidance in the case of large projects.

6.7 SUCCESS FACTORS

Communication - The IPF Requirements Specification brings together information supplied by a number of disciplines that is critical to the successful implementation of the IPF. Effective communication between disciplines will be necessary to manage issues such as the control of change of information, physical communication of information and maintenance of information.

7. DESIGN AND DEVELOPMENT - HARDWARE



7.1 OBJECTIVE

IPF hardware has been designed to fully meet the detailed requirements of the IPF Requirements Specification.

7.2 SCOPE AND TIMING

The scope is limited to the design of all IPF sub-systems (excluding application software but including operating system software), including the initiators, logic solver, final elements and associated HMI(s).

The detailed design shall be carried out during the Implementation/EPC project phase.

7.3 INPUTS

IPF Requirements Specification
Engineering design standards

7.4 ACTIVITIES

7.4.1 Detailed design

A detailed design of the integrated IPF hardware shall be undertaken. The detailed design shall ensure that the requirements of the IPF Requirements Specification and, in particular, of the associated SIL are fully met. Specific design requirements can be found in PTS 32.80.10.10

7.4.2 Hardware procurement

General requirements for procurement of IPF components can be found in PTS 32.31.00.10 Requirements for SIL certification may be found in PTS 32.80.10.10