

PETRONAS TECHNICAL STANDARDS

HEALTH, SAFETY AND ENVIRONMENT

GUIDELINE

DESIGN INTEGRITY (DI)

PTS 60.2206
JANUARY 2011



© 2011 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.

PTS Circular 2009



PTS No:	60.2206
PTS Title:	Design Integrity

This revision of **PTS 60.2206 – Design Integrity (January 2011, Revision 1)** has been updated to incorporate PETRONAS Lessons Learnt, Best Practice and new information issued by relevant industry code and standards. All updates in the document are highlighted in *italic* font.

The previous version of this **PTS 60.2206 (September 2006)** will be removed from the PTS binder/ e-repository from herein onwards.

The custodian of this PTS is: Manager - HSE MS, Standards & Regulations, GHSED.

Please direct any questions regarding this PTS to the above-mentioned.

Document Approval

	Name	Designation	Date	Signature
Prepared	Gusni bin Jabar	Principal, Safety Management Operations, Group HSE Division	10/2/2011	
Technical Approved	Morris Kho Kee Wae	Custodian, Safety Management Operations, Group HSE Division	10/2/2011	
Vented	Maureen Song Chai Kee	General Manager, Group HSE Strategy and Performance, Group HSE Division	11/2/2011	
Approved	Mohd Tarmizi Bin Munir	Head, Group HSE Division	14/2/2011	

Revision History

Date	Version	Description of Updates	Author
Oct '06	Original	-	-
Oct '09	Rev 1	Reformat as per PTS standard format	GHSED
Jan '11	Rev 1	Reformat as per PTS standard format	GHSED

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 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 standardization.

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, it is expected of 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 owner.

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

- 1) PETRONAS and its affiliates.
- 2) Other parties who are authorized 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 CONTENT

1.0	INTRODUCTION.....	6
1.1	DESIGN INTEGRITY	6
1.2	USING THE PTS	6
1.3	RELATIONSHIP WITH OTHER SYSTEMS	7
2.0	OVERVIEW	8
2.1	APPLICABILITY	9
2.2	AIM	9
2.3	EXPECTATIONS.....	9
2.4	LINKS WITH OTHER SYSTEM ELEMENTS	10
2.5	BASIS AND COMPATIBILITY	11
2.6	OVERALL ROLES AND RESPONSIBILITIES	11
3.0	DESIGN INTEGRITY FRAMEWORK	12
3.1	BACKGROUND	12
3.2	DESIGN INTEGRITY PHILOSOPHY	13
3.2.1	Risk Management	13
3.2.2	Compliance Assurance.....	15
3.2.3	Lifecycle View	15
3.2.4	Knowledge and Communication.....	16
3.3	RISK REVIEW PROCESS.....	16
3.4	DESIGN STANDARDS	17
3.5	SAFE OPERATING ENVELOPE	18
3.6	SAFEGUARDING MEMORANDA	19
3.7	KNOWLEDGE RETENTION AND COMMUNICATION PROCESSES.....	20
3.8	OTHER SUPPORTING PROCESSES	21
3.9	ASSURANCE & REVIEW	21
4.0	RISK REVIEW GUIDELINES.....	24
4.1	BACKGROUND	24
4.2	COST BENEFIT ANALYSIS	25
5.0	MANAGING CHANGES.....	26
6.0	DELIVERABLES FROM DI	26
7.0	PERFORMANCE MONITORING	27
7.1	MONITORING	28
7.2	ASSURANCE	28
7.2.1	Tier 1 - Compliance with DI Philosophy	28
7.2.2	Tier 2 - System Audit.....	28
7.2.3	Tier 3 - Corporate.....	28
7.2.4	Assurance Reporting	29

7.2.5	Action Tracking	29
8.0	RECORDS AND DOCUMENT MANAGEMENT	30
9.0	MANAGEMENT ACTIONS	30
10.0	GLOSSARY	32
	APPENDIX 1 – ASSRUANCE CHECKLIST FOR DI SYSTEM	38
	APPENDIX 2 – RISK ASSESSMENT TECHNIQUES.....	42
	APPENDIX 3 – SAFE OPERATING LIMITS.....	45

1.0 INTRODUCTION

1.1 DESIGN INTEGRITY

Objectives

This PTS covering Design Integrity (hereinafter referred to as DI) has been written to provide the guidance and tools necessary to develop and operate a system for managing the risks inherent in operating a process system. It follows and is aligned with the principles described in the PETRONAS Health, Safety, and Environmental Management Systems Manual (HSE MS Manual, PTS 60.0101).

This PTS provides:

- a reference for OPU/HCU and Project Managers needing guidance in implementing a DI process
- a description of methods which should be deployed and links to other documents and standards with guidance on their application.

Structure and Content

Refer to the Table of Contents for an overview of how this PTS is structured.

Format

This PTS is arranged in either hardcopy or softcopy format, which are available on the PETRONAS intranet for downloading and subsequent reference and usage.

User Base

Operating Procedures PTS users are expected to be OPU/HCU and Project Teams. The PTS will either serve as a reference for others to assist in the development of 'in-house' specific reference documents, or will be used as a first-line reference in the case of smaller organizations.

1.2 USING THE PTS

Language

In this document the recommendations for a course of action are made with varying degrees of emphasis. As a rule:

'shall' indicates a course of action with a required, mandatory status within the OPU/HCU. The English language equivalent or interchangeable term of "shall" is 'must.'

'should' indicates a preferred course of action.

'may' indicates a possible course of action

In this PTS document the collective expressions of PETRONAS are sometimes used for convenience in contexts where reference is made to the companies of the OPU/HCU in general. These expressions are used where no useful purpose is served by identifying the particular company or companies.

Application

Should any significant deviations be made from the guideline recommendations in this PTS document then users are required to inform PETRONAS of the nature and justification for these if it is intended that the deviations are to be permanent.

Feedback

This PTS document is not intended as a static set of rules, but a growing collection of HSE expertise. Consequently, users are invited to comment on the PTS to PETRONAS and to suggest changes and additional material which they consider would be useful for inclusion in future revisions.

1.3 RELATIONSHIP WITH OTHER SYSTEMS

This PTS on Design Integrity PTS has been designed and written so as to include PETRONAS Process Safety requirements and to harmonize and link back to the higher level document, the PETRONAS Health, Safety, and Environmental Management System (HSEMS), PETRONAS Project Management Systems (PPMS) and Design Engineering Manual (DEM)

Furthermore, this PTS has been developed to be an integral part and tool to assist in managing risk within the overall PETRONAS HSE MS. Figure 1 below illustrates the elements of the PETRONAS HSE MS and their interactions.

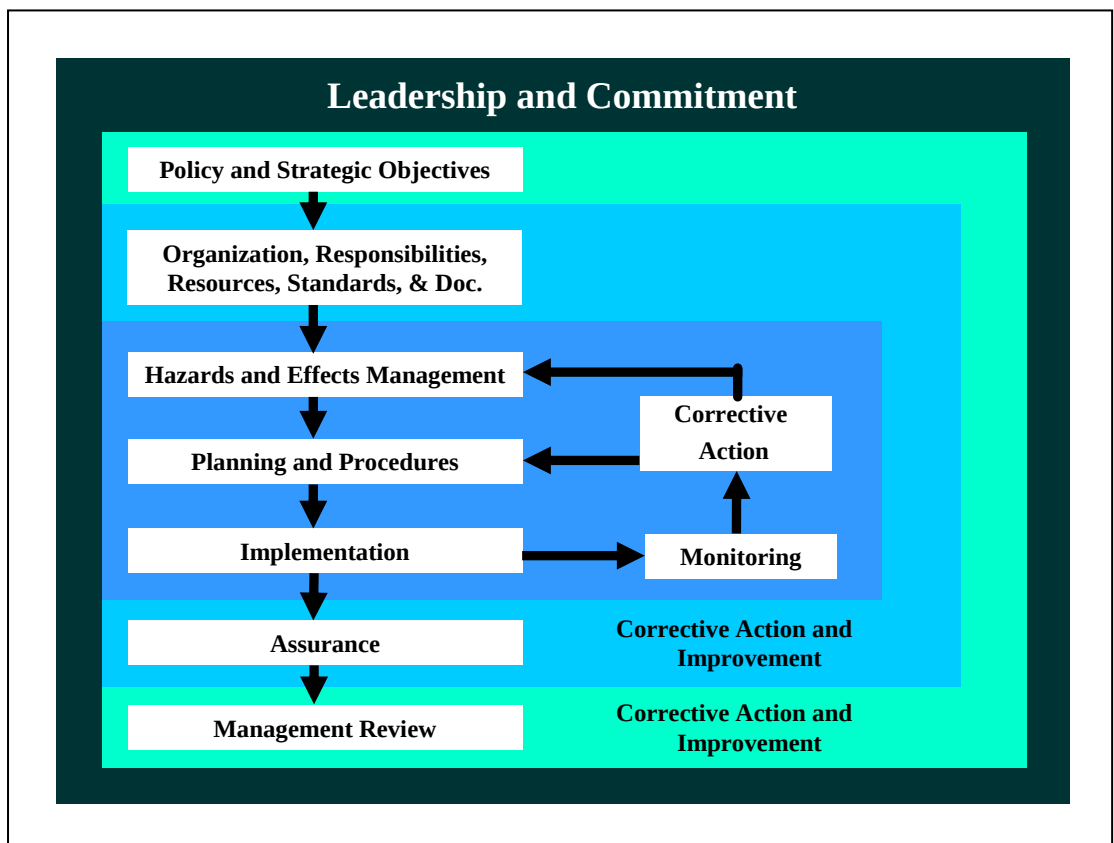


Figure 1: The PETRONAS HSE MS

The activities covered by this PTS fit into the overall PETRONAS HSE MS, and include, but are not limited to, the following examples:

Leadership and Commitment: PETRONAS Management commits and expects all managers to proactively manage risk throughout the lifecycle of facilities in their respective OPU/HCU.

Organization, Responsibilities, Resources, Standards, and Documentation: OPU/HCU management shall create an organizational structure for managing Design Integrity. This is to include designation of responsible personnel / Custodians to manage all aspects of the development and implementation process, ensuring suitable communication with users, allocation sufficient resources to the process, develop standards to ensure suitable, adequate, and effective performance of the process on site, and establish both Document and Records Control Management systems to handle management of related documentation.

Hazards and Effects Management (HEMP): The Design Integrity system shall draw on the Hazards and Effects Management system to provide guidance and support to the project risk reviews process. As design projects provide the best opportunity for risk reduction, the design integrity system supports the ongoing demonstration of risk management required by HEMP.

Planning and Procedures: Design Integrity should be planned for, when commencing a project and should be an integrated into the project specification and sanctioning process.

Implementation: Design Integrity shall be effectively and comprehensively implemented. Training programmes shall ensure that personnel are familiar with and competent in its requirements.

Assurance: From time to time, and based on planned schedules, the Design Integrity processes shall be subject to PETRONAS Assurance activities.

Management Review: The suitability, adequacy, and effectiveness of Design Integrity shall be periodically reviewed by the OPU/HCU as part of formal and periodic Management Review processes.

2.0 OVERVIEW

This section deals with the implementation of Design Integrity as part of Project Management, and presents a strategy that supports HSE performance, other business aspects, and success of the organization.

The design phase of the asset lifecycle is the point at which the most cost effective risk reduction is possible both through eliminating or reducing the consequences of a hazardous event, or incident, and reducing the probability of it occurring. The DI process is intended to ensure that risk management is an underlying process during projects, supporting and justifying decision making, and ensuring that inherent hazards and required management measures are communicated in to the operational phase.

The technical integrity of a facility is achieved when, under specified operating conditions, there are no foreseeable risks of failure endangering safety of personnel/environment/asset value. HSE activities are directly related to this purpose.

This PTS is not intended to replace the requirements of the 10.000 series PTS on Project Management or PTS 60.0107 Design, but to support these documents by ensuring a structured DI process is adopted to meet the HSEMS requirements.

“Management Actions” provides a summary of the actions to be carried out in applying DI to a project process.

2.1 APPLICABILITY

The intent of this document is to cover the following circumstances:

- The project is undertaken by a special team or task force dedicated to the task.
- The project involves a significant capital expenditure and/or involves high complexity.

The OPU/HCU should define what it considers to be “significant” and “complex”, and when special project teams or task forces are formed.

In general terms, changes to existing facilities should be managed by MOC (see PTS 60.[HOLD] Management of Change), unless the change meets the criteria above.

The requirements of this PTS shall be incorporated into project tender documents.

2.2 AIM

The aim of Design Integrity is:

To ensure that equipment and systems are designed, constructed and commissioned such that risk are maintained at ALARP.

For PETRONAS OPU/HCUs, this aim requires a sufficient understanding of the project process such that the requirements of risk management can be seamlessly incorporated into it. The OPU/HCU holds accountability for effective implementation of Design Integrity for each project within its remit, although the responsibility for actual operation of the system will lie with the assigned Project Manager¹.

2.3 EXPECTATIONS

When implementing Design Integrity, the OPU/HCU and Project Manager shall ensure that the following expectations, as a minimum, are delivered:

Equipment and systems shall be designed with due consideration of the hazards associated with their construction and operation. Hazard identification shall be applied from the earliest stages of the project process through to close-out.

The assessment of HSE risks shall be used as a basis for decision-making during the design process. In making decisions about the design of facilities, projects shall use risk assessment to consider the impact of the design on the hazard exposure to people, assets, environment and the reputation of the company. Cost benefit analysis may be used where it is necessary and can be properly applied.

¹ For the purposes of this document “Project Manager” refers to OPU assigned Project Manager or Project Director.

Compliance with company, industry and legal requirements shall be assured. Compliance is a prerequisite for the project and shall be demonstrated on a continuous basis. Variation from compliance requirements shall be reviewed and approved through a defined process involving suitable authorities.

Operational performance requirements shall be defined to ensure suitable levels of dependability and effectiveness are achieved through the lifecycle of the facility. The use of performance standards within specifications is aimed at clearly describing the expectations for the system and associated equipment. Performance standards may be defined in terms of functionality, reliability, availability, inspectability and maintainability, although all of these aspects should be considered.

Equipment and systems shall be designed such that they can be decommissioned. The decommissioning of equipment includes taking out of service (mothballing or abandonment), removal, disposal and recycling, and site clean-up and decontamination. The use of recyclable materials, features that facilitate removal of equipment and mechanisms for reducing the contamination of the surrounding environment all contribute to meeting this expectation.

The design integrity processes shall be assured and, where necessary, corrective action taken. Design integrity shall be an integral part of the project process and shall be seen as a key deliverable and performance indicator.

Competent independent review shall be carried out as part of the assurance process on higher risk projects. The use of independent review shall be a critical part of the project process for larger projects. The purpose of the reviews is to ensure the design integrity process has been applied and the above expectations have been met.

OPU/HCU may develop a dedicated DI document outlining how the OPU/HCU is going to address the requirements of this PTS or incorporate the requirements of this PTS into their respective Project Management System Manual. In either case, the requirements of this PTS shall be comprehensively addressed.

2.4 LINKS WITH OTHER SYSTEM ELEMENTS

The following HSE MS processes will normally have a direct link to the DI system. It is the responsibility of the Custodian of the system and his/her team to ensure that all suitable links are identified for their relevance on a case-by-case basis, and if affected, appropriate control measures are identified, implemented, and monitored.

Management of Change (MOC) – Provides the framework for the inclusion of risk in the decision making process. The tie-in of new equipment and systems to existing facilities shall be addressed by the MOC system.

Mechanical Integrity (MI) – Equipment and systems shall be designed and constructed to facilitate ongoing integrity throughout their lifecycle.

Training and Competency – New equipment and systems may require new skills and expertise to be developed in project and operational personnel.

Contractor Management – Engineering projects involve contractors, vendors and consultants in all their phases. These personnel need to be effectively incorporated into the DI process.

Emergency Response (ERP) – Emergency plans shall be reviewed and updated as required as a result of the addition or modification of equipment and systems.

Process Safety Information (PSI) – Such information is a key deliverable from the DI process.

Operating Procedures (OP) – Procedures and practices may require to be updated as a result of the DI process.

Process Hazard Analysis (PHA) – The PHA methodologies should support DI as part of the risk review process.

Hazard Effect Management Programme (HEMP) – DI implements the requirements of HEMP in a project environment. HEMP requires a wider range of methodologies are applied (e.g. EIA, CHRA, EAIA etc.) and provides the infrastructure (Hazard & Effect Register and Critical Activity Register) through which the results of the risk review process are managed.

Proprietary and Licensed Technology Assessment (PLTA) – The acquisition, introduction and use of licensed or proprietary technology in a OPU/HCU will require an assessment of the changes such technology brings to the OPU/HCU.

2.5 BASIS AND COMPATIBILITY

This PTS:

1. Supports PTS 60.0101, HSE MS Manual, which provides “global” HSE management system guidance for PETRONAS companies,
2. Recognises the requirements of compliance with legal, corporate and regulatory requirements.
3. Is compatible with the ISO 14001 : 2004 Standard for Environmental Management Systems and the OHSAS 18001 : 1996 Specification for Occupational Health and Safety Management Systems
4. Incorporates other internationally accepted “best management practices.”

2.6 OVERALL ROLES AND RESPONSIBILITIES

The roles and responsibilities of individuals involved in the development, application, supervision, monitoring, and review of the DI system shall be defined by each OPU/HCU.

An acceptable means for doing this is the use of RACI Charts (**R**esponsible, **A**ccountable, **C**onsult, **I**nform) as shown in Management Actions.

Ideally roles and responsibilities should be documented as a performance standard defining:

- **What** is to be done?
- **Who** is to do it?
- **When** or **how often** it is to be done?
- The **deliverable(s)** expected.

The OPU/HCU shall have a Custodian with overall responsibility for ensuring the DI process is suitably managed. Custodianship / Custodian positions shall be defined by the OPU/HCU.

3.0 DESIGN INTEGRITY FRAMEWORK

3.1 BACKGROUND

This document describes a framework for application during projects to deliver the aims and expectations of DI. As projects vary greatly in their complexity, duration, use of technology, mix of personnel and contractual arrangements, it is considered preferable for projects to create their own systems based upon the framework defined in this PTS. OPU/HCU's should specify the requirements of this framework when sanctioning projects.

The processes within the framework are described in the table below along with which project phases they should be completed.

Process	Description	Project Phases (Typical)				
		Concept & FEED	Detailed Design	Procurement	Construction & Installation	Commissioning & Handover
Design Integrity Philosophy	The underlying philosophy when designing equipment to meet the aims and expectations of DI. This will include objectives such as aiming for inherently safer design, the application of a risk management process, and having an asset lifecycle view in assessments.	✓				
Risk Review Process	The review process should focus on the identification, assessment and management of hazards inherent to the construction, installation, operation and decommissioning of equipment. The ongoing control of risks during the project is managed after the initial reviews have been completed. Significant changes in the design are referred back for assessment with regard to their impact on risk.	✓	✓	✓	✓	✓
Design Standards	Design standards should be assessed to ensure they are suitable and fit for purpose. Deviation from their requirements should be managed in a robust and competent manner.	✓	✓			
Safe Operating Envelope	Safe Operating Limits are determined to ensure that the envelope within which the equipment will operate, and the associated process safety buffer, is understood.	✓	✓			

Safeguarding Memoranda	The safeguarding systems associated with the equipment are summarised and their performance defined.		✓	✓	✓	✓
Knowledge Retention & Communication Processes	Key information is captured, contextualised and transmitted to others, particularly those who will operate, inspect, maintain and decommission the equipment.		✓	✓	✓	✓

It is expected that Project Managers will ensure that the framework is in place and operational from the earliest point in the project process. In most cases the requirements laid out here are not over and above the best practices operational in most projects. However, the requirements to formalise these processes and ensure that knowledge is captured are likely to be the most difficult to apply.

3.2 DESIGN INTEGRITY PHILOSOPHY

The philosophy shall be defined at the start of the project and adopted across all the relevant project functions. The philosophy should be incorporated into the basis of design for the project. The philosophy shall be written and adopted by the project team and be aligned with the magnitude of the project activity and the potential hazards to be managed. However, the document must include the requirements defined in the following sub-sections.

It is expected that there is a defined risk management basis within the philosophy. This requires ongoing identification of hazards and the use of relevant risk assessment techniques to support the decision making process. The balance between risk and expenditure can be managed through the use of cost-benefit analysis wherever this is deemed necessary.

For example, to achieve the same relief rates from an upgraded system may require an increase in size of the relief system header. However, the cost of this equipment would make the project prohibitively expensive. Risk assessment should be used to determine the acceptable blow-down time, and cost-benefit analysis may be used to determine what should be spent to upgrade the relief system, or whether the project should actually proceed.

3.2.1 Risk Management

Risk management is an ongoing process as the risk profile may change as decisions are made. It is considered to be a project management activity to ensure that the results of the risk management process are regularly revisited. A key document in this process is the Hazards & Effects Register which is a deliverable from the project. The register acts as a repository of the identified hazards and associated risks and shall be developed and maintained throughout the project lifecycle (see PTS 60.149 HEMP). It fulfils three main functions:

- To ensure that the project management can quickly see the risk profile of the designed facility, particularly the high-risk items.
- To provide information to design teams about identified hazards which may affect the design of equipment and systems.

- To provide a means for communicating identified hazards to the OPU/HCU at project close-out.

When acting to manage hazards and drive down risk it is expected that the approach described in Figure 1 - Risk Management Hierarchy, or equivalent approach, be adopted.

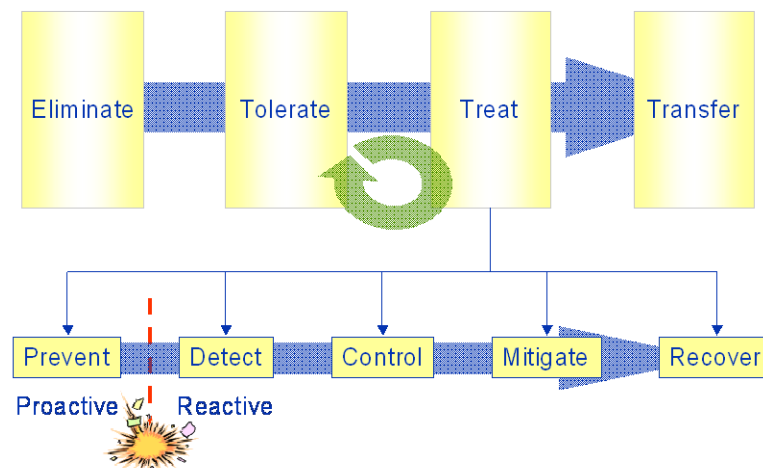


Figure 1 - Risk Management Hierarchy

• Eliminate	The hazard should be removed altogether by substituting a less hazardous alternative, or by eliminating its need altogether.
• Tolerate	If it is not possible to terminate the hazard then it is necessary to determine whether the risk it poses can be tolerated – i.e. it is within the risk acceptance criteria. If this is true no further action may be needed.
• Treat	If the risk is intolerable, then measures need to be put in place to manage the risk to a tolerable level. These measures are explained below.
• Transfer	If the risk cannot be reduced to a tolerable level, then it may be possible to transfer some or all of the risk through the use of competent 3 rd parties or and use of insurance.

If the risk is still intolerable, then the activity should not continue and an alternative should be sought.

When treating the risk the following steps should be taken to apply suitable safeguards:

- Prevent Put in place safeguards to prevent a hazardous event occurring by interrupting the causes.

• Detect	Rapid detection of the hazardous events allows the early deployment of reactive safeguards with benefits in managing the consequences of an event.
• Control	Containing the hazardous event, removing sources of energy, and preventing it from escalating ensures that consequences are minimised.
• Mitigate	Mitigating the effects of the hazardous event involves dealing with the consequence such as fire fighting and evacuation of personnel.
• Recover	Dealing with the aftermath of a hazardous event and returning to an operational state is essential for the ongoing health of the organisation. This step includes investigating the incident, clean-up, restoring operation and communicating with stakeholders.

As part of this process it will become clear where there are gaps in the provision of safeguards, or where hazards could be eliminated. At this point recommendations should be made as to means for reducing the risk to a tolerable level. The use of inherently safe design will assist in meeting these requirements.

3.2.2 Compliance Assurance

It should be remembered that the use of risk assessment does not negate the need to comply with industry-accepted codes and standards and these documents should be a starting point for the design process. Risk assessment simply provides a mechanism for determining whether the requirements of the code and standard are acceptable in the particular case in which they are being applied. Deviations will require suitably justified, risk-based decision making.

Compliance with regulatory requirements is usually non-negotiable and the project shall ensure that local laws and regulations are complied with. Assurance plan shall be established throughout the life of the project e.g. PIR schedule in to ensure compliance issues are identified and appropriately mitigated.

3.2.3 Lifecycle View

Design Integrity is the first step in a process that will manage integrity of equipment through-out the lifecycle of the facility. As such the design process must also consider how the facility will be operated, maintained, inspected and decommissioned and facilitate that process in a safe manner. This may well include specifying more reliable equipment with its associated additional cost to reduce the amount of intervention required later.

For example, by specifying a corrosion resistant coating inside a process vessel the requirement for vessel entry to conduct inspections may be at considerably lengthened intervals or eliminated altogether.