

**PETRONAS TECHNICAL STANDARDS**  
**HEALTH, SAFETY AND ENVIRONMENT**

**DESIGN**  
**(GUIDELINE)**

**PTS 60.0107**

**JUNE 2006**



## PREFACE

PETRONAS Technical Standards (PTS) publications reflect the views, at the time of publication, of PETRONAS Group of Companies.

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' Group of Companies 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.

**AMENDMENT RECORD SHEET**

| <b>Chap<br/>No.</b> | <b>Sect<br/>No.</b> | <b>Description</b>            | <b>Issue<br/>No.</b> | <b>Date</b> | <b>Rev<br/>No.</b> | <b>Date</b> | <b>Approve<br/>by :<br/>(initial)</b> |
|---------------------|---------------------|-------------------------------|----------------------|-------------|--------------------|-------------|---------------------------------------|
| All                 | All                 | Renumbering to PTS<br>60.0107 | 1                    | June<br>06  | 1                  | June<br>06  | IGA                                   |

## CONTENTS

|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>1. Introduction</b>                              | <b>8</b>  |
| 1.1 Objective of this Document                      | 8         |
| 1.2 Background                                      | 8         |
| <b>2. Overview</b>                                  | <b>9</b>  |
| 2.1 Scope of the Document                           | 9         |
| 2.2 Area of Coverage                                | 9         |
| 2.3 Organisation of the Document                    | 11        |
| <b>3. HSE Management System</b>                     | <b>12</b> |
| 3.1 Leadership and Commitment                       | 13        |
| 3.2 Policy and Strategic Objectives                 | 13        |
| 3.2.1 Policy                                        | 13        |
| 3.2.2 Strategic objectives                          | 14        |
| 3.3 Organisation, Resources and Documentation       | 14        |
| 3.3.1 Organisational structure and responsibilities | 14        |
| 3.3.2 Management representative                     | 16        |
| 3.3.3 Resources                                     | 16        |
| 3.3.4 Competence                                    | 16        |
| 3.3.5 Contractor HSE management                     | 17        |
| 3.3.6 Communication                                 | 17        |
| 3.3.7 Documentation and its control                 | 17        |
| 3.4 Hazards and Effects Management (HEMP)           | 20        |
| 3.4.1 Overview                                      | 20        |
| 3.4.2 HEMP in design                                | 20        |
| 3.5 Planning and Procedures                         | 21        |
| 3.5.1 General                                       | 21        |
| 3.5.2 Asset integrity                               | 22        |
| 3.5.3 Procedures and work instructions              | 22        |
| 3.5.4 Management of change                          | 22        |
| 3.6 Implementation and Monitoring                   | 23        |
| 3.6.1 Activities and tasks                          | 23        |
| 3.6.2 Monitoring                                    |           |
| 3.6.3 Records                                       | 23        |
| 3.7 Assurance                                       | 24        |
| 3.7.1 Assurance                                     | 24        |
| 3.7.2 Assurance action and feedback                 | 24        |
| 3.8 Review                                          | 24        |

|           |                                                      |           |
|-----------|------------------------------------------------------|-----------|
| 3.8.1     | Review                                               | 24        |
| 3.8.2     | Feedback from reviews                                | 24        |
| <b>4.</b> | <b>Identification and Assessment of Hazards</b>      | <b>25</b> |
| 4.1       | Hazard Identification                                | 25        |
| 4.1.1     | Experience                                           | 25        |
| 4.1.2     | Checklists                                           | 25        |
| 4.1.3     | Codes and standards                                  | 26        |
| 4.1.4     | Structured review techniques                         | 26        |
| 4.2       | Hazard Assessment                                    | 28        |
| 4.2.1     | Overview                                             | 28        |
| 4.2.2     | Codes and standards                                  | 29        |
| 4.2.3     | Qualitative analysis                                 | 29        |
| 4.2.4     | Consequence analysis                                 | 29        |
| 4.2.5     | Quantitative Risk Assessment (QRA)                   | 30        |
| 4.3       | A Framework for Hazard Identification and Assessment | 32        |
| <b>5.</b> | <b>Control of Hazards</b>                            | <b>35</b> |
| 5.1       | Overview                                             | 35        |
| 5.1.1     | Design for ease of operation and maintenance         | 35        |
| 5.1.2     | Substitution                                         | 35        |
| 5.1.3     | Reduce inventory of toxic/hazardous materials        | 36        |
| 5.1.4     | Simplify the process                                 | 36        |
| 5.1.5     | Reduce probability of loss of containment            | 37        |
| 5.1.6     | Eliminate sources of ignition                        | 37        |
| 5.1.7     | Reduce pressure                                      | 37        |
| 5.1.8     | Reduce temperature                                   | 38        |
| 5.1.9     | Reduce volatility                                    | 38        |
| 5.2       | General System Design Considerations                 | 38        |
| 5.2.1     | Overview                                             | 39        |
| 5.2.2     | Operability and maintainability                      | 39        |
| 5.2.3     | The design envelope                                  | 45        |
| 5.2.4     | Corrosion mitigation                                 | 50        |
| 5.3       | Specific Equipment Design Considerations             | 50        |
| 5.3.1     | Overview                                             | 50        |
| 5.3.2     | Piping and pipelines                                 | 50        |
| 5.3.3     | Pig launchers and receivers                          | 54        |
| 5.3.4     | Pressure vessels                                     | 55        |
| 5.3.5     | Heat exchangers                                      | 56        |
| 5.3.6     | Furnaces and heaters                                 | 57        |
| 5.3.7     | Machinery                                            | 58        |
| 5.3.8     | Atmospheric storage tanks                            | 63        |
| 5.3.9     | Electrical systems                                   | 66        |

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>6. Recovery From Hazardous Events</b>              | <b>67</b> |
| 6.1 Facilities Layout                                 | 68        |
| 6.1.1 Objective                                       | 68        |
| 6.1.2 Functional requirements                         | 68        |
| 6.1.3 Guidelines                                      | 69        |
| 6.2 Facility Control Centre                           | 79        |
| 6.2.1 Objective                                       | 79        |
| 6.2.2 Functional requirements                         | 79        |
| 6.2.3 Guidelines                                      | 79        |
| 6.3 Process Safeguarding                              | 83        |
| 6.3.1 Objective                                       | 83        |
| 6.3.2 Functional requirements                         | 83        |
| 6.3.3 Guidelines                                      | 83        |
| 6.4 Fire and Gas Detection System                     | 86        |
| 6.4.1 Objectives                                      | 86        |
| 6.4.2 Functional requirements                         | 87        |
| 6.4.3 Guidelines                                      | 87        |
| 6.5 Emergency Shut-Down System                        | 96        |
| 6.5.1 Objective                                       | 96        |
| 6.5.2 Functional requirements                         | 96        |
| 6.5.3 Guidelines                                      | 97        |
| 6.6 Emergency Depressurisation (EDP) - Vent and Flare | 99        |
| 6.6.1 Objective                                       | 99        |
| 6.6.2 Functional requirements                         | 99        |
| 6.6.3 Guidelines                                      | 99        |
| 6.7 Emergency Power System                            | 104       |
| 6.7.1 Objective                                       | 104       |
| 6.7.2 Functional requirements                         | 104       |
| 6.7.3 Guidelines                                      | 104       |
| 6.8 Drainage Systems                                  | 106       |
| 6.8.1 Objective                                       | 106       |
| 6.8.2 Functional requirements                         | 106       |
| 6.8.3 Guidelines                                      | 106       |
| 6.9 Active Fire Protection                            | 109       |
| 6.9.1 Objectives                                      | 109       |
| 6.9.2 Functional requirements                         | 109       |
| 6.9.3 Guidelines                                      | 110       |
| 6.10 Passive Fire Protection                          | 124       |

|                                               |     |
|-----------------------------------------------|-----|
| 6.10.1 Objectives                             | 124 |
| 6.10.2 Functional requirements                | 124 |
| 6.10.3 Guidelines                             | 124 |
| 6.11 Evacuation, Escape and Rescue Provisions | 128 |
| 6.11.1 Objective                              | 128 |
| 6.11.2 Functional requirements                | 128 |
| 6.11.3 Guidelines                             | 129 |
| I Fire and Explosion Strategy                 | 137 |
| Abbreviations                                 | 142 |
| Glossary                                      | 144 |
| References                                    | 144 |

## 1. INTRODUCTION

### 1.1 OBJECTIVE OF THIS DOCUMENT

This document has been prepared for those involved in supervising the engineering design of oil and gas facilities. The objectives of the document are:

- to describe the specific application of Hazards and Effects Management Process (HEMP) in engineering design, namely:
  - the techniques available for hazard identification
  - the varying approaches to hazard assessment
  - methods of controlling and recovering from hazardous events.
- to provide a route map to more detailed references and provide guidance in their application.
- to provide a frame of reference for the application of hazard management tools and techniques.

### 1.2 BACKGROUND

In the engineering design phase, there is considerable scope to remove or minimise hazards. It is during this phase that provision can be made to reduce the risks associated with a process, system or facility to a level that is as low as reasonably practical (ALARP).

This can be achieved in a number of ways. In order of preference these are:

- removal of hazards
- reducing the probability of hazardous events occurring
- minimising the risk of escalation should a hazardous event occur.
- Once the hardware has been installed, retroactive implementation becomes relatively more hazardous and considerably more expensive:
- new design teams have to be mobilised
- the introduction of new facilities may introduce previously unrealised hazards
- construction activities have to take place in the midst of an operational plant
- the implementation of new hardware may attract loss of revenue due to production downtime.

It is crucial therefore that the opportunities available for minimising risk in the design and engineering phase are not lost.

## **2. OVERVIEW**

### **2.1 SCOPE OF THE DOCUMENT**

This document provides the information required to manage HSE during engineering design. It provides guidance on:

- the organisation and procedures necessary for management of HSE
- the tools available for HSE analysis, or Hazards and Effects Management Process (HEMP)
- the identification, assessment and control of hazards associated with common oil and gas and petrochemical plant and equipment
- recovery from hazards
- the objectives, functional requirements and guidelines for specific safety systems.

Although this is a 'design' document, it mainly addresses the hazard management process as it relates to the containment of hydrocarbons. It does not as yet address many other areas of design such as offshore structures, floating units and subsea processing facilities and risers.

### **2.2 AREA OF COVERAGE**

The document provides guidance on the HSE issues to be addressed in engineering design.

Engineering design in this context is identified as the period that commences with the issue and approval of the Project or Field Development Plan. At this stage the previous consideration of a variety of development options has been narrowed down for more detailed optimisation and engineering. The period concludes with the issue of the approved AFC drawings, completion of the material requisitions, and provision of agreed commissioning and operating manuals and procedures.

The principal activities undertaken during this period include:

- preparation of the Basis for Design
- execution of Conceptual Engineering Design and preparation of the Project Specification
- execution of Detailed Design (including preparation of construction work scopes).

Within the context of the total project development, hazards and effects management in this phase will build upon the studies and decisions made in the foregoing phases. Equally the decisions made during this phase will have implications for future phases. Below is a synopsis of the changing emphasis of HEMP, complete with an indication of where guidance on each phase can be found.

**Concept Development** - during this phase most of the major hazards and effects will be identified and an initial assessment of their importance will take place. In this phase there is considerable scope for removing potential hazards. The emphasis is on safeguarding HSE by adopting, where possible, an inherently safe approach, e.g. specifying unmanned (rather than manned) facilities, placing processing facilities onshore rather than offshore etc.

**Conceptual Design and Project Specification** - During this phase there is still a clear identification and assessment focus, albeit at a more detailed level of application. The emphasis is on incorporating inherently safe features at a detailed level, and prescribing passive and active control measures for remaining hazards. These are incorporated into the philosophies and engineering drawings (process engineering flow scheme [PEFS], process flow schemes [PFSs], Cause and Effects etc) which constitute the base documents for the remainder of the design phase.

**Detailed Design** - By the time the detailed design phase is reached, the cornerstones of the HSE safeguards will have been placed. The emphasis becomes directed to the detailed engineering of the agreed control and recovery measures, and developing procedural control and recovery mechanisms.

**Construction and Commissioning** - The methods of construction imposed by the design will dictate, to a certain extent, the risks associated with the construction and commissioning phases. Where possible the risks associated with construction should be minimised by careful design. Residual risks will be fed forward as input to the construction contracting process. Construction execution presents its own hazards, and for major projects a separate construction HSE Case may often be prepared.

**De-commissioning** - Decisions made in the design phase will often have considerable impact on the options available for decommissioning. The physical difficulties associated with decommissioning and the obligations placed on the operator during the decommissioning should be considered during design.

## Operations

Decisions made during the engineering phase should reflect an agreed operations and maintenance philosophy. At the handover stage a HSE case should be in existence which formally documents the hazards and effects associated with the facility and the methods for their control.

## 2.3 ORGANISATION OF THE DOCUMENT

The document is structured in the following way:

### **Chapter 3 HSE Management**

Highlights the elements of an HSE management System and the HSE Management principles relevant to engineering design. The structure of this section is consistent with Section PTS 60.0101 Group HSE Management System Manual and builds on the generic HSE management principles described within that section.

### **Chapter 4 Identification and Assessment**

Describes the various methods of identifying and assessing hazards and effects - both qualitative and quantitative.

### **Chapter 5 Control of Hazards**

Defines the principles of inherent safety and hazard control, and indicates how these principles are applied to design.

### **Chapter 6 Recovery from Hazardous Events**

Defines for those systems provided for recovering from the consequences of hazardous events:

- system objectives
- functional requirements
- guidelines.

### 3. HSE MANAGEMENT SYSTEM

Figure 3.1 HSE Management System



#### Overview

A management system describes the way a process or activity is managed with respect to its stated objectives (Figure 3.1). It does this by concentrating on critical aspects, ensuring they are properly controlled, measured and reported so as to assure performance and identification of areas for improvement. The introduction of such systems for the management of health, safety and environment is required in many areas by legislators, and many of them now require the production of a facility specific Safety, or HSE, Case.

Where an HSE Management System has been developed and implemented, management, shareholders, employees, and where appropriate, regulators, will have assurance that:

- the hazards and effects associated with the asset and its operation have been fully identified and are properly managed
- the assets being operated by the company have been designed and are being operated to meet known criteria
- the methods employed to manage risks have been systematically identified and appropriate know-how, controls and verification processes have been applied
- the methods and quality of application are continually assessed and improved by a systematic programme of performance monitoring, audit and review
- there is documentary evidence of the above.

OGP has produced guidelines for HSE Management which has been adopted by the PETRONAS as the basis for their HSE MS, PTS 60.0101. It contains details of that HSE MS which is applicable at both corporate and activity level. The remainder of this chapter retains the same structure as that section and provides guidance particularly relevant for engineering design.

For a specific facility the HSE Management System is translated into a facility-specific document (the HSE or Safety Case). A central element of that HSE Case is produced during the engineering design phase, i.e.:

- the demonstration that all potentially significant hazards have been identified
- the risks from those hazards evaluated, understood and minimised to ALARP level
- the controls to manage the causes (threats) and consequences of hazardous events are in place.

The format of the documentation of that Hazards And Effects Management Process (including the Hazard Register) is included in PTS 60.0303 Documenting a HSSE Management System and HSE Cases.

### **3.1 LEADERSHIP AND COMMITMENT**

Strong and visible leadership from Management is necessary to promote a culture conducive to minimising risks. Senior Management must foster the active involvement of employees and contractors towards improving HSE performance by encouraging a culture of belief, motivation, individual responsibility, participation and commitment.

Demonstration of commitment to HSE includes:

- ensuring that HSE criteria are explicitly considered in decisions
- providing appropriate resources for HSE studies and analysis
- communicating (in presentations and documentation) the HSE aspects of design in the development.

### **3.2 POLICY AND STRATEGIC OBJECTIVES**

#### **3.2.1 Policy**

Policies are the means by which Management communicate their intentions and expectations. A policy is a concise statement of belief, principles and direction.

HSE policy documents should form part of a structured hierarchy. At the highest level is the PETRONAS HSE Policy. This in turn has been customised by individual Operating Companies (OPU / JV) into policy statements that reflect local conditions and priorities. The policy is normally restricted to one A4 page of concise action-

oriented statements.

For major projects the development of a specific project HSE policy statement, signed by the project manager should be considered. The preparation of such a document gives a clear HSE focus both internally to the project team, and equally to external agencies, both contractors and regulatory bodies.

The project HSE policy document should set out both the overall policy of the project (which recognises the specific scope and external considerations) and also the roles and responsibilities of the project organisation.

### **3.2.2 Strategic objectives**

At the end of the design phase all potential opportunities for hazards and effects reduction should have been evaluated and, where appropriate, incorporated. Within the operations phase the only ability to control hazards is by the application of procedural controls and employee competence assurance.

The strategic objectives of a design should therefore include:

- the provision of a facility where the risks have been reduced to a level that is ALARP
- the provision of documentation to demonstrate the above, and to provide a link into the operations phase.

In relation to these overall objectives a number of sub-objectives should be defined in areas such as asset loss and damage, personnel injury, damage to health, escape and rescue, environmental effects etc. Performance criteria should be defined to allow measurement of the degree of success in meeting the stated objectives.

## **3.3 ORGANISATION, RESOURCES AND DOCUMENTATION**

### **3.3.1 Organisational structure and responsibilities**

#### **Single Point Responsibility**

Regardless of the size of a design, or structure of the project organisation, the responsibility for implementation of all HSE objectives must always lie with the project manager. The project manager is responsible for ensuring that HSE considerations are given appropriate weighting, equivalent to the project cost, schedule and quality.

Two relatively independent tasks face the project manager in managing the HSE aspects of his project:

- to optimise the development of the facilities and the associated procedures and technical information so as to minimise the hazards and effects during their operating life and subsequent decommissioning

- to exercise full control of the HSE aspects in the execution of the project itself (i.e. the day-to-day HSE risks encountered by the project team (transport, office, health etc).

Within the design phase the development of a 'safe and environmentally acceptable facility' will tend to be the dominant task. It should however be realised that decisions made in the design phase will have an impact on the direct HSE risks imposed in the construction phase. Further consideration of the impact on construction is given in PTS 60.0108 Construction and Commissioning.

### **Interdisciplinary Involvement**

Representatives from operations and maintenance should be fully involved from the earliest moment, either on a permanent or part-time basis. They will provide valuable input in the following areas:

- definition and interpretation of the operating and maintenance philosophies
- hands-on experience of operating hazards
- relative merits of hardware and procedural controls for managing hazards
- development of commissioning and handover plans
- requirements for, and contents of, operating documentation

Most importantly, they will prepare the first draft of the Operations HSE Case.

The personnel seconded for this role should have an adequate level of seniority, experience, vision and authority to ensure that operating hazards are fully identified and that suitable control measures are put in place.

The optimisation of the facility design with respect to HSE also requires a high level of interdisciplinary co-ordination between the engineering disciplines. The project manager should ensure that the schedule of preparation of key design deliverables is supported by a schedule of interdisciplinary reviews.

### **Specialist HSE input**

The size and scope of a project will determine the need for full-time specialist advisors in the field of HSE. Where full time HSE staff are not included the detailed project plan, showing the specific HSE studies planned, should be agreed with the OPU / JV HSE department to ensure that resources (internal or external) will be available.

In cases where it is proposed to carry out detailed HSE studies using external contract resources, specialist in-house HSE resources should be consulted regarding:

- the choice of contractor

- the scope of work
- study outputs and evaluation criteria
- selection of input data and study assumptions.

### 3.3.2 **Management representative**

Within the design phase of a project, significant quantities of work are often undertaken in a contractor's office. A client representative should be nominated to be the focal point for overall contractor - client communication. He should be made responsible for monitoring and ensuring client verification and approval of HSE issues e.g. deviations from standards, design changes etc and for verifying that the necessary interdisciplinary communication is taking place within the contractor's design team to ensure an integrated approach to the management of hazards. It is his contractor counterpart who should ensure execution.

### 3.3.3 **Resources**

The resources required are a function of the project scope size and complexity, the geographical spread of the individual work packages, and the selected contract strategy. In respect of HSE, the resources required should be mapped out after development of the overall project schedule which clearly identifies the individual studies, reviews and deliverables throughout the design phase.

### 3.3.4 **Competence**

It is fundamental to HSE management that people required to plan and execute HSE critical activities are competent - competency being achieved by a combination of theoretical knowledge and practical experience. Detailed guidance on the assurance of competency is given in PTS 60.0304 HSE Competence Assurance. In relation to design, this issue is likely to be of most relevance during the selection of contracting organisations and specialist consultancy services.

The best indicator of competence is the successful execution of similar previous work and studies. It should be noted however that guarantees of competency are not provided just by the selection of a 'reputable' company or contractor. That reputation has been achieved by the work of specific individuals, and therefore the CV's of nominated individuals should be screened. In times of high demand for the contractor's services there may be a temptation to substitute the individuals proposed by less qualified and experienced staff. The possibility of awarding a contract subject to the availability of named individuals should be investigated.

### 3.3.5 **Contractor HSE management**

As noted above a large part of design activities are normally executed by contractors. The selection of a suitably resourced competent organisation is therefore critical.

The formal links and reporting relationships to the client should be clearly defined at

the outset of the contract and internal quality control procedures should be one of the first agreed deliverables.

These should include formal procedures for:

- approval and release of accredited personnel
- design check and review
- interdisciplinary checks
- deviation and change control
- drawing and document registers and controls
- agreed authority levels for sign off
- the specific routing and authority levels for client review and approval of specific deliverables.

### **3.3.6 Communication**

Within the design phase the basic data, assumptions, and system descriptions are undergoing gradual evolution as the level of engineering becomes more detailed. It is therefore essential that the updated status of the information is clearly communicated across the project organisation. Interdisciplinary and inter-functional mis-communication is frequently the cause of HSE problems that come to light later in the development. Similarly the later transmission of information to the eventual Asset Holder needs to be considered early. The quantity and format of data needs to be defined and agreed in order to avoid the rework associated with the conversion of project databases.

### **3.3.7 Documentation and its control**

Design generates a substantial number of documents and data which can be divided into three broad categories:

|                |                                                                                             |
|----------------|---------------------------------------------------------------------------------------------|
| <b>Input</b>   | Legislation, Philosophies and Policies, Standards, Corporate Guidelines.                    |
| <b>Control</b> | Internal procedures - defining how the work is conducted.                                   |
| <b>Output</b>  | Engineering deliverables, calculations, drawings, MTOs, procedures, Safety (HSE) Case, etc. |

For all control and output documents a custodian list should be developed and an archiving system put in place to maintain an auditable trail of revisions.

### **Regulatory and Legal Requirements**

Early in the project the existence of national or regulatory requirements which have a potential impact should be identified and the initial project plan should clearly list the public bodies having jurisdiction over design, construction and operation.

These requirements will form the minimum mandatory acceptance criteria. As such they should be reviewed to identify any specific deliverables (e.g. Environmental Assessment, HSE Case) and the project plan should include milestones for the delivery of these.

### **Philosophies**

In order to provide a clear framework for the engineering of facilities, a number of high level objectives and philosophies should be explicitly documented early in the project. These include:

- Operating philosophy
- Sparing philosophy
- Maintenance philosophy
- Fire and Explosion Strategy (FES)
- Security philosophy.

These strategies and philosophies together with their objectives and performance criteria become part of an HSE Case for an installation or operation. Further information on the FES is provided in Appendix I.

### **Standards**

PETRONAS projects should conform to the standards prevailing in the Group. Where regulatory standards are more stringent then they should augment the PETRONAS requirements.

Standards form the primary source of reference during the project, and also partly the criteria against which the project may be assured. Care should be taken in the selection of standards to ensure that they are relevant and applicable.

The principles set by the Standardisation Spearhead should be followed - i.e. adoption and adaptation is preferable to creation. Where possible international standards should be specified, amended only where necessary to reflect local circumstances and Group experience. The following hierarchy is applicable:

**Industry standards** National, international and industry standards (e.g. ISO, API, BS)

### **PETRONAS Standards**

Standards such as the PETRONAS Health, Safety and Environment Committee (PHSEC) standards, PTS, EDPs, PQAIR (PETRONAS Quality And Inspection Requirements).

### **OPU / JV standards**

OPU / JVs may have standards which reflect local operating conditions

### **Contractor standards**

Specialist contractors may require their own standards or they may be more applicable than OPU requirements.

The standards and procedures to be applied during the project should be clear and auditable. Having agreed the suite of project standards it is accepted that there will be occasions when deviations are deemed applicable. A procedure and set of authorised signatories for the deviations shall be created. In addition, a log of deviations should be maintained.

### **Acceptance Criteria**

A project may be judged on its success in meeting its declared HSE objectives. As the project progresses, the overall objectives should be increasingly refined to provide lower level measurable objectives for individual elements of the design.

Details are provided in PTS 60.0303 Documenting a HSE MS of how to formulate acceptance criteria.

### **Health, Safety and Environment Management System and the HSE Case**

The OPU / JV HSE MS defines the policy, objectives, organisation responsibilities, standards and procedures, business processes and controls that are required to manage HSE. Documentation of this management system forms the HSE MS Manual. As such the HSE MS should provide guidance on the steps necessary to ensure that the risks within a facility are ALARP.

The primary HSE output document of a project is the HSE case new or modified for the facility.

The HSE Case is the documentation of the HSE MS to a site-specific installation or operation. The HSE Case also provides a comprehensive description of the hazards and effects associated with the particular installation or operation, and the means by which they have been assessed and controlled. It also details emergency preparedness and contingency planning aimed at safeguarding life, the environment and the asset as well as recovering from any emergency situation that may occur. The Case concludes with a Statement of Fitness, demonstrating that all potential hazards and effects have been evaluated and measures have been, or will be, taken to reduce the risks to the lowest level that is reasonably practicable.

The means of preparing the HSE MS, and the HSE Case complete with a recommended format are described in PTS 60.0303.

### 3.4 HAZARDS AND EFFECTS MANAGEMENT (HEMP)

#### 3.4.1 Overview

As noted in PTS 60.0401, the process of Hazards and Effects Management (HEMP) comprises five steps to minimise risks to Health, Safety or the Environment:

- systematically identify hazards, threats and potential hazardous events
  - what can go wrong?
- evaluate (assess) the risks against accepted screening criteria, taking into account the likelihood of occurrence and severity of the consequences to people, assets and the environment
  - how likely is it to occur?
  - how serious is it?
- Record the significant hazards and effects
  - document the findings implement suitable risk reduction measures (control and mitigate)
  - can the hazard be eliminated or controlled?
  - reduce the probability of occurrence
  - reduce the consequences
- plan for recovery in the event of a loss of control
  - what measures are required if the hazard occurs?

#### 3.4.2 HEMP in design

Design and engineering, includes the following major activities and deliverables.

**Prepare conceptual** Carry out all activities concerning project technical scope definition in design sufficient detail to allow the preparation of the firm budget proposal.

This activity includes the following sub-activities:

**Make Basis for Design**  
**Produce Conceptual Design**  
**Compile Project Specification**

**Prepare detailed design** Carry out all discipline and inter-discipline activities necessary to prepare the detailed design of new or modified facilities or for facilities decommissioning.

The HEMP in design is based on the systematic identification and assessment of potential hazards and effects, and the subsequent definition of suitable control and recovery provisions. The activities within design are a continuation of the work that

will have commenced earlier in the project development. The earlier HEMP activities will have focused on the high level identification and assessment of hazards and effects, and their minimisation by overall concept selection, e.g. by use of HAZID, see PTS 60.2004 HAZID. The activities within the phases described above consist of the more focused application of the HEMP process. Control provisions can be hardware or administrative/procedural controls. Inherent or passive control mechanisms being preferred to active or procedural measures.

Recovery provisions are implemented to mitigate the consequence of hazardous events. Again the emphasis is on applying inherent and passive techniques where possible.

A summary of the HEMP process and the associated tools and techniques is contained in PTS 60.0401.

The detailed application of HEMP in design is described throughout the remainder of this document within the following chapters:

**Chapter 4 Identification and assessment of hazards**

**Chapter 5 Control of hazards**

**Chapter 6 Recovery preparedness.**

### **3.5 PLANNING AND PROCEDURES**

#### **3.5.1 General**

The foundation for the successful application of HSE MS, is a detailed plan which integrates the various steps of HEMP into the overall project schedule. PETRONAS Technical Standards (HSE) gives details of the available hazards and effects management tools, reviews, studies, methodologies and their associated objectives, scope, timing and deliverables.

The cost, time and resources required for HSE management must be fully integrated into the overall planning. The project plan should specify the milestone points at which HSE studies and activities (e.g. reviews, audits, HAZOPs, QRA, EA) are required. Sufficient allowance must be made in the project schedule to incorporate the accepted recommendations arising from such activities.

#### **3.5.2 Asset integrity**

Activities undertaken during the design phase are aimed at specifying a facility or asset that has a defined level of technical integrity. The activities within the construction and commissioning phases will ensure that the appropriate tests and checks are carried out to confirm that this integrity has been achieved. During its operational phase the asset must be operated and maintained within the designed operating envelope. In summary design creates technical integrity and operations safeguard technical integrity.

In specifying the facility during the design phase it is recognised that it is not appropriate to provide hardware for all eventualities (including low probability events) and that in many cases the controls in the operational phase will be procedural/competency controls, not hardware.

It is therefore crucial to the operation of the facility that the assumptions and design rules selected are explicitly documented and passed on to the operations phase in a readily usable and understandable format. The key deliverables that contain this essential asset integrity information are the Operations HSE Case (particularly with respect to the Hazards and Effects Register) and its associated Manual of Permitted Operations (MOPO). The MOPO defines the level and numbers of barriers installed initially and the recovery preparedness measures to be in place and the limits of safe operation if the barriers and/or recovery preparedness measures are reduced or removed.

Of particular importance is the management of corrosion and its relationship with inspection. This needs to be defined in the HSE Case.

Further details are contained in PTS 60.0303 Documenting an HSE Management System and HSE Cases.

### **3.5.3 Procedures and work instructions**

Details are given in 3.3.5 of those areas of the design activity for which formal control, monitoring and authorisation is required. The adherence to these procedures should be the subject of regular review and audit.

### **3.5.4 Management of change**

At the end of the Basis for Design and conceptual design the documents produced should be 'frozen', and any subsequent changes subject to a formal change control procedure. Prior to freezing the documents, considerable resources will have been spent in creating technical integrity. The simplest, smallest and cheapest changes can have the effect of destroying technical integrity. The formal change system should include the effect of the changes on technical integrity, as well as cost, schedule and contractual impacts.

### **3.6 IMPLEMENTATION AND MONITORING**

#### **3.6.1 Activities and tasks**

The activities and tasks carried out within design are essentially intellectual in nature. The nature of the work is such that it relies heavily on professional competence and the application of good practice, supported by codes, standards and analysis techniques. Whilst detailed engineering itself cannot be easily regulated by procedures, overall control guidelines should be in place to regulate the checking and authorisation of the output. In order to ensure interdisciplinary communication, regular cross-discipline reviews should be scheduled.

#### **3.6.2 Monitoring**

A formal system should be in place for assuring the HSE aspects of design. This should apply to the development of drawings and specifications and to the verification of calculations.

A minimal level of assurance will normally require at least the following three signatures:

- the person preparing the document
- a supervisor who checks the work
- the project manager, or his designate, who approves it.

The procedure should be formalised, and the listing of authority levels kept up to date.

Where work is carried out by consultants/contractors, the provision of internal QA procedures should be specified in the contract. A schedule should be agreed to regularly review the system and ensure it is being followed.

#### **3.6.3 Records**

Procedures should be established to ensure the integrity, accessibility and control of HSE critical documents and records. The control of these documents should form part of the contractors QA procedures. In addition a policy should be established as to which documents to archive, and for what period.

### 3.7 ASSURANCE

#### 3.7.1 Assurance

During the design a programme of assurances should be conducted to ensure that the control processes described above are being effectively implemented. Where design activities are being undertaken by a third party, control measures and associated QA procedures should be a requirement under the contract. Assurance of those agreed procedures should be a contractual right.

PTS 60.0301 HSE Assurance Guideline gives more detailed advice on the application of assurance techniques.

#### 3.7.2 Assurance action and feedback

Action items will be generated by the various assurances. A system should be set up to ensure that there is an assurance trail from an initial recommendation, to its final close out.

Periodic reviews of the action log should be undertaken to ensure that the system is working effectively and that sufficient detail is being recorded. It is not sufficient to record comments such as 'done, checked, rejected, etc' in response to action items. The system should record reasons for rejection, references to checks made and conclusions and references to the action implementation, e.g. drawing revisions, etc.

### 3.8 REVIEW

#### 3.8.1 Review

In the same way that the control measures are subject to periodic review, so the technical development of the facility should be subject to reviews at agreed milestones.

Whilst a number of these will be internal interdisciplinary reviews, it is essential that a number be conducted with a degree of independence. The resources to conduct the independent reviews can be:

- a separate Project Group (peer review)
- Central Engineering Function
- PETRONAS.

The role of review is described in PTS 60.0101 HSE Management System Manual.

#### 3.8.2 Feedback from reviews

Experience gained from the development of a design and the reviews of the design should be available for future projects in quality close-out reports.

Sections describing the design should be written on completion of the design phase not on completion of the project.

#### **4. IDENTIFICATION AND ASSESSMENT OF HAZARDS**

##### **4.1 HAZARD IDENTIFICATION**

The starting point in any HEMP is Hazard Identification. Failure to identify potential hazards and effects, or identifying them too late in the development cycle may lead to failure to implement control measures, or to the provision of inefficient control measures (e.g. a hazard has to be controlled over the operational life of the facility by procedures, whereas hardware could have been provided).

At the commencement of design, there should be an initial listing of high-level hazards and environmental effects as a result of a Hazard Identification (PTS 60.2004 HAZID) study and an Environmental Aspect Impact Assessment (PTS 60.3202) conducted during the feasibility stage of the project. During the conceptual design, this identification process is taken to a finer level in order to allow detailed assessment and the provision of control measures at a detailed level.

Hazard Identification can be assembled from a number of sources:

- experience
- checklists
- codes and standards
- structured review techniques.

##### **4.1.1 Experience**

It is possible to identify a large number of hazards and effects from the experience of personnel. Some hazards are obvious, but others less so. Success in identifying the less obvious is a function of individual experience, operational input from existing facilities, and the ability of the organisation to document the lessons from previous incidents/accidents. Whilst single events are often easy to envisage, those events which present hazards in combination with others are less easy to foresee.

##### **4.1.2 Checklists**

A number of checklists can be developed to aid the Hazard Identification process. The potential danger of checklists is that they encourage a 'tick off' mentality and stifle the search for issues not covered by the lists. Equally, as with 'experience', they do not deal effectively with hazards that arise from interactions.

### 4.1.3 Codes and standards

### 4.1.4 Structured review techniques

Codes and standards are the collective knowledge of many years of operating experience. As such they are focused examples of HEMP for a defined area or piece of equipment.

To overcome the limitations of individual experience, and checklists, a number of structured review techniques have been developed:

- HAZID (HAZard IDentification), PTS 60.2004
- HAZOP (HAZard and OPerability study), PTS 60.2209
- SAFOP (SAFety and Operability study)
- EAIA (Environment Aspect Impact Assessment), PTS 60.3202
- HF (Human Factors Analysis), PTS 60.0103
- HRA (Health Risk Analysis), PTS 60.1400

The above are not restricted to identification but include assessment.

#### **HAZID**

HAZID is a methodology for the early identification of high-level hazards. The technique is based on a set of guidewords in a team brainstorming process. The methodology is directed towards the earliest stages of project development where major directional changes can be made to the project.

It is suitable for application during concept selection, and equally for review of basic development concepts when the following level of information is normally available:

- operations philosophy
- sparing and maintenance philosophy
- process flow schemes
- preliminary layouts
- fire and explosion strategies.

The methodology is described fully in PTS 60.2004. This study will normally have been performed in the feasibility stage and provides a basis for hazard identification during conceptual design.

#### **HAZOP**

A HAZOP study is the most widely accepted and powerful of the hazard

identification tools available for reviewing the design of process facilities and, if used properly, can overcome many of the shortcomings of process design checks alone.

The HAZOP study is undertaken by a multi-disciplinary team. The team considers for each element of the design possible deviations from the design intent to determine whether appropriate means of protection have been provided. The study is structured around simple guidewords which are used to prompt the team to identify deviations. The HAZOP technique can be used for any flow process (as reflected in a flow diagram) or a sequential procedure.

All new 'greenfield' and 'brownfield' projects should be subjected to Project Definition and Design Freeze HAZOPs. Pre-startup and procedural HAZOPs may also be used in critical areas. Depending on their complexity, change proposals may also be subjected to a HAZOP.

It should be emphasised that HAZOP is to be used in addition to, and not in place of, conventional design checks. It is used after these conventional checks have been carried out.

Full details of the methodology, scope, timing, and team composition are included in PTS 60.2209

### **SAFOP**

For projects involving complex electrical power generation, transmission and distribution systems a SAFOP study may be performed. The SAFOP method is broadly similar to a HAZOP although different deviation prompting lists are used. The objectives of a SAFOP are to:

- identify potential hazards to personnel in the vicinity of electrical installations or instrumentation systems
- provide a critical review of both network design and plant; and assess any limitations and their effects on operability and security of the system
- analyse tasks and procedures set for operators, assess facilities and recommend measures to avoid operator error.

A full description of the methodology will be provided in a Future PTS. In the interim further details may be obtained from PETRONAS electrical engineers.

### **EAIA – Environment Aspect Impact assessment**

The objective of an EA is to predict the significant chemical, biological and socio economic aspects of an activity and to make recommendations on activities, sites, techniques and technologies to be adopted in order to maximise the positive and minimise the negative effects. Within the EA an environmental description is developed and the potential environmental hazards and effects identified in order to determine any environmental control and recovery provisions necessary.

Full details of the methodology, scope, timing, etc are included in PTS 60.3202

## **HF - Human Factors**

HF considers ergonomics in design, see PTS 60.0103

## **HRA - Health Risk Assessment**

HRA considers health risks. PTS 60.1400 guides on Chemical Health Hazards (Refs. 2 and 3).

## **4.2 HAZARD ASSESSMENT**

### **4.2.1 Overview**

#### **General**

Having identified the scope of hazards and effects, the next step in the HEMP is Assessment. The assessment techniques should consider the following:

- the effects on the health and safety of personnel
- effects on the environment
- risk to assets and production
- effects on reputation
- the cost effectiveness of risk reduction measures.

#### **Assessment Techniques**

Some of the above issues cannot be quantified; those that can may still carry considerable uncertainty. Therefore, decision-making guidelines have to contain a large element of management and engineering judgment. What is possible, however, is to ensure that the best available knowledge is presented to the decision-maker in a useful, complete and concise manner. The decision-maker must be made aware of what is fact, what is judgment and the nature, direction and magnitude of uncertainty. The two most common types of decisions required are:

- (i) whether a facility is safe and environmentally acceptable to operate, or an operation safe to carry out
- (ii) whether an HSE improvement can be justified.

Just what constitutes a 'safe design, a 'safe operation' or a 'justifiable HSE improvement' is not something that can be simply described. Individual judgment is inevitably a major factor. However, what is often called 'judgment' is usually supported by different levels of evidence appropriate to the scale of the issue.

Broadly speaking, the supporting information can be split into four categories:

| <b>Evidence</b>      | <b>For comparison with</b>                       |
|----------------------|--------------------------------------------------|
| Engineering judgment | Codes, standards, objective argument (4.2.2)     |
| Qualitative analysis | Goal setting criteria (4.2.3)                    |
| Consequence analysis | Physical parameters, acceptance criteria (4.2.4) |
| QRA                  | Options, risk criteria (4.2.5)                   |

r approaches form a hierarchy of evidence. The vast majority of issues should be resolved at the first level (engineering judgment) with a gradually reducing number requiring additional analysis.

#### **4.2.2 Codes and standards**

For well understood hazards and effects, there will often be existing codes and standards that specify recognised means of control. Compliance with accepted national, international or industry codes and standards will in many cases be sufficient. This does not imply that they should be followed 'blindly'. Intelligent analysis of the problem and sound engineering interpretation of the standards are required to prevent gross over/under specification of control measures or to identify unusual circumstances not (adequately) covered by them.

Many of the new generation of standards have moved away from a prescriptive approach, to one of goal-setting objectives. Greater emphasis is given to inherent safety, i.e. designing out the hazard. Also recognised is the fact that there may be several means of providing the same protection and that providing many 'layers' of protection may be difficult to justify.

The approach in these cases is to undertake the analysis. Then, with a better understanding of the consequences of the hazardous event, the most appropriate (cost-effective) means of control or mitigation may be selected.

#### **4.2.3 Qualitative analysis**

In some cases it may be possible to demonstrate on the basis of probability alone that no action can be justified. In these cases it is not necessary to evaluate the consequences because the event itself is so unlikely. It must be appreciated, however, that even though the event is of low probability it might still happen. It is on these grounds that oil installations are not protected, for example, against impact from falling aircraft or meteorites.

#### **4.2.4 Consequence analysis**

##### **General**

If it can be demonstrated that a hazard is adequately controlled even under a worst case scenario, it may not be necessary to evaluate all possible (i.e. less severe) outcomes. This is especially relevant in the design of onshore facilities where less

space constraint mean that layout can readily cater for maximum credible events. This approach should, however, be treated with caution. A fire resulting from a release from a large diameter hole may be a less severe case than that from a smaller leak. In the first case the pressure, and hence the flame length, decline rapidly. In the latter case the flame length remains more constant and may impinge on a structural member for longer.

In order to evaluate physical effects associated with hydrocarbon events a number of physical effects models have been developed within the Group. Physical effects modelling is described in detail in PTS 60.2211.

Methods are available for predicting the scale of leaks, fires and explosions. These predictions are for various single fire incidents and relate such factors as pressure, leak size and vessel inventory to, for instance, thermal radiation and overpressures.

#### **Effects of gas leaks and fires (not to use FRED model)**

The SHELL suite of programmes - FRED (Fire, Release, Explosion and Dispersion which is available from SHELL) provides a suitable method for calculating the magnitude of leaks from process equipment, the dispersion of released hydrocarbon vapors and the flame shape and associated radiation due to any ensuing fires. (PETRONAS is not using FRED. Insert PETRONAS equivalent here)

#### **Explosion Overpressures**

There are no simple prediction programs for explosion overpressure. Thornton Research Centre, United Kingdom (TRC) has developed methods for both confined and partially confined explosions. The programme SCOPE can be used to give reasonable predictions of overpressure in enclosed modules but does require major simplifying assumptions about the shape and position of equipment within the module.

For onshore plant a method is given in the FRED suite of programmes which can predict the scale of explosion overpressures. Further research work is ongoing to develop more accurate methods for confined and semi-confined explosions.

### **4.2.5 Quantitative Risk Assessment (ORA)**

#### **Overview of the Method**

QRA provides a structured means for assessing risk and expresses this numerically. The technique is fully described in PTS 60.2210.

QRA of process-related events usually commences with the identification of initiating events for complex accident scenarios. Formal analytical methods, such as fault and event trees, are used to show the relationships between initiating event, affected systems and final outcomes. The frequency of the initial event is estimated, usually using historical data. The probabilities for the subsequent branches in the fault or event tree are taken from historical data, modeling or expert judgment. The

final outcomes will be expressed as a frequency of occurrence and a measure of the consequence of that particular scenario. The final outcomes may be summed to provide quantitative measures of risk for the range of scenarios considered. These measures of risk (the product of risk analysis) are then used to identify the main risk contributors and compare the relative effectiveness of risk reduction options.

The overall measures of risk used (which would normally also include day-to-day risks such as slips, trips and falls and transport) are Individual Risk of death Per Annum (IRPA) and, for specific installations and activities, Potential Loss of Life (PLL), Potential Loss of Asset and Potential Loss of revenue. For offshore installations, temporary refuge, escape and evacuation impairment frequencies may also be calculated. Onshore an estimate of risk to the public may be appropriate.

### **Application of QRA**

The use of QRA to improve HSE by comparing alternative designs or methods of operation is now widely used. It is considered a valuable tool in the decision-making process, providing a means to communicate, to quantify opinions and to combine these effectively with available historical data and experience.

In the industry, QRA has two main functions:

- to assist in the comparison of design and operating philosophy options with a view to effective and efficient HSE management
- to demonstrate when required within OPU / JVs and to third parties including the regulating authorities that risks are ALARP.

QRA may also be used in circumstances where:

- (combinations of) equipment or operating philosophy are intended that could not possibly have been anticipated by those formulating standards and practices (e.g. application of new technology or new combinations of existing technology); or
- it is agreed beforehand by the function that there are strong grounds for challenging standards and practices, e.g. on the basis of engineering judgment and reasoned evaluation.

QRA should not be used to justify a reduction in the level of HSE of current activities, and should not be used on a case-by-case basis to challenge accepted HSE standards and practices.

QRA is considered to be the best means of combining historical data, effects modeling and judgment in determining the likelihood and consequences of accidents. It should present the best knowledge available and decisions based on it will generally be better than those based on subjective assessment.

PTS 60.2210 Quantitative Risk Assessment describes the QRA technique in detail and provides advice on the use and misuse of the technique.

### **Scheduling of QRA in a project**

QRA is not always appropriate/applicable. For many onshore or simple facilities the application of the other assessment techniques described may be entirely suitable and sufficient for decision-making.

As noted in PTS 60.0104 Concept Development, the use of risk assessment early in project development can be extremely beneficial in the comparison of development options. A comparison of risks associated with, for example, onshore versus offshore processing, platform versus subsea installation, location of onshore installations, etc may be effectively studied by QRA.

During conceptual design, more detailed and focused risk assessment(s) may be undertaken to assist with final major decision-making with respect to design options and to provide a basis for further optimisation during completion of conceptual engineering.

At the end of detailed engineering, i.e. when all optimisation has been completed, the risk assessment may be issued in the form of a final report for input to the Operation HSE Case. This is intended to demonstrate that the risk criteria have been achieved, and that the risks can be demonstrated to be ALARP.

## **4.3 A FRAMEWORK FOR HAZARD IDENTIFICATION AND ASSESSMENT**

The flow scheme in Figure 4.1 gives an overview of the hazard management objectives for various phases of a development and some of the tools and techniques available. A summary of the referenced tools is given in PTS 60.0401 Hazards and Effects Management Process which in turn provides further references to detailed application.

The activities in the industry described below encompass the life cycle of an asset. The HSE Case which is prepared during the execution of these activities becomes the HSE Case for the asset and forms part of the Asset Reference Plan.

The broad HSE objectives are bulleted on the left of the table. Some of the tools and techniques available are listed on the right.

Figure 4.1 – Hazard Identification and Assessment – Tools and Techniques

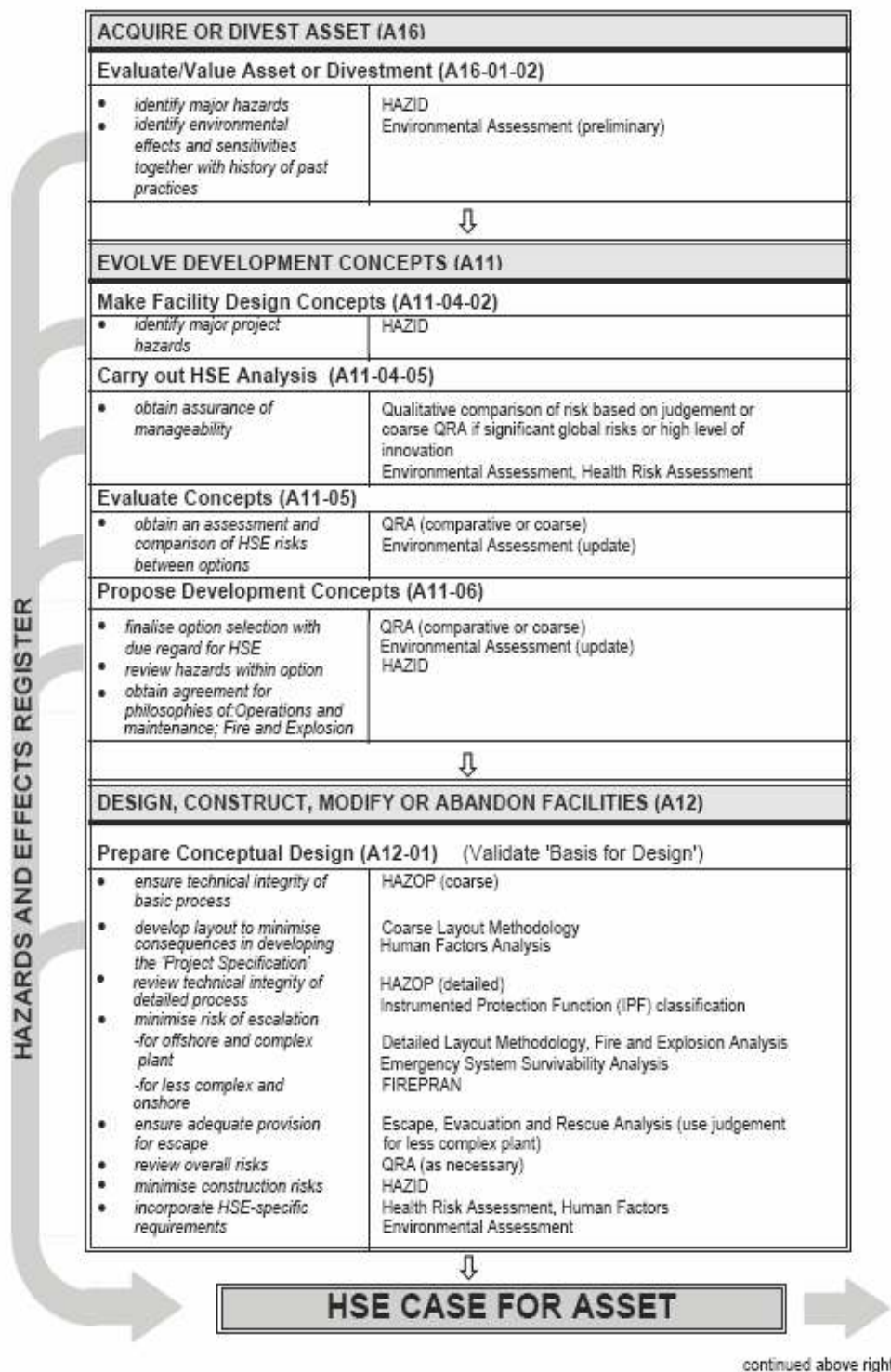
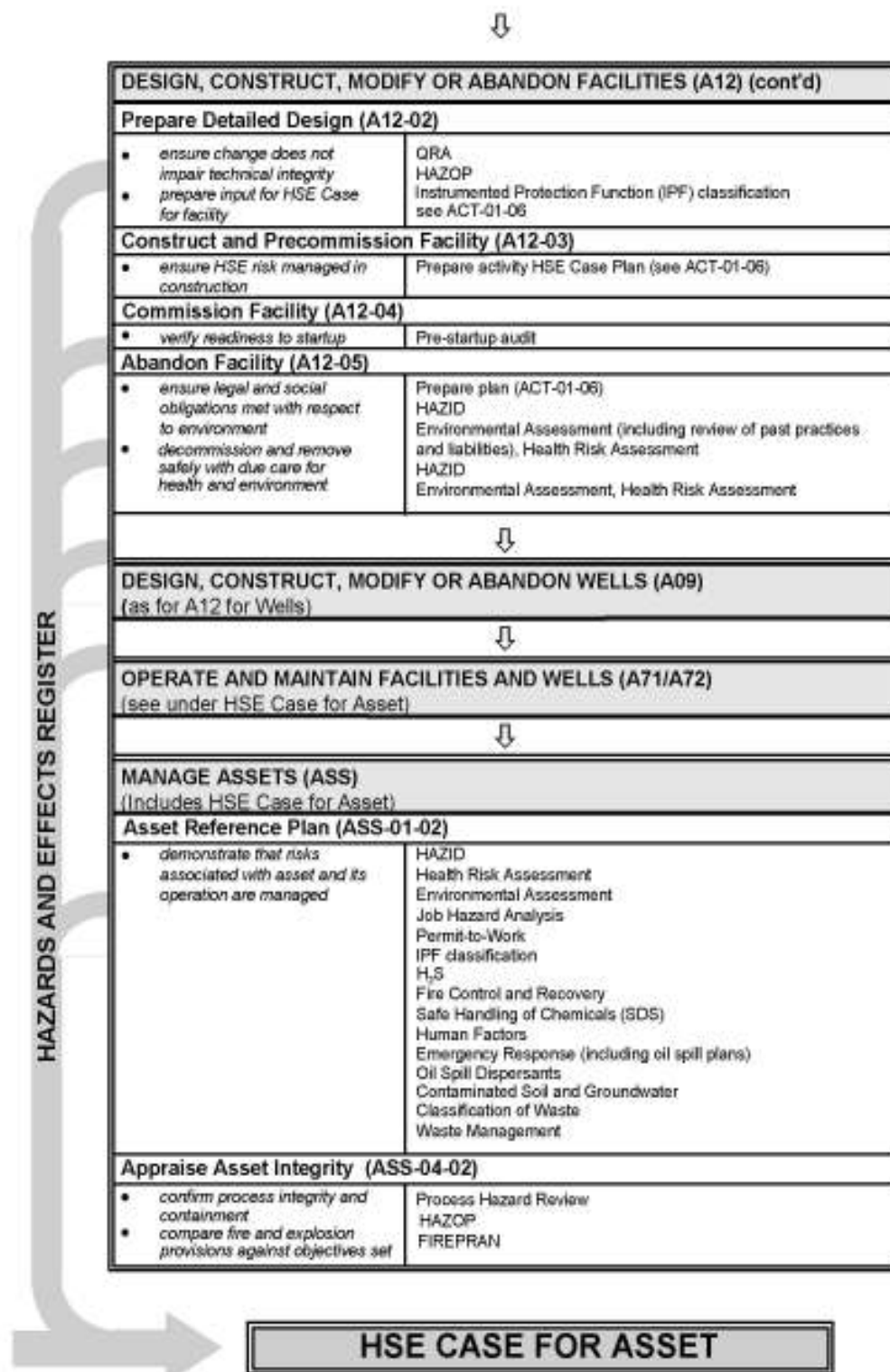


Figure 4.1 Hazard Identification and Assessment - Tools and Techniques (continued)



## 5. CONTROL OF HAZARDS

### 5.1 OVERVIEW

**Control** = Prevent the incident  
 = Reduce the probability of the incident

The optimum way of controlling hazards is to prevent hazardous events from occurring. The emphasis in design should therefore be on removing hazards altogether (inherent safety). If it proves impossible to remove the hazards completely, then efforts should be taken to reduce the probability of hazardous events occurring. This chapter contains an overview of the principles behind control techniques and their resulting benefits. Later in the chapter it explains in more detail how these principles are applied in the overall design of facilities and specific equipment.

The principles consist of:

- design for ease of operation and maintenance
- substitution of hazardous materials
- reduce inventory of toxic/hazardous materials
- simplify the process (e.g. eliminate equipment, minimise probability of error)
- eliminate sources of ignition
- minimise the probability of loss of containment
- reduce pressure
- reduce temperature
- reduce volatility.

#### 5.1.1 Design for ease of operation and maintenance

A large proportion of the incidents occurring on facilities occur as a result of operator error, or during maintenance. The root cause of these incidents, however, can normally be traced back to missed opportunities or oversights during the design phase where the potential exists to make the plant more operator- and maintainer-friendly and tolerant, thus reducing the probability of incidents occurring. The key factors to address include:

- simplicity of process configuration
- transparency of control
- adequate provisions for process isolation
- good access to all equipment
- design provisions for non-routine operations
- provision of appropriate lifting devices.

#### 5.1.2 Substitution

The most direct way to achieve inherent safety in a process is to substitute hazardous with non hazardous materials, e.g.:

- replacing combustible components with non-combustible components (e.g. replacing a hot oil heating system with a tempered water system)
- replacing toxic components with non-toxic components.

### **5.1.3 Reduce inventory of toxic/hazardous materials**

Reduction in the inventory of flammable or toxic material will reduce the potential magnitude of a release for a given event.

- isolating valves should be specified between multiple vessels/tanks and they may be separated by fire breaks or fire walls (see ESD valves)
- consideration should be given to using different equipment types to reduce inventory (e.g. using packing rather than tray internals in columns or thermosyphon rather than kettle reboilers)
- the size of process vessels and storage tanks containing hazardous material should be reduced if viable. This should be balanced against the increased number of leak sources introduced
- the surface area of a liquid spill that could be exposed to a fire should be minimised to control burning and to prevent escalation. Liquid surface area should be reduced by incorporating intermediate walls in multi-tank bunds
- the use of gas-powered systems should be minimised, particularly in manned areas (e.g. electrical systems should be used for heating and cooking rather than bottled LPG).

### **5.1.4 Simplify the process**

The process should be as simple as necessary to achieve the production objectives (i.e. yields, product specifications and export conditions). Justification for additional equipment (e.g. to increase yield or efficiency) should take account of any increased HSE risks in addition to the normal cost benefit considerations. The following points should be considered:

- consider the provision of single train facilities (which increases plant simplicity) within the constraints of availability requirements
- avoid the use of crossovers between sections of plant

These can cause confusion during maintenance and increase the complexity of the control and shutdown logic.

- set the pressure profile of the process with the aim of minimising items of rotating machinery. For instance:
  - transfer liquid by gravity (rather than pumping)
  - specify the operating pressure of low pressure gas sources at the required fuel gas pressure.
- specify equipment that is proven in a similar operating environment (ideally within the OPU)
- minimise use of complex or nontraditional unit operations which may be difficult

- to understand or may require high levels of maintenance
- minimise the potential for onstream maintenance within the constraints of the availability requirements.

#### **5.1.5 Reduce probability of loss of containment**

- provide adequate overpressure protection
- specify realistic design margins on capacities and performance requirements
- select material to minimise corrosion
- provide appropriate mechanical design (e.g. minimise flanges, small bore and screwed fittings, use effective seals)
- provide protection from mechanical damage by mechanical barriers, layout or shutdown
- provide assurance of operation within the design envelope
- specify a robust and transparent process control system.

#### **5.1.6 Eliminate sources of ignition**

Where possible ignition sources should be eliminated from the plant, for instance:

- replace fired heaters with electrical heaters or waste heat recovery units
- eliminate rotating machinery where possible
- import electrical power (rather than generating on site)
- reduce the temperature of the process
- minimise the number of junction boxes.

#### **5.1.7 Reduce pressure**

Reducing the operating pressure of a process is desirable, because:

- the mass per unit volume of hydrocarbon in the vapour phase is reduced
- the leakage rate of fluid through a fixed orifice is smaller
- the energy released from a catastrophic failure of a piece of equipment is lower
- there is a reduced chance of hydrate formation
- emergency depressurisation can be achieved more readily
- the likelihood of over pressuring low pressure downstream systems is reduced.

The designer should examine ways of reducing the operating pressure in the process. The optimum solution should be ascertained by trading off the benefit to safety against any increased expenditure.

### 5.1.8 Reduce temperature

Reducing the operating temperature of a process is desirable, because:

- lower proportion of vapour generated from a volatile liquid, giving a reduced spread of vapour from a leak
- reduced propensity for temperature-related material failure problems (e.g. metal creep or hydrogen embrittlement)
- safer heating systems are feasible (e.g. pressurised water instead of hot oil)
- reduced utilisation of energy
- reduced corrosion rate
- reduced risk of unwanted heating of the environment (e.g. in cooling water discharge lines)
- lower risk from problems associated with thermal expansion.
- less risk of personnel injury from hot surfaces.

The designer should examine ways of reducing the operating temperature in the process, e.g. by using reduced pressure in conjunction with reduced temperature to meet a TVP specification.

### 5.1.9 Reduce volatility

Reducing the volatility of the constituents reduces the likelihood of a hydrocarbon release escalating. The volatility of fluids can be reduced by:

- reducing temperature and pressure
- adopting a balanced approach to recovering NGLs from a gas stream particularly in offshore locations
- reducing the vapour pressure of stored LPG products by specifying refrigerated or semi-refrigerated storage
- ensuring that incoming liquids from other facilities are stabilised to a satisfactory TVP.

## 5.2 GENERAL SYSTEM DESIGN CONSIDERATIONS

### 5.2.1 Overview

Application of the principles outlined above to specific types of equipment are covered in 5.3. A number of the principles are, however, sufficiently general, or are applied at the system design level, to be covered here generically.

In oil and gas facilities the most hazardous events are those related to loss of containment. The principal causes of loss of containment are:

- operator error
- excursions of the process outside the design envelope.
- corrosion/erosion
- third-party activities.

## 5.2.2 **Operability and maintainability**

A large proportion of the incidents occurring on oil and gas facilities occur as a result of operator error, or during maintenance activities. The root cause of these incidents, however, can normally be traced back to miss opportunities or oversights during the design phase where the potential exists to make the plant more operator- and maintainer-friendly and tolerant. This section is concerned with reducing potential hazards relating to the human interaction with the plant during production and maintenance operations.

### **Simplicity/Transparency of Plant**

The potential for errors during operations and maintenance is greatly reduced with simple plant whose function, status and interconnectivity are transparent to all.

Preference should be given to minimising the number of trains and reducing the degree of interconnectivity between the system elements. The control system should be designed with maximum operator involvement to ensure that information is presented in a manner that is clear and concise.

A logical naming and numbering system should be adopted for equipment and this should be reflected in the layout. For example, a set of identical pumps (three operating/one standby) should be oriented in the same sequence as the numbers to avoid confusion during maintenance operations. Particular care should be taken in numbering equipment that is retrofitted at a later date.

The provision of a plant colour code system for piping greatly improves transparency and the requirement for a coding system should be included in the plant piping specification.

For safety-critical activities, physical mechanisms should be considered in the design which 'force' an operator to carry out tasks in the correct sequence, thus achieving a degree of inherent safety. Care must be taken not to introduce provisions which will become cumbersome. Such complexity may encourage unauthorised 'by-passing' with the consequence of increased risk.

### **Accessibility to Equipment**

During design the requirement for access to equipment should be reviewed. The following factors should be considered:

- access arrangements for all regular operations shall be straightforward and simple

These points shall be accessible and visible from main floors or aisles, preferably without the help of auxiliary platforms and ladders.

- where such platforms and ladders are required they shall be permanently installed

Portable ladders are not acceptable substitutes.

- equipment which requires attention on a less regular basis (e.g. scheduled maintenance yearly) need not necessarily be provided with permanent platforms and ladders unless emergency access is a requirement
- arrangements shall be made for all routine operations which involve handling and storage of materials and equipment

Permanent equipment (e.g. runway beams, hoists) should be provided for equipment that is critical to plant availability or requires regular attention.

- every instrument and operational checkpoint shall be so positioned that access and/or calibration is possible from permanent walkways, stairs or platforms PTS 32.37.00.33 should be consulted for specific advice on the mounting of plant instruments (Ref. 4).
- equipment parts, instruments, valve hand-wheels and piping shall not protrude into access ways
- normal entrance and exit points shall be located so as to enable easy access and egress to work areas
- in considering access, suitable provisions should be provided to prevent contact with hot surfaces

If applicable, all external surfaces of equipment and accessible piping operating at temperatures in excess of 70°C shall be provided with protection to personnel to prevent contact by personnel, (see PTS 30.46.00.31 Thermal Insulation for Hot Services Ref. 5). Where protection is provided solely for personnel protection preference should be given to shielding of all parts which are accessible during normal operation, rather than insulation to avoid corrosion under the insulation. Protection shall be provided for parts accessible by temporary maintenance platforms or scaffolding if it is the intention to provide such access while the equipment is hot. Warning signs and barriers shall be provided to prevent access to any hot equipment which is not provided with such personnel protection. On no account should asbestos be used as an insulating material.

### **Provisions for Non-Routine Operations**

Formalised operating and maintenance philosophies are developed during the preparation of the Basis for Design. These documents provide the operational framework for the design. At a detailed level the full scope of operational requirements and constraints should be reviewed to ensure that adequate provisions are made in the design to allow such activities as:

- hydro testing of equipment and pipelines
- black start
- startup following a manual shut-down
- startup following a Process Shut-down (PSD) or Emergency Shut-down (ESD)
- purging
- venting

- manual shutdown
- manual depressurising
- draining
- cleaning/desanding of vessels
- pig launching/receiving
- catalyst change-out (e.g. molecular sieves)
- well testing.

It may be necessary to develop and review the procedures associated with these activities at an early stage, typically in the Project Specification period, to ensure that the necessary hardware is specified on the PEFS (e.g. purge points, temporary flaring points). To do this the following factors will need to be established:

- modes of operation and flexibility required
- role of operators
- length of shift, manning pattern
- mechanical handling equipment to be used
- skills and experience of operators
- skills and experience of maintenance personnel.

Where simultaneous drilling or workover and production may take place sufficient space shall be available for pipe handling, mud handling, chemicals delivery, sludge removal and other well operations without interfering with production. The need for temporary lay down areas associated with maintenance activities e.g. space to withdraw heater tube bundles should also be considered.

Space shall be provided for the lay down of equipment during maintenance or replacement particularly for large items such as turbines, heat exchanger bundles and compressor shafts.

Sample points should be designed to allow safe operation. The requirements for sampling should be established at the design stage and sample points shall be readily accessible, have an easy escape route and be designed based upon a defined procedure. The design shall take account of the type of sampling equipment used and where necessary suitable overpressure protection shall be provided.

### **Isolation/maintenance philosophy**

A philosophy for isolation shall be developed that is consistently applied. Where possible the facility should be simplified by reducing to a minimum the number of individual units which may be isolated. Manifolding of spare valves, controls and equipment is not recommended and should only be considered where high availability is demanded which cannot be achieved in other ways.

The safest maintenance philosophy is one that allows work to be performed only when the plant, unit, or system has been shut down, isolated, depressurised to atmosphere, drained, and freed of flammable and toxic gas. When a total shutdown is not practicable, the design shall incorporate facilities to ensure adequate isolation of a

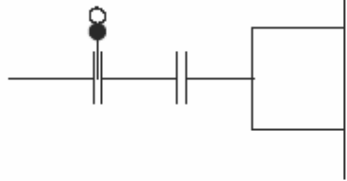
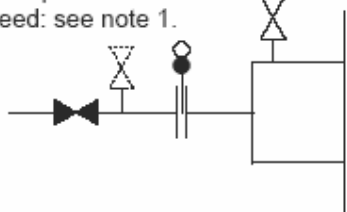
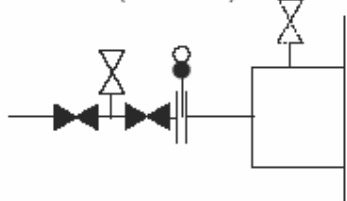
complete train or individual equipment. The isolation facilities shall be provided at the boundaries of the unit. This shall include not only main inlet and outlet lines, but also drains, vents, and other interfaces.

The design of the isolation requirements shall be the result of a task analysis of the actions required to isolate, depressurise and purge the system. This shall also take into account the service conditions (e.g. corrosive, fouling).

Except as noted below, isolation facilities shall include a means of 'positive isolation'. Positive isolation is achieved by fitting a blank, insertion of a spade or by rotating a spectacle blind. For hazardous service, flange bolts shall not be loosened unless it has been proven that the isolation valve or valves are containing the fluid or gas. If full expected activity to be performed and its likely duration. In cases where the work is relatively minor (and the expected duration short), the overall risk in performing the isolation and de-isolation (i.e. swinging and reswinging the spectacle) may be greater than the risks imposed in doing the actual work with only valved isolation for that short period of time. An example of this might be the simple change-out of a defective control valve with a replacement unit. Under no circumstances shall non-return valves be relied on to provide isolation of equipment for maintenance. This applies also to proprietary swing check valves with manual actuation since there is no way to check visibly if the internal parts of the closure mechanism have functioned correctly.

Recommended isolation provisions are indicated in Table 5.1

**Table 5.1 Recommended isolation requirements**

| System | System Description                                                                                                                                                   | Minimum Requirement                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| A      | Shutdown, depressurised and hydrocarbon free system.                                                                                                                 | Positive isolation by a spade or remove spool and install blind.<br> |
| B      | System in service, of ANSI class 600 and below .<br>For flashing liquids and toxics see C below.                                                                     | Single leak tight valve plus spade/blind.<br>Bleed: see note 1.<br>  |
| C      | System in service, of ANSI class 900 and above.<br><br>All systems containing toxic fluids (note 2).<br>Systems containing flashing liquids above ANSI 300 (note 3). | Double block and bleed plus spade/blind. (see 6.3.1)<br>            |

**Notes:**

1. A bleed connection should be installed between the valve and the spade/blind for line sizes 6" and above. The purpose of the bleed is to establish that positive isolation is achieved and to provide a means of draining or depressurising the volume between spade/blind and isolation valve. Depending on circumstances (including inventory and likely valve integrity), it may be appropriate to install bleed connection in lines less than 6".
2. For the purposes of this requirement, toxic in case of H<sub>2</sub>S is defined as more than 500 ppm H<sub>2</sub>S in the process stream.
3. The definition of flashing liquids for the purposes of this Table is that given for cat A fluids in Appendix B of the IP Code part 15 (Ref. 6).

Equipment in 'operationally critical service' may be subject to more stringent requirements than those given in this table. 'Critical' in this context means that a non-scheduled shutdown due to failure of the isolation would be unacceptable in view of economic or business loss.

The design shall take into account the operational consequences of an isolation valve failing to seal when required, and the chance of this happening. An example would be a pig receiver in a main trunk line. When for any reason the receiver cannot be properly isolated from the line, the economic losses due to downtime and/or line depressuring would be considerable. A pipeline isolation valve, which under normal conditions would never be operated, may be installed as an 'insurance premium' upstream of the normal receiver isolation. If there is an ESD valve in the pipeline, there may be a manual valve required on the pipeline side of it to allow repair of the ESD valve even though the normal isolation criteria here may not require such a double block-and-bleed.

An isolation design for a particular service must achieve a balance between increased isolation integrity and the risk from extra leak sources due to additional flanges, valves and bleeds.

### **Lifting Provisions - Manual Handling Aids**

Following the initial layout, a detailed study should be undertaken to analyse the requirements for manual handling facilities required for maintenance (e.g. removal of major items of equipment, electric motors, etc). Where the expected frequency of use is such that permanent lifting facilities (cranes, runway beams etc) cannot be justified the provision of padeyes should be considered to allow the use of temporary lifting equipment.

The normal operational swing zones of permanently installed cranes shall not pass over hydrocarbon-containing equipment unless this has been designed for impact resistance to loads dropped from the crane. Where such resistance has not been provided, crane use shall be limited to maintenance activities on the equipment after it has been depressurised and drained.

A review should be undertaken to identify any operational activities that involve frequent manual handling of appreciable loads (e.g. chemical stock replenishment, filter change outs, etc) and appropriate aids provided.

### **Working Environment**

Appropriate standards should be set for the working environment as this can be an important factor in the performance and health of operational and maintenance personnel. Factors to be considered are:

- noise
- vibration
- lighting
- climate (temperature, humidity, ventilation, weather protection) chemical and dust
- radiation (heat and radioactivity)
- cleanliness
- social amenities
- organisation of work (shift and leave patterns, working alone, variety, etc)

- chemical exposure.

### **Ergonomics and Human Factors**

Ergonomics and human factors aim at optimising the human-machine interface with respect to efficiency and safety by examining the design of products, tools and working methods (factors such as motivation, work stress and human relations are also taken into account).

The benefits which can accrue from an ergonomic design are:

- reduction in operator errors
- reduction in work load, fatigue and stress on the operator
- improved system performance/efficiency
- reduction in hazards for the individual worker and the general work environment.

PTS 60.0103 Human Factors describes in more detail the human-machine interface and describes the role of human factors engineering. The document introduces a number of tools and techniques that may be of benefit in minimising hazards and errors and improving efficiency and usability.

The application of these tools and techniques should be considered for:

- layout of control rooms and panels
- layout of normal and emergency controls
- analysis of the appropriate degree of automation
- determination of the extent of protective systems
- layout of valves and equipment where manual operations are envisaged
- determination of equipment layout for maintenance access.

In all of the above areas it is essential that the operators and maintainers are fully involved in the application of the tools and techniques.

Further guidance on the design of control rooms and control panels is given in 6.2.

#### **5.2.3 The design envelope**

The facility will be designed with a defined operational envelope. Suitable control provisions shall be installed to ensure that the normal operational range of the plant remains within that envelope and contingency provisions (overpressure relief etc) shall be installed to cater for any excursions beyond the defined envelope. In order to ensure the safe ongoing operation of the facility, the limits of that original design envelope need to be documented and understood by the operations personnel. As noted in 3.5.2 the development of a MOPO provides the vehicle for this knowledge capture and transfer.

### **Design Conditions, Specification Breaks**