



RP 30-6

DESIGN PHILOSOPHY FOR PROTECTIVE INSTRUMENT SYSTEMS

August 1994

Copyright © The British Petroleum Company p.l.c.

All rights reserved. The information contained in this document is subject to the terms and conditions of the agreement or contract under which the document was supplied to the recipient's organisation. None of the information contained in this document shall be disclosed outside the recipient's own organisation without the prior written permission of Manager, Standards, BP International Limited, unless the terms of such agreement or contract expressly allow.

BP GROUP RECOMMENDED PRACTICES AND SPECIFICATIONS FOR ENGINEERING											
Doc. No. RP 30-6		Issue Date August 1994	Latest Amendment Date								
Document Title DESIGN PHILOSOPHY FOR PROTECTIVE INSTRUMENT SYSTEMS (Replaces BP Engineering CP 48 Parts 1 & 2 and BPE.91.ER.103 App.1)											
APPLICABILITY Regional Applicability: International											
SCOPE AND PURPOSE This document specifies the general philosophy and functional requirements for the development of Protective Instrument Systems to shut down, totally or partially, a facility in order to place it in an acceptably safe condition or to avoid major economic loss.											
AMENDMENTS <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;">Amd</td> <td style="width: 20%;">Date</td> <td style="width: 25%;">Page(s)</td> <td style="width: 40%;">Description</td> </tr> <tr> <td colspan="4"> </td> </tr> </table>				Amd	Date	Page(s)	Description				
Amd	Date	Page(s)	Description								
CUSTODIAN (See Quarterly Status List for Contact) Control & Electrical Systems											
Issued by:- Engineering Practices Group, BP International Limited, Research & Engineering Centre Chertsey Road, Sunbury-on-Thames, Middlesex, TW16 7LN, UNITED KINGDOM Tel: +44 1932 76 4067 Fax: +44 1932 76 4077 Telex: 296041											

CONTENTS

Section	Page
FOREWORD	iii
1. INTRODUCTION.....	1
1.1 Scope	1
1.2 Application.....	1
2. SHUTDOWN PHILOSOPHY GENERAL PRINCIPLES	1
2.1 Objectives	1
2.2 Safety Management Plan.....	2
2.3 Design Procedure and Risk Acceptability Criteria	3
2.4 Risk Assessment	3
2.5 Protective Measures	3
2.6 Process Conditions to be Considered	4
2.7 Benefit Assessment.....	5
2.8 Change Control	5
3. PROTECTIVE INSTRUMENT SYSTEM CATEGORISATION.....	5
3.1 General	5
3.2 Categorisation Definitions.....	6
4. METHODS OF PROTECTION.....	8
4.1 General	8
4.2 Protection Against Over Pressuring	8
4.3 Protection Against Overheating	9
4.4 Prevention of Uncontrolled Chemical Reaction	9
4.5 Protection against Abnormal Liquid Levels.....	10
4.6 Depressurisation	10
4.7 Isolation/Removal of Liquid Inventories.....	11
4.8 Prevention of Atmospheric Release.....	12
4.9 Prevention of Interaction with Other Plant or Tankage.....	12
4.10 Prevention of Damage to Equipment.....	13
5. IMPLEMENTATION.....	13
APPENDIX A.....	14
DEFINITIONS AND ABBREVIATIONS	14
APPENDIX B.....	16
LIST OF REFERENCED DOCUMENTS.....	16
APPENDIX C.....	18
CATEGORISATION PROCEDURE	18
FIGURE C1.....	24
CATEGORISATION DESIGN CYCLE	24
FIGURE C1 - NOTES	25
CATEGORISATION DESIGN CYCLE	25
FIGURE C2.....	26



CATEGORISATION OF PROTECTIVE INSTRUMENT SYSTEMS	26
FIGURE C3	27
OUTLINE OF QRA PROCESS	27
APPENDIX D	28
SHUTDOWN DESIGN REQUIREMENTS.....	28
D1 GENERAL	28
D2 EMERGENCY SHUTDOWN	28
D3 PROCESS OR PRODUCTION SHUTDOWN	30
D4. HEAT-OFF	31
D5. EQUIPMENT TRIP	35
D6. OFFSHORE	35



FOREWORD

Introduction to BP Group Recommended Practices and Specifications for Engineering

The Introductory Volume contains a series of documents that provide an introduction to the BP Group Recommended Practices and Specifications for Engineering (RPSEs). In particular, the 'General Foreword' sets out the philosophy of the RPSEs. Other documents in the Introductory Volume provide general guidance on using the RPSEs and background information to Engineering Standards in BP. There are also recommendations for specific definitions and requirements.

Value of this Recommended Practice

1. There are not yet any industry codes covering this important and developing area.
2. There is a risk of over-indulgent categorisation without this document being followed.

Application

Text in *italics* is Commentary. Commentary provides background information which supports the requirements of the Recommended Practice, and may discuss alternative options.

This document may refer to certain local, national or international regulations but the responsibility to ensure compliance with legislation and any other statutory requirements lies with the user. The user should adapt or supplement this document to ensure compliance for the specific application.

Principal Changes from Previous Edition

Now incorporates findings from the BP multi-Business Working Group on Instrument Protective Systems and introduces the use of a risk based approach. Readers should be aware of IEC work under Standards Committee 65A to develop IEC Standards for the functional requirements for electrical/electronic/ programmable electronic safety related systems. These are still in the working group phase and some realignment of this RP may be necessary once the IEC document is issued.

Feedback and Further Information

Users are invited to feed back any comments and to detail experiences in the application of BP RPSE's, to assist in the process of their continuous improvement.

For feedback and further information, please contact Standards Group, BP International or the Custodian. See Quarterly Status List for contacts.



1. INTRODUCTION

1.1 Scope

1.1.1 This document provides guidance on the design philosophy required for the development of Protective Instrument Systems to ensure safe operation and appropriate control of environmental pollution or economic loss.

1.1.2 It is stressed that the use of Protective Instrument Systems should not be used as a means to avoid good basic plant design or to overcome design errors.

Protective Instrument Systems can introduce the requirement for continued attention throughout the life of the plant and result in operational costs which are frequently under estimated. This is even more pronounced where there are requirements for High Integrity Systems. The design of a plant should therefore include consideration of the need for instrument protective systems with the aim to minimise the requirement.

1.1.3 The requirements for detection devices and logic systems are not covered by this Recommended Practice and reference should be made to BP Group [RP 30-5](#), Section 2 for applicable recommendations.

The requirements for fire and gas systems are treated separately in BP Group [RP 30-7](#).

1.2 Application

It is applicable to onshore and offshore facilities for production, refining and chemicals applications. It is applicable to site fabricated or pre-assembled plant and to packaged units. It is not applicable to drilling operations, including workover and wirelining.

2. SHUTDOWN PHILOSOPHY GENERAL PRINCIPLES

2.1 Objectives

The requirements for Protective Instrument Systems have to be considered as part of the overall health, safety and environmental protection facilities for a plant or installation. The aim will be to ensure the safety risks are reduced to a level which is as low as reasonably practicable (ALARP), as agreed with the Business Unit responsible for the installation, and as required by any applicable Local or National Regulatory Authority. Protective systems may also be provided to minimise the risk of commercial loss.

The risks that the Protective Instrument Systems will be protecting against will include but not necessarily be limited to:-

- (a) Loss of life or serious injury



- Directly in the incident.
- Indirectly (e.g. through impairment of escape or refuge).
- Through escalation of an incident.

(b) Commercial Loss

- Directly in the incident (property damage and business interruption).
- Through pollution clean up costs.
- Through escalation of the incident.

There may also be other risk involved due to the market place where the facility is installed or where the 'product' is being supplied. Risks such as Company standing within the local community or image with customers may have an influence on the specific installations. It is therefore perfectly possible that, due to the size of the potential economic loss, some Category 2 systems will justify greater integrity than some Category 1 systems.

This Recommended Practice recognises the move to a risk based approach to safety and introduces alignment with known emerging international standards on the subject (such as IEC working group 65A currently in draft form). This cannot be fully achieved until such time that these standards are completed and issued.

2.2 Safety Management Plan

The total design process for protective systems should be controlled within an overall safety management plan which should be established before commencement of design. This should be a life cycle plan covering all aspects of the installation safety from conceptual design through to final termination of use. The aspects covered should include, but not necessarily be limited to the following:-

- Safety strategy and criteria to be used
- Definition of responsibilities/accountabilities
- Safety assessment process
- Dependency between life cycle activities
- Competency requirements
- Risk identification
- Risk categorisation
- Risk quantification
- Design process
- Design integrity confirmation
- Design change control
- Test and maintenance requirements
- Confirmation of operating performance
- Documentation/record requirements and control
- Regular review of safety cases

2.3 Design Procedure and Risk Acceptability Criteria

The design procedure is described fully in Appendix C. It is essential that the Business Unit responsible establish the risk acceptability criteria for the installation. The first step in designing protection facilities will therefore be the identification of the overall risks involved for the installation. The Business Unit responsible, will then need to set the criteria for risk assessment.

These may be qualitative or quantitative risk acceptability criteria and may be governed by local or National Regulation or Practice. In general, risk acceptability criteria associated with loss of life tend to be of a quantitative nature. Measures which mitigate commercial loss tend to be evaluated using Cost Benefit Analysis.

2.4 Risk Assessment

Having established overall risk acceptability criteria, a more detailed study can be made of the installation to establish the contribution to the total risk from each identified risk source. The level of detail assessment will need to be commensurate with the stage of the design completion at that time, however, the validity of the assessment would need review as detail is developed.

The outcome of such studies may have significant impact on the design of plant and proposed shutdown systems. It is essential therefore that risk assessments are carried out early in the design process to ensure design is such to minimise inherent design risks and thus need for protection systems.

2.5 Protective Measures

The protective measures may include, but not necessarily be limited to, the following:-

- Protection against over pressuring.
- Protection against overheating.
- Prevention of uncontrolled chemical reaction
- Protection against abnormal liquid levels.
- Activation of depressuring systems.
- Isolation/Removal of liquid inventories contained in vessels.
- Prevention of flammable or toxic material atmospheric release.
- Prevention of interaction with other plant or tankage.
- Prevention of damage to equipment

Prevention of over pressure will also include consideration of the potential for back flow through pumps and settle-out pressures following shutdown.

Facilities which may present risk will include, but not necessarily be limited to, those containing a quantity of flammable fluid or toxic material (which could give rise to serious hazard), a fired process heater, or those additionally specified as a requirement for the specific application.

A process unit containing a flammable inventory of the order 15 tonnes or more would generally be considered as being a plant that could give rise to hazard due



to the scale of the consequence of failure of containment, however, due regard will need to be given to any extra-ordinary hazard due to the material being handled. .

Material will generally be considered flammable if any of the following apply:-

- (a) It has a flash point below 100°C.
- (b) It is processed at a temperature greater than its flash point.
- (c) It is processed at a temperature above its auto-ignition temperature. For crude oil and petroleum products this shall be taken as 210°C. For pure chemicals, published values of the auto-ignition temperature shall be used.

The designer will need to give consideration as to whether a particular process or material being handled gives additional risks such as:-

- (a) Other flammable material or chemical which can give rise to extraordinary risk (e.g. toxic or highly corrosive).
- (b) Applications specified of particular environmental hazard.
- (c) Applications specified as requiring special facilities for terminating a chemical reaction.

2.6 Process Conditions to be Considered

During the design process all anticipated conditions leading to potential risk should be considered for all phases of the plant operation including shutdown, startup, emergencies, hold etc. Exact requirements of the arrangements and the need for a protection system should be defined after considering the following:-

- Statutory requirements.
- Information from the Process Licensor.
- Information from Equipment Vendors.
- Requirements defined by this and other BP Group Recommended Practices.
- Characteristics of the process
- Local conditions such as location layout, manning levels/skills
- The operational testing philosophy to be adopted

It is the total arrangement of safety systems that is important. Its adequacy for the anticipated conditions and other related codes must be considered such as BP Group [RP 22-1](#), [RP 44-1](#), [RP 44-3](#), [API RP 520](#), [521](#) and [ISO 10418](#) (based on [API RP 14C](#)).

The design process should be reinforced and confirmed by means of routine HAZOP/HAZID exercises and the Safety Audit process.

[ISO 10418](#) is more generally applicable to installations within the US or where US practice prevails. It provides a protection system design methodology for offshore production platforms utilising SAT (Safety Analysis Tables). Where the ISO/API practice is not to be applied, the BP Hazop and trip system categorisation procedure gives an equivalent to the Safety Analysis Tables.

[ISO 10418](#) calls for 2 levels of protection, the first being provided by means of instrumentation and the second provided by a pressure relief valve. This arrangement is equivalent to the Category 2B system detailed in this practice. For wellheads and flowlines, [ISO 10418](#) allows the alternative of use of duplicate instrument trip arrangements but with cautionary statements. The caution given is



that it should only be used after 'thorough consideration of alternatives' and that pressure relief may still be necessary. The ISO/API practice gives no guidance as to how to assess the requirements, and this Recommended Practice addresses these issues for non Category 2B systems. Where protection is provided by a Category 1 system, a further level of protection may be unnecessary provided a full integrity analysis confirms that the acceptable risk criteria are met.

2.7 Benefit Assessment

An assessment then needs to be made to establish whether the provision of any Protective Instrument System will give benefit in making a significant contribution to reducing the risk involved. The risk reduction benefits of using alternative measures also needs to be assessed to ensure the optimum arrangement is provided. Included within this assessment should be consideration of any facilities that need to be provided to meet Regulatory/Inspection Authority specific requirements.

The use of Instrument Protection Systems can be very expensive to engineer install and subsequently maintain during the life of an installation. There may well be benefits, therefore in considering redesign of plant or layout. The use of Quantified Risk Assessment and Cost Benefit Analyses may also be considered, however this will depend on project/installation philosophy. The cost, time and resources required for such analysis can be considerable and should not be under estimated when deciding on this route.

2.8 Change Control

- 2.8.1 A review of the risk assessment should be made whenever there is a modification of the design or operating conditions that could affect the level of risk. The review should include the revised conditions and is necessary to ensure that requirements for protection are maintained.

The Register of Safety Related Devices should be updated where appropriate following any modifications. (Refer BP Group [RP 44-1](#) 'Over Pressure Protection Systems').

3. PROTECTIVE INSTRUMENT SYSTEM CATEGORISATION

3.1 General

- 3.1.1 The integrity of a Protective Instrument System must be sufficient to ensure that the resulting HSE and/or economic risk is acceptable to the Business concerned. Initial specification and design considerations typically require the up-front categorisation of a protective system based on a qualitative consideration of the likelihood and consequences of its failure. Subsequently the design selected according to this categorisation should be assessed to ensure that the residual risks accord with the relevant Business defined criteria. Satisfaction of these criteria may require redesign.

A Protective Instrument System will ideally be defined by consideration of a hierarchy of options with QRA being interactively applied to ensure that the



business defined criteria are satisfied. In practice it is rarely feasible to adopt such a rigorous procedure and resort has to be made to categorisation. It must be recognised however that this categorisation needs to meet business defined risk acceptability criteria, i.e. according to the frequency of occurrence as well as the effect of the protected situation arising.

3.1.2 The method for categorisation of Protective Instrument Systems is included in Appendix C - 'Categorisation Procedure' - Figure C2 - 'Categorisation of Protective Instrument Systems'.

3.1.3 Before categorisation it should be noted that other protection methods not using a Protective Instrument System may be employed where a self acting mechanical device or system is used as the sole protection against dangers to personnel. This is sometimes referred to as a Category 0 system, particularly within some parts of BP Exploration.

Examples include relief valves and bursting discs etc.

3.2 Categorisation Definitions

3.2.1 Category 1

An application where to meet the risk acceptability criteria it is necessary to use a Protective Instrument System and where failure of the system to act on demand is likely to lead to risk of serious permanent injury or loss of life to one or more persons and where exposure to such risks is significant and cannot be avoided.

Appendix C, Figure C2, details the assessment method for determination of Category 1 systems.

Category 1 example:-

An application where loss of life is likely could be where the failure of the Protective Instrument System to operate on demand resulted in overpressure and rupture of a vessel containing 200 tonnes of hot liquid propane. This inventory would be released as an instantaneous fireball which would engulf the local control building giving no time for evacuation. The permanently occupied control room within the building has a large area of glazing facing the plant and would not, therefore, afford any protection to the occupants against the fireball.

3.2.2 Category 2A

An application where risks are controlled by a Protective Instrument System and where failure of the system to act on demand is unlikely to result in serious injury or loss of life. Failure may well however, result in extensive or prolonged damage to the environment, major economic risk due to loss of plant/production/product or penalty due to uncontrolled release and cannot be effectively avoided by operator intervention.

Appendix C, Figure C2, details the assessment method for determination of Category 2A systems.

Category 2A examples:-

Where the companies license to operate would be threatened, protection against damage to unspared equipment essential for production and where potential downtime could result in major commercial loss..

Protection against significant leakage from pipelines which could cause environmental pollution.

The consequences of failure of Category 2A system will not result in loss of life for reasons such as there being adequate time to escape or because people are not close enough to be affected. Also, where pollution is a consideration this poses no serious threat to human health.

3.2.3 Category 2B

An application where risks are controlled by a Protective Instrument System and where failure of the system to act on demand would not result in risk as defined for Category 1 or 2A systems, but could result in undesirable disruption to operating or process conditions.

Category 2B examples:-

Where failure to act could result in demands being placed on the ultimate protection system e.g. pressure relief system which is itself adequate to handle the duty.

Where failure to act would result in the need for operator intervention but adequate time and facilities are available to avoid major disruption.

Where failure to act could result in damage to spared equipment.

Where failure to act could result in temporary loss of quality of product.

3.2.4 Category 3

An application where the normal control system ensures reliable production and maintains plant operation within the operational limits. A Category 3 system is therefore not deemed to be a Protective Instrument System. It is included here for completeness and to clarify the interface between the normal plant control system and Protective Instrument Systems.



The possibility of including Category 2B protection systems in the control system may be considered, but this would be dependent on the security of the arrangement. The 2B system will frequently be in place to protect against failure of the associated Category 3 control element. If the control system is to be used, diversity of inputs and control processors should be included, together with error reporting, in order to minimise the possibility of unrevealed common mode failure.

4. METHODS OF PROTECTION

4.1 General

Situations requiring Protective Instrument Systems will typically include, but no necessarily be restricted, to the following:-

4.2 Protection Against Over Pressuring

4.2.1 Requirements for over pressure protection are detailed in BP Group [RP 44-1](#) and are generally achieved by provision of pressure relief valves, wherever practical.

The requirements are based broadly on:-

(a) *Continuation of the use of pressure relief devices, wherever practicable, as the main method of over pressure protection.*

(b) *The use of pressure-limiting instrumentation as the sole method in a limited number of cases where alternative means are not practical.*

4.2.2 The provision of complete relief system capacity as the final protection for individual equipment items will in most cases be adequate to avoid the need for additional Protective Instrument Systems in order to achieve the required performance. The design process, however, needs to include consideration of the performance achievable with relief valves against the identified risk.

Additional Protective Instrument Systems required to meet acceptability risk criteria may need to be classified as Category 1.

4.2.3 Where complete system relief is adequate, consideration should be given to using pressure-limiting instrumentation where benefits can be identified from minimising the demand rate for relief device operation and to:-

(a) Reduce possible hazards of atmospheric relief.

(b) Reduce any environmental nuisance from atmospheric relief or relief to flare to a level acceptable to local regulations.

(c) Minimise loss of material arising from pressure relief device operation.



- (d) Minimise the cost of any closed system that has to be provided.
- (e) Reduce requirements for test/reseat following operation to avoid release due to failure to reseat.

Pressure-limiting instrumentation in this case will generally be Category 2B although may still be required to be 2A or 1 where highly toxic material is involved, and may, where appropriate, include automatic actuation of the following:-

- (a) *Feed or pipeline transmission pump or compressor trips.*
- (b) *Fuel shutoff valves.*
- (c) *Re-boiler heating medium bypasses and shutoff devices.*
- (d) *Fired re-boiler shutdown and heating medium circulating pump trips.*
- (e) *Pressure and temperature-limiting systems to protect reactors.*
- (f) *Start-up of standby pumps and compressors.*
- (g) *Standby cooling water sprays to air coolers.*
- (h) *Operation of dump/divert facilities.*

4.3 Protection Against Overheating

Generally, there is no self acting system analogous to a relief system in this area. Overheating may be as a result of external influence, such as ambient temperature or fire, or from sources within a process. For external influences, measures such as insulation or cooling may be considered adequate, however for sources within a process it may be necessary to rely on Protective Instrument Systems. Heat off or quench systems can be considered to allow prompt action to reduce heat input to a process.

4.4 Prevention of Uncontrolled Chemical Reaction

4.4.1 For each reactor, information from the Process Designer (normally a process licensor) should be supplied on:-

- (a) Any reactions which are possible, together with the conditions of pressure, temperature and reactants which may initiate the reaction, the rate of temperature and pressure change and the expected final temperature and pressure.
- (b) The recommended procedure to ensure risks are minimised in the event of loss of control.

4.4.2 Facilities should be provided to carry out the recommended procedure to stop any reaction which could result in the identified risk. The effect of carrying out this procedure on the process should be determined. The design should ensure that all equipment is adequate or protected for the pressures and temperatures to which it may be exposed during this operation.

4.4.3 For catalytic reactors, information from a Process Designer should be supplied on any actions required to protect the catalyst in the event of a failure of a reactor feed stream, equipment malfunction or utilities failure. The necessary facilities required should be agreed with the Process Licensor including whether any trip system should be manually or automatically initiated and the protective system category.

4.4.4 The design should ensure that all equipment is adequate or protected for the pressures and temperatures to which it may be exposed for possibly short periods of time as a result of the actions required by the heat-off protective systems.

4.5 Protection against Abnormal Liquid Levels

4.5.1 The effect of abnormal liquid levels in tanks or vessels which normally contain liquid and in vessels which normally contain no liquid needs review on a case by case basis. Shut down of equipment may be necessary in cases where serious spillage or damage could result to down stream equipment e.g. compressor subject to liquid carry over from k.o. pots, or large multi-stage pumps which may be running without liquid feed.

The loss of liquid level could result in loss of vapour from high pressure to low pressure equipment, or to atmosphere, which may necessitate closure of isolating valves to avoid such breakthrough occurring. The breakthrough of vapour from high pressure equipment can result in the potential for over pressure of the downstream equipment and the protection provided needs to be designed to prevent this. For high liquid levels, it may be considered necessary, in certain circumstances, to automatically stop feed to the system.

4.6 Depressurisation

4.6.1 Emergency depressuring facilities on high pressure systems reduce the magnitude of stresses in vessels and equipment, by removal of sources of energy and flammable fluid, and hence reduce the risk of failure under fire conditions and potential for escalation under failure conditions. They also facilitate rapid shutdown of the plant in the event of mechanical failure and reduce the risk of fire.

4.6.2 Automatic depressuring of equipment may be required in certain circumstances e.g. to protect catalysts. It can also be required if shutdown of rotating equipment causes loss of auxiliary systems, such as seal oil, with consequent loss of vapour to the atmosphere.

4.6.3 The need for depressurisation should give consideration to the amount of vaporisation that will occur, resulting in loss of inventory, together with the effects of the release and impact on other plant and flare systems.

Depressurisation should be considered when the process system runs full of liquid, in normal operation, provided this does not result in vaporisation which causes unacceptable loss of product or excessive venting/flaring with no external heat input, e.g. from a fire (typically more than 10% of the liquid contents) .

4.6.4 Where depressurisation facilities are provided, the time for depressurising and associated valve/restriction orifice sizing, should be decided after considering:-

- (a) The rate required to reduce the pressure to levels to where the probability of failure of vessels or equipment is minimised.
- (b) Potential over pressure/low temperature effect on the flare/vent system and interaction with other relief to the system.
- (c) The effect of the depressurising rate on vessel internals (e.g. high pressure reactors) or other process equipment.
- (d) The temperature after depressurising of vessels and equipment not exposed to the fire and the effect of any low temperatures on material properties.
- (e) The generation of additional vapours resulting from external fire on the system.
- (f) Any requirement for delay of depressurising initiation following shutdown to protect plant or equipment.

4.6.5 Where automatic depressurisation facilities are not provided, consideration needs to be given to what manual facilities will be required.

4.7 Isolation/Removal of Liquid Inventories

4.7.1 The provision of isolating valves should be considered to allow affected sections of plant to be isolated in the event of an emergency were major hazard may result if inventory is not contained.

This can assist in limiting the potential for incident escalation and ensuring containment within the capacity of protection capabilities. Isolation can be applied to single items of equipment, sections of the plant, or to entire process units.

The provision of isolation valves can be expensive and result in over complex installations. The over zealous application of such facilities, should therefore be avoided.

4.7.2 Isolating valves should be installed upstream of pumps on volatile or high temperature liquids and where it is necessary to contain inventory within a section of the plant. Isolation of inventories may also be necessary to ensure that depressuring operations can be achieved.



- 4.7.3 Certain applications may require the capability for removal of inventory to enable minimisation of risk. The control method used for isolation therefore needs to consider any such requirements and where required, it should be ensured that facilities are readily available.

4.8 Prevention of Atmospheric Release

- 4.8.1 This should normally be achieved by containment, however, this will not always be practical or economically viable. Consideration should therefore be given to the provision of discharge systems which ensure minimum risk of impact from such releases or additional Protective Instrument Systems may be considered to reduce the incidence of release.

Closed flare and drainage systems are examples of discharge systems which can be considered.

4.9 Prevention of Interaction with Other Plant or Tankage

- 4.9.1 A shutdown on a section of plant or a piece of equipment may well have an impact on other plants from which feed or discharge is normally taken. There may also be an impact due to the necessity to vent or remove inventory. The design of the interface with these other areas therefore needs to include protection measures to ensure additional risks are not created within those areas due to change in operating conditions or as a result of those areas experiencing conditions outside the limits of their design.

- 4.9.2 The possibility of interaction with adjacent plant/equipment in the event of failure must also be considered. It needs to be ensured that this will not result in escalation of an incident, inhibit operation or means of access/escape from that adjacent plant.

4.10 Prevention of Damage to Equipment

Automatically initiated protective systems should be provided for equipment and machinery where malfunction can result in safety hazards or major economic loss due to replacement/repair costs or disruption to operations.

These protection measures will generally be Category 2B applications, however, careful assessment should be made of the inherent risk resulting from failure of the trip to operate to ensure a higher level of criticality does not exist.

The following are examples of systems normally included.

- (a) Shutdown systems recommended by the equipment manufacturer.
- (b) Machinery shutdown on for example low-low lube oil pressure or high bearing temperature.



- (c) *Compressor shutdown on any of the following:- high-high liquid level in the suction drum, high-high gas temperature at any point in the machine, low-low seal oil pressure, low suction pressure and, on turbine driven machines, over speed.*

5. IMPLEMENTATION

- 5.1 The shutdown system may be divided into several levels of shutdown dependent upon the severity of the potential hazard and requirements for start up. Guidance for design is given in Appendix D.
- 5.2 Where the form of the Protective Instrument System has been fully defined according to its categorisation, its integrity characteristics need to be assessed to verify that the residual risk meets the business criteria.
- 5.3 Detailed requirements for the engineering of Protective Instrument Systems components are given in BP Group [RP 30-5](#) and BP Group [RP 30-3](#).



DEFINITIONS AND ABBREVIATIONS

Definitions

Standardised definitions may be found in the BP Group RPSEs Introductory Volume.

category 0/1/2A/2B/3	refer to Section 3 of this Practice.
demand rate :	the frequency with which a safety system is called upon to perform its safety function.
emergency shutdown system (ESD):	instrumentation manually or automatically initiated to enable an installation, in the event of a major emergency, to be placed in an acceptably safe condition and to minimise release to atmosphere of flammable or toxic fluids.
high integrity systems:	a system and all its associated equipment that has a high probability of operating correctly when required to do so.
integrity assessment:	study which considers all aspects relating to the capability of a system as a whole to fulfil its requirements. This will usually include a full hazard and reliability analysis and design audit to establish that design guidelines have been followed and the quality at each stage has been consistent with the criticality of the application.
process designer:	the organisation carrying out the process engineering design, normally a contractor to BP, but in some cases BP or a process licensor.
process licensor:	the organisation with ownership of patents, trademarks and know-how relating to the process and normally with the responsibility for process performance.
	any specific application of the terms and responsibilities for the parties defined above are a matter for the Conditions of Contract on a project.
process unit :	a main process section of a refinery or chemical complex, which is separately operable except for reliance on other units for feed stock and off take. (e.g. Catalytic Cracker or Acrylonitrile Unit)



protective instrument systems:	instrumentation provided to prevent losses of all kinds, particularly in process upsets or emergencies, as distinct from instrumentation provided for normal process control and annunciation.
quantified risk assessment :	the quantitative evaluation of the likelihood of undesired events and the likelihood of harm or damage being caused together with the value judgements made concerning the significance of the results.
risk :	the product of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence.
- individual risk:	the frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards.
- societal risk:	the relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realisation of specified hazards.
system integrity:	the characteristic of a system relating to its ability to perform its intended function in the desired manner under all relevant conditions and on the occasions when it is required to perform.

Abbreviations

ALARP	As low as reasonably practicable
API	American Petroleum Institute
BS	British Standard
CBA	Cost Benefit Analysis
ESD	Emergency shutdown
HSE	Health Safety and Environment
IEC	International Electrotechnical Commission
PSV	Pressure Safety Valve
QRA	Quantified Risk Assessment



LIST OF REFERENCED DOCUMENTS

A reference invokes the latest published issue or amendment unless stated otherwise.

Referenced standards may be replaced by equivalent standards that are internationally or otherwise recognised provided that it can be shown to the satisfaction of the purchaser's professional engineer that they meet or exceed the requirements of the referenced standards.

ISO 10418	Petroleum and Natural Gas Industries, Offshore Production Platforms - Recommended Practice for Analysis, Design, Installation Design, Installation and Testing of Basic Surface Safety Systems. (Based on API RP 14C)
API RP 520	Recommended Practice for the design and installation of Pressure Relieving systems. Parts I and II
API RP 521	Guide for Pressure - Relieving and Depressuring Systems

BP Group Documents

BP Group RP 22-1	Fired Heaters (replaces BP CP 7)
BP Group RP 30-3	Instrumentation and Control, Selection and Use of Control and Shutoff Valves (replaces BP CP 18 Part 4)
BP Group RP 30-5	Instrumentation and Control, Selection and Use of Equipment for Instrument Protection Systems (replaces BP CP 18 Part 5)
BP Group RP 30-7	Process Design Guidance for Fire and Gas Systems
BP Group RP 43-3	Sub-Sea Isolation Systems
BP Group RP 44-1	Over Pressure Protection Systems (replaces BP CP 14)
BP Group RP 44-3	Relief Disposal Systems (replaces BP CP 25)
BP Group RP 46-1	Unfired Pressure Vessels (replaces BP CP 8)
Corporate HSE Team (1993)	Guidelines on the Use of Quantified Risk Assessment (QRA) and the Development of Risk Criteria (in draft)



United Kingdom Specific Requirements:-

[SI 1029](#), 1989

The Offshore Installations (Emergency Pipeline Valves) Regulations 1989.



CATEGORISATION PROCEDURE

To implement Protective Instrument Systems in a cost effective way which will meet the requirements of the application requires a systematic approach. The steps necessary for the implementation of protection systems are listed below and summarised in Figure C1. It is important that each step is well documented and shown to be in accordance with acceptable procedures. Safety reviews and design audits at successive stages will monitor the work as the project progresses and will need to establish that adequate quality has been achieved during each stage.

Step 1

Establish the safety plan for the protective systems (Refer section 2.2 of this Practice). This plan should then form an integral part of the overall safety plan for the project. Establish with the Business Unit involved, in collaboration with the responsible design, safety and operations groups, the risk acceptability criteria that are to be imposed on the design for risk of serious injury or fatality and for what is to be considered 'major' commercial loss.

See also steps 3 and 5 below.

Step 2

When the process design has been established, the first requirement will be to identify where process conditions could exceed design limits. The protection provided should then be evaluated and it be established whether any Protective Instrument Systems are being used to provide this protection. The justification should be formally recorded for future design review where modifications or changes in conditions occur.

The design should be reviewed to establish the abnormal conditions which could lead to the design limits being exceeded. During this systematic review it may be assumed that pressure relief valves/ bursting discs function according to design requirements. It will need to be ensured, however, that these devices will be able to provide total protection if the instrument system were to fail to operate. It also needs to be ensured that the mechanical devices give the necessary protection if high demand rates exist and that this does not introduce a requirement for additional measures in order to minimise the demand rate on these devices..

In some cases temporary conditions which marginally exceed design limits may be acceptable but this will need to be agreed with those responsible for the mechanical integrity of the plant.

The effects of common mode failure of distributed control systems should be considered.

Step 3

A systematic examination of the process/equipment design is then required to establish the application category of any instrument systems included in the protection arrangements. The categorisation will be dependent on the level of risk that will occur in the event of failure of the protection system. The method for doing this is detailed in Figure C2. The categorisation

assessment should be formally recorded for audit and future operations use when redesign or changes in operating conditions occur.

In order to complete the Category 2A/B assessment, it will be necessary for the Business Unit responsible for the investment, to define the value per incident or per year which is judged to be serious commercial risk and where higher levels of integrity are required. For applications where the risks include environmental damage, the operating unit interpreting Corporate and HSE policy should define the criteria to be applied.

Instrumentation provided for normal process control and operator convenience alarms should not be included except where these are used for consideration as giving a contribution to reduction in frequency of demand, for the protective systems to act, within any detailed Integrity Assessment.

Note: The flow chart for assessment of Category 1 systems is based on the draft IEC working group 65A qualitative methodology which is in turn based on DIN standards. It is intended that this will be further developed to permit assessment as to the required safety integrity levels to permit protective system equipment selection. This practice will require amendment to incorporate this guidance once confirmed.

The approach of using an initial qualitative approach to categorisation involves many high level judgmental decisions. To ensure that such assessment has credibility, and is open to audit, it is essential the participants in the exercise have extensive and broad industry experience of the issues involved and are of a seniority and standing to be objective and influential.

The issues which may need to be dealt with include :-

- *Release from protection devices and dispersion characteristics*
- *Flammable or toxic consequence of such releases*
- *Design limits of release discharge systems*
- *Operational issues relating to potential commercial losses*
- *Operational requirements influencing probabilities of risks to personnel*
- *Equipment/plant design considerations for loss of containment*
- *Experience, on broad front, of issues which influence demand rates*
- *Design limitations for shutdown systems*
- *Control system interaction with plant and shutdown systems*

For the Category 2A/B assessment a Cost Benefit Analysis will need to be carried out and the results will depend upon economic criteria based on the criticality of the plant and the cost of the Protective Instrument Systems necessary to give protection to an acceptable level as defined by the business unit involved. It is essential that too onerous limits are not set in order to avoid proliferation of over complex, expensive to install and maintain, protective systems. The following are suggested as a starting point, considering a single event occurring once in ten years, for the business to decide whether criteria that are more or less onerous should be imposed.

2B - Loss < \$1,000,000

2A - Loss > \$1,000,000

The Cost Benefit Analysis should also consider whether there is a lower limit where even a Category 2 system cannot be justified. A suggested limit in this context may be <\$50,000. This lower limit is again an individual business decision.

If the event is considered as likely to occur more or less frequently than once in every 10 years then the level of risk for a single event would require adjustment accordingly to give an equivalent level of residual risk.



The categorisation proposals will be re-affirmed during the various stages of Hazard and Operability Studies (HAZOP) and therefore need to be completed before these studies are initiated..

Step 4

The design of the installation should be reviewed to establish if modifications can be made to the process or equipment design to eliminate the need for Category 1 or 2A Protective Instrument Systems.

It is stressed that the number of Category 1 or 2A systems should be minimised and only used where it proves impractical to provide alternative protection. These systems should not be used as a means to avoid good basic plant design or to overcome design errors, unless fully documented whole of life cost justification is developed.

The capital, design and operating costs of such systems are usually underestimated and redesign to enable self-acting systems to be used is often cost effective. The provision of High Integrity Systems may also only solve an immediate problem and not solve the basic problem which may resurface on further plant or process modification. The cost assessment should also therefore address the longer term requirements for protection.

Step 5

The approach of performing a Quantified Risk Assessment (QRA) may be considered at this stage. The aim will be to ensure that risks of serious injury or loss of life are reduced to a level which is as low as reasonably practicable (ALARP) whilst ensuring reasonable cost. A QRA is recommended for Category 1 systems and may, in fact, be a statutory requirement depending on the country or state in which the installation is located. For Category 2A systems the decision is for the business involved. (Refer to Figure C3 for outline of QRA process)

The QRA may assist in optimising the design requirements, for Category 1 or 2A systems. For Category 2A systems, however, the costs involved in completing such a study, as against the potential benefits that may be foreseen, should be considered before deciding to take this route.

In order to carry out a QRA the following requires definition:-

Category 1 criteria

(i) Individual Risk Levels Acceptability Criteria

It is essential that these be defined by the Business unit, as appropriate to their operation and for the installation involved, prior to the start of design and that these be confirmed before any attempt at performing a QRA is initiated. It should be noted that these figures will need to be considered within the context of the overall plant risk to which an individual Protective Instrument System may contribute only a part of that risk.

(ii) Demand Rates

These can either be determined by a reliability analysis or obtained from previous operator experience.

(iii) Consequence of Failure

The losses (i.e. loss of life and commercial loss on failure of the Protective Instrument System to act on demand) are obtained by modelling the consequences of failure (fires, explosions, toxic release



etc.), and determining the effect on personnel and equipment (to calculate commercial loss due to property damage and business interruption). The risk is calculated by multiplying the frequency that the Protective Instrument System fails on demand by the total value of the losses.

It needs to be stressed that setting very onerous targets for risk protection can result in the requirement for complex and expensive Protective Instrument Systems and the whole of life costs for maintenance and test of these systems should not be under estimated. Such targets need to be realistic and supportable.

At this stage it is possible that a proposed Category 1 system will not reduce the risk levels to those specified. If this is the case, then redesign the process will be essential or, if this is not possible, the defined risk level requirements will need to be review by the Business Unit..

Category 2A Criteria

Refer Step 2 above

For some applications the use of Category 2B systems may be found acceptable with or without enhancements such as duplicate or alternative sensors. The use of a Cost Benefit Analysis (see Step 7) may assist in defining the optimum required system.

Step 6

All protective systems should be listed together with failure conditions which the systems are designed to respond to and the consequences of failure on demand. The listing should be in a format which enables audit during safety reviews and permits the consequences of any modification to be assessed and updated. Any QRA carried out should also be included in this document.

Step 7 and 8

A fit for purpose system design should be selected for each Category 1/2A to meet the required risk reduction criteria. Justification can be aided by the use of Cost Benefit Analysis. Systems should achieve the required risk reduction whilst maintaining test intervals acceptable to the operator. Category 2A optimum system configuration requirements should be to meet the agreed commercial risk, however, it may be decided that this may be assessed qualitatively.

It is common for protective system requirements to be established from preliminary process and plant design. It is therefore essential that these be reviewed once the design is confirmed or subsequently changed.

Test requirements should not be too frequent as this can be very manpower expensive and because of the resourcing aspects and disruption to day-to-day activities there is a risk of not meeting the requirements and thus jeopardising the integrity of the system. Due regard should be given to system function test which is achieved during normal operation e.g. starting and stopping of electric pumps tests the integrity of switch gear. This can reduce the required burden on scheduled testing. Maximum use should be made of self-testing equipment, on-line diagnostics and on-line testing.

It is necessary to ensure that facilities are provided to enable testing to be performed and that the test periods assumed are adhered to. This will need to be continued through the life of the installation and reviewed whenever modifications or changes in conditions occur. Similarly, if the assumed reliability of devices proves to be different in practice, the test arrangements and frequency should also be review.

Step 9



The integrity of the protective instrumentation on Category 1 systems should be determined by analysis. The level of integrity check made for Category 2A systems will depend on criticality and this will be for the Business Unit decision.

For Category 1, a fully quantified assessment of the system reliability should be carried out, together with a qualitative assessment of the design to ensure quality and configuration are adequate for the required risk reduction.

For Category 2A applications involving major environmental risk, a fully quantified assessment of the system may be considered depending on business requirements. A qualitative assessment, however, may be considered adequate provided system integrity and reliability is assured in a manner acceptable to the business. Where considered adequate, the reasons shall be recorded for approval.

For Category 2A systems involving economic or minor environmental risk, the reliability of systems should be qualitatively assessed.

Step 10

The integrity levels in Step 9 should be compared to the integrity targets set in Step 5.

If adequate integrity levels have not been achieved then redesign will be necessary unless a reduced level of integrity can be agreed with the final operator.

Step 11

Design dossiers should be prepared for protective instrumentation on Category 1 and 2A systems. The Design Dossier for Category 1 system protective instrumentation should be referenced in the Register of Safety Related Devices.

The dossier requirements for Category 2A systems will depend on the criticality of the application. Where quantitative assessment is to be made, the documentation will be similar to that for Cat. 1 and should include a Cost Benefit Analysis. Where a qualitative approach is to be accepted, the justification and assessment should be included together with system test requirements

Step 12

The Design Dossiers for Category 1 and 2A systems protective instrumentation shall be submitted to the final operator. The dossier should include all design details, analyses (including QRA and Cost Benefit Analysis where performed) and test requirements/procedures.



Step 13

Prove and record satisfactory operation, to meet design, prior to putting into operation.

Step 14

Monitor and record operation of the protective system during life of plant and check that the original design assumptions on system performance and demand rates are still valid. Also control proposed changes in plant design or operating conditions to ensure that the protective system design basis is not altered. If changes or alterations do occur, re-assessment and possible redesign may be necessary.

Design dossiers will be active during the life of the plant and will require updating when there is any change in design, operating conditions or actual system performance. The dossiers should be presented in a format such that changes can be readily made.



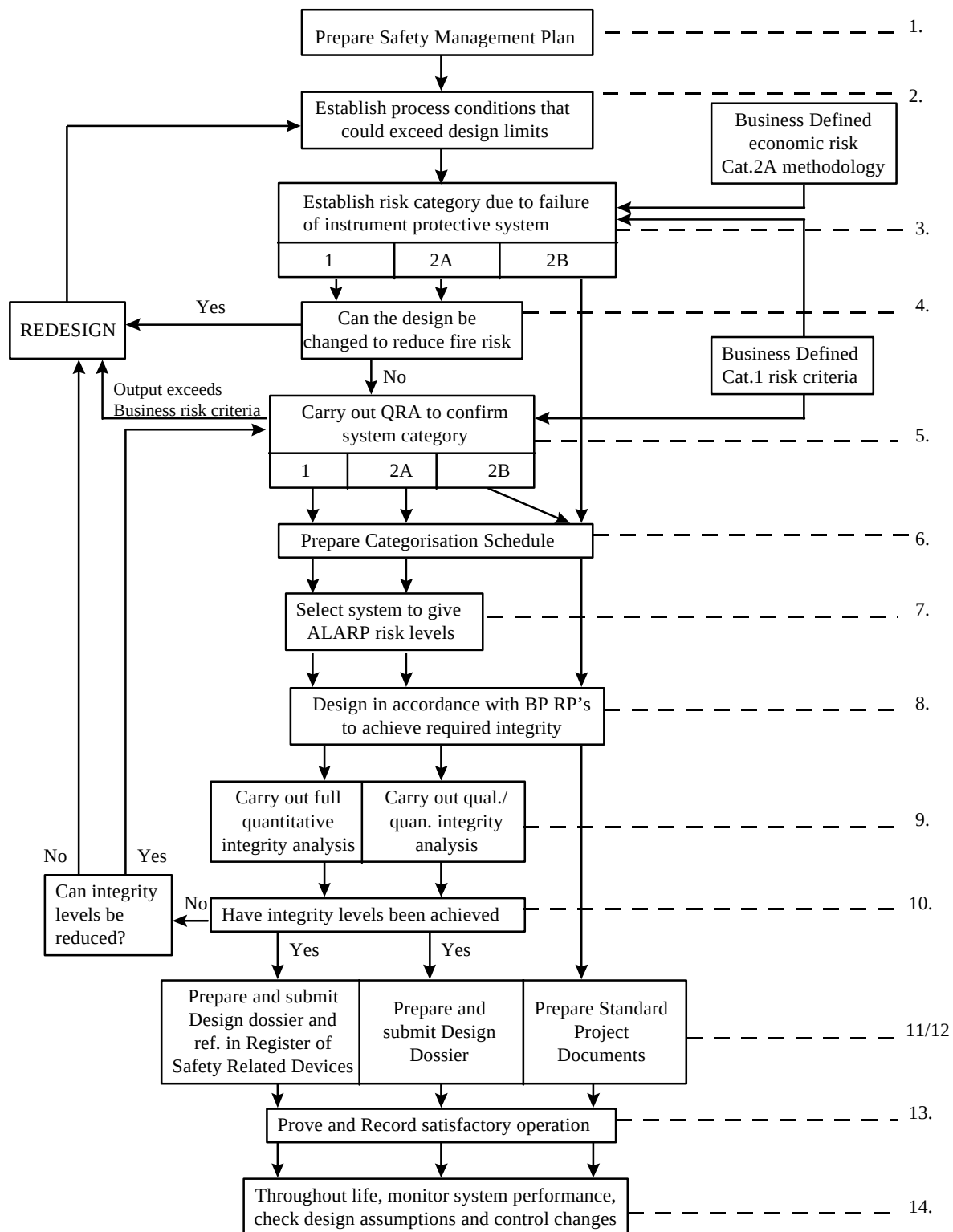


FIGURE C1

CATEGORISATION DESIGN CYCLE

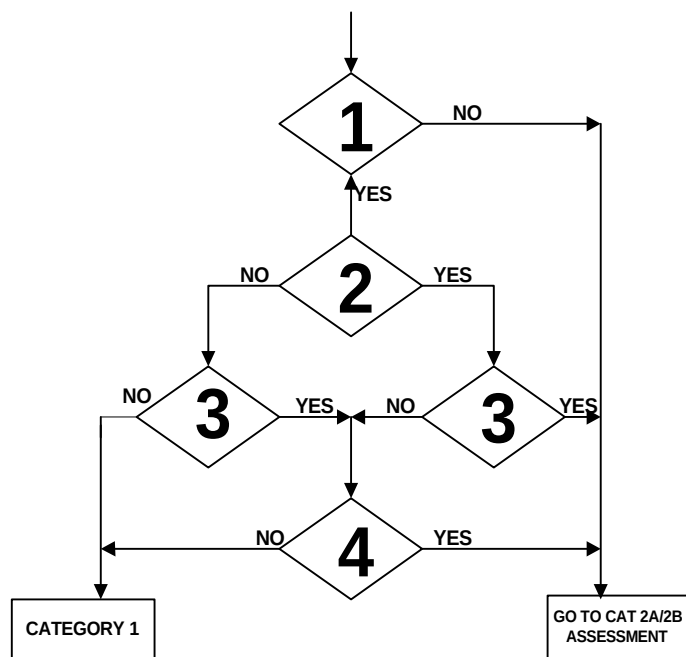
GOAL		OUTPUT
1.	Establish whole life design processes, responsibilities and accountabilities.	List of total design, audit maintenance actions and responsibilities.
2.	Determination of all reasonably foreseeable failures that could exceed design condition.	Schedule of process deviations.
3.	Determine the Category of application from assessment of risk.	Schedule of risk categories together with justification.
4.	Reduce the number of Category 1/2A application by design change to reduce risk.	Revised list after considering alternative design.
5.	Reduce the number of Category 1/2A applications because of acceptable risk levels.	Revised list together with detail justification for system integrity requirement category change.
6.	Document category assessment to permit audit and control of future modification.	Finalised categorisation schedule to form the basis for design of protective instrument system.
7.	Cost effective design with integrity to achieve ALARP risk levels demonstrated by cost benefit analysis.	System design configuration and test intervals.
8.	Design to ensure the required integrity levels are met.	Detail design.
9.	Confirm the integrity level achieved by the design	Document integrity analysis.
10.	Ensure the integrity achieved meets those in step.	Decision as to whether adequate integrity has been achieved.
11/12	A fully detailed dossier to enable whole life audit, modification, control, maintenance and test.	Design dossiers submitted to installation operator.
13.	Ensure the system performs in accordance with design.	Test certificates detailing all tests performed and acceptance criteria.
14.	Performance/design tracking to identify and redesign requirement.	Formalised periodic reports detailing checks made.

FIGURE C1 - NOTES

CATEGORISATION DESIGN CYCLE

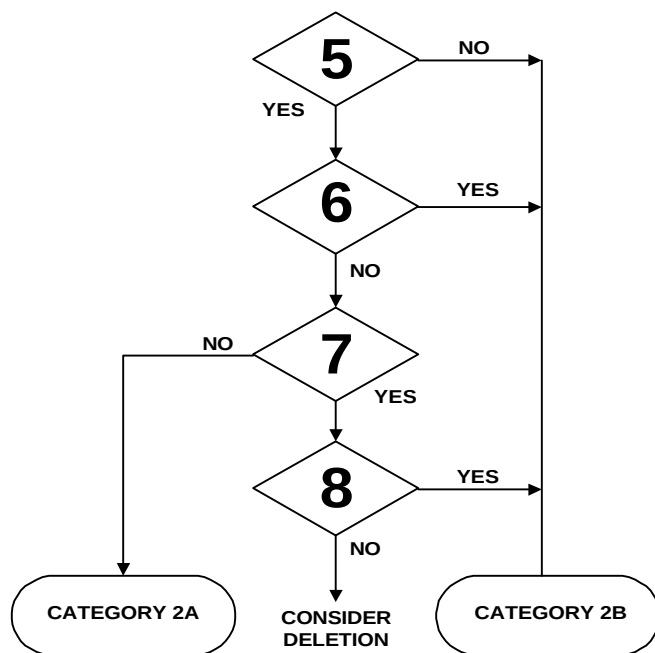


CATEGORY 1 ASSESSMENT



1. If the protection fails to operate on demand are the consequences likely to cause serious injury or loss of life to one or more persons ?
2. Will the exposure, and the exposure time, to the hazardous zone be minimal?
3. Is the demand rate low? (ie. Frequency of demand on the protective instrument system).
4. In the event that a hazard occurs can personnel readily or easily avoid the consequences ?

CATEGORY 2A/B ASSESSMENT

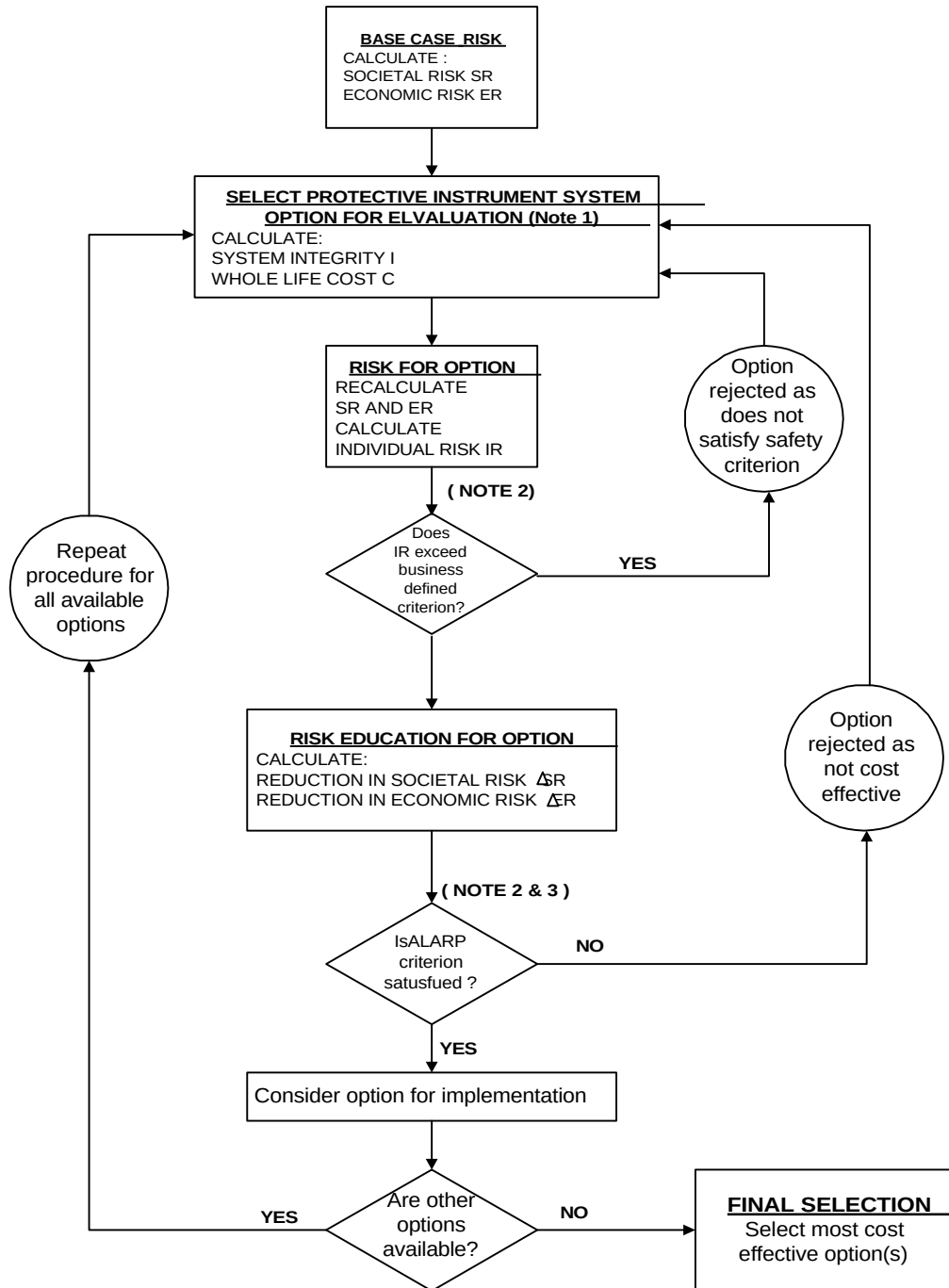


5. If the protection arrangement does not operate on demand can it result in a 'major' loss due to any of the following:-
 - (a) Damage to plant or equipment
 - (b) Loss of product or lost production.
 - (c) Loss of Company image or standing.
6. Are the following satisfied?
 - (a) Independent operator alarms and indications give advanced warning of impending failure.
 - (b) Alarms give clear indication of urgency and are not lost when many alarms are sounding.
 - (c) The control room is continually manned and alarms allow the operator time to act to prevent failure.
 - (d) The operator will have adequate training and competence to take control of the situation.
 - (e) The operator can identify that the protection arrangement has failed to act on demand.
7. Will the protective system demand rate be very low?
8. Is the protection arrangement essential for satisfactory plant operation? If not consider deletion.

FIGURE C2

CATEGORISATION OF PROTECTIVE INSTRUMENT SYSTEMS

(Refer Step 3 From Categorisation Design Cycle - Figure C1)



Notes:

1. Procedure should initially be executed using base data (ie. without protective instrument system)
2. Business defined criteria for safety and economic risk.
3. The ALARP criteria may be satisfied on safety or economic grounds or a combination of both.

FIGURE C3

OUTLINE OF QRA PROCESS

(Refer Step 5 From Categorisation Design Cycle - Figure C1)

SHUTDOWN DESIGN REQUIREMENTS

D1 GENERAL

D1.1 The shutdown System may be divided into several levels of shutdown dependent upon the severity of the potential hazard and requirements for start up. These can be generalised as:-

- Emergency Shutdown
- Process or Production shutdown
- Heat Off
- Equipment Trip

D2 EMERGENCY SHUTDOWN

D2.1 Emergency shutdown should be activated by one or more emergency switches in the control room. Where more than one unit is controlled from the control room then a separate switch should be provided for each unit.

The switches are additional to any heat-off or other lower level shut down switches and would normally be hard wired and independent from any associated logic system in order to provide back-up in the event of failure of the logic system.

D2.2 Automatic initiation of the emergency shutdown is required only where operating conditions could occur which can result in major hazard, e.g. pressure vessel failure, fire, or explosion, and the operator will have inadequate time, training or facilities to initiate the shutdown to ensure safety is maintained. The time shall be determined from the agreed operating philosophy for the plant and the hazard being protected against. Consideration should also be given to the circumstances under which the operator will be expected to intervene and the consequences should he fail to act. When automatic initiation is provided it should still be possible to initiate manually the ESD from the control room.

Particular areas that should be addressed are:-

- (a) *Where major loss of containment of flammable or toxic fluid may result,*
- (b) *The possibility of any runaway chemical reactions,*
- (c) *The possibility of internal explosion, e.g. where a process vessel contains flammable material and oxygen.*

Information on exothermic and potentially runaway reactions should be supplied by the process licensor and should be assessed by the process designer.



D2.3 The required action on operation of the emergency shutdown will depend on the plant being controlled but will typically:-

- (a) Actuate the heat-off systems, where necessary, in accordance with Section D4 of this Appendix.
- (b) On fired heaters, close the tight shut-off valves in the pilot gas lines as well as main fuel lines.
- (c) Stop input of all materials to the unit except those materials required for safe shut-down e.g. utilities, nitrogen. Consideration should also be given to the need to stop all outputs from the unit, however, this will depend on any requirements for removal of inventory in the event of a hazard situation, and what alternative disposal routes are available.

Supplies to the unit should be stopped by stopping all pumps or compressors and closing valves which could feed fluids into the unit.

- (d) Close all emergency shutdown valves.

Closure of remotely operated inventory isolating valves should be considered if necessary to mitigate against the emergency condition, however, the effect on any potential need for removal of product from vessels should also be reviewed.

- (e) Stop all machinery, including air cooler fans and heater fans unless it can be demonstrated that greater hazard may result.

The system for machinery stop should be Category 2B if the machinery can be stopped manually, additional to and independent of the ESD from an area outside the likely fire zone.

For electrical driven equipment this may be the substation provided local access is readily available and emergency lighting remains operational together with any power systems required for fire fighting, emergency evacuation or other emergency operations.

Steam driven machinery may be stopped by a readily accessible valve in the steam header provided emergency steam for snuffing remains available.

- (f) Depressure the process system as necessary depending on the plant design, materials being handled and potential loss of product.

D2.4 An additional readily accessible method of isolating the feed and product should be available from an area outside the unit. These should be located where safe access will be ensured in the event of incident on the unit to be isolated. Such methods may include manually operated block valves or manual pump shutdown at another unit or tankage area.



Typically they should be at least 15 m. from equipment containing significant inventory of flammable material and the likely fire zone, however greater distances may be necessary, depending on the hazard, and assessment of the requirements needs to be made. An example where greater distances will be required is where there is the potential for jet flames which could influence the location of such facilities.

- D2.5 On some process plant, there can be a requirement to shutdown equipment in a specific sequence to avoid increased hazard. Where provided, an assessment should be made of the probability of sequence failure and the consequences, including any potential effects on relief systems.

Facilities should be provided to enable a safe start-up to be made from any failure state.

D3 PROCESS OR PRODUCTION SHUTDOWN

D3.1 Plant Shutdown

- D3.1.1 Full or partial shutdown of the process plant, or production, should be available manually from the main control point, local control room and automatically from protective instrumentation on detection of abnormal process conditions.
- D3.1.2 The various levels of process shutdown should be designed to shutdown and isolate the area of process plant and equipment as necessary to contain the potential hazard. It may be permissible for other process sections to continue to operate providing the safety of the installation is not compromised.
- D3.1.3 Where the detected abnormal process condition requires the shutdown and isolation of a number of process sections, this should be initiated directly and not require the sequential operation of other protective instrument sensors or systems.
- D3.1.4 A philosophy of automatic turndown using partial heat-off may be applied to permit time for effective operator action in order to avoid both the operation of relief devices, and widespread shutdown.

D3.2 Unit Shutdown

- D3.2.1 This is generally the lowest level of shutdown whereby process or utility equipment is shutdown manually or automatically on detection of malfunction. This is normally only possible where the unit is independently operable and does not result in the requirement to trip associated plant providing feed or allowing off take.



D3.2.2 It should be possible to stop, from the control room, the process fluid flow upstream of a heater in the event of tube leakage..

A flow control valve in the process fluid line to a heater may be suitable, provided any pump or compressor is adequately protected against damage when the valve is closed. Where there is a heater charge pump, a remote stop located in the control room and acting on the drivers may be used provided any automatic start-up is overridden. The effect of any back flow should be examined. The system should be designed to prevent over pressure of equipment.

Stopping the process flow to a heater should not restrict emergency blow through steam or allow the steam to bypass one or more passes.

D4. HEAT-OFF

D4.1 General

D4.1.1 The requirement for a heat-off system should be established as part of the over pressure protection study, in accordance with BP Group RP 44-1. Heat-off systems are normally required to achieve one or more of the following objectives:-

- (a) As a part of an emergency shutdown system to avoid the need for operation of over pressure protection relief and minimise material loss.
- (b) To allow an operator in a control room to minimise a potential hazard in the event of localised equipment failure, e.g. a fired heater.
- (c) To reduce the total heat input to a process in a wider emergency than (b), as a prelude or alternative to an emergency shutdown.
- (d) To prevent equipment temperature from exceeding an acceptable value.

Details of how heat off facilities can be achieved are included in the following sub-sections.

On process equipment, the heat input can be from an external source independent of the process e.g. from steam generated outside the process, or can be dependent on the process e.g. from a circulating reflux stream. With an independent source, the effect of the actuation of a heat-off system on the process will probably be limited. When a heating medium is dependent on the process, operation of a heat-off system can have appreciable and undesirable effects on other parts of the plant by reducing heat removal from those parts of the plant.

Examples of heat input dependent on the process includes:-

- *Feed, product (including an intermediate product)*



- Reflux streams,
- Steam generated within the process,
- Hot oil or hot air heating systems where the heating fluid is heated by a process fluid.

The heat-off study is intended to include assessment of the maximum economic benefits of a heat-off system as a result of reduced flaring. Therefore, favourable but credible assumptions are made, e.g. with respect to the operations of check valves. These assumptions apply only to this study. They should not be assumed to apply for the design of relief systems.

The heat off study should fully consider the potential to cause a major upset elsewhere on a facility, e.g. by a sudden reduction in steam consumption.

D4.1.2 Automatic initiation of a heat-off system should be provided when protection cannot be obtained with a simple action by an operator within an operationally acceptable time. Initiation on high temperature should be considered where vessel design temperature can be exceeded without causing an associated pressure rise that initiates the heat-off system.

D4.2 Fired Heaters

D4.2.1 A manually operated heat-off switch should be provided in the control room for each fired heater. Operation of this switch should:-

- (a) Close the fuel shut-off valves in the fuel gas and fuel oil lines to the heater, including any foul gas and waste liquid or gas lines to the heater.
- (b) Stop forced draught fans where necessary to protect the burners, for example of the high intensity type, or to prevent too rapid cooling of the furnace tubes.

The fuel shut-off system on fired heaters should be in accordance with BP Group RP 22-1.

Alternative disposal routes should be provided for foul gas and waste fluid streams. The pilot gas system should be designed to remain in operation.

The manual heat-off arrangement should normally be hard wired and bypass any associated logic protection in order to provide back-up in the event of failure of that logic system.

D4.2.2 The need for automatic initiation of the heat-off system on a low flow should be studied. The study should consider the warnings provided for low flow and the time available for the operator to respond before damage occurs, and the consequence of any such damage.

Low flow may result from such as control failure or tube coking.

Automatic initiation is not normally required. Where provided, the setting of the low flow initiation should be selected after considering the minimum acceptable



flow rate without hazard. Consideration should also be given to the method of detection where multiple passes are involved.

- D4.2.3 In a heater with more than one pass, any alarm or automatic low flow actuation of a heat-off system should be initiated from a flow-measuring element in the inlet to each pass.

Where individual pass flow measuring elements are not provided, low flow actuation may be considered from a flow element in the main feed line before splitting into individual passes, however, it must be recognised that this will be a less secure arrangement.

- D4.2.4 Where there is more than one feed stream to a heater and the flow of the combined stream cannot be metered (e.g. a two phase flow), then metering of individual component streams should be provided.

- D4.2.5 It should be possible to stop forced and induced draft fans from the control room when these fans are not stopped by the heat-off system.

D4.3 Pressure Vessels

- D4.3.1 For the purposes of this document, pressure vessels including heat exchangers connected together without valves or with valves used only during shut-down and which can be locked open in operation, should be considered as a single vessel.

- D4.3.2 A heat-off system should be provided, unless a vessel cannot be over pressurised by the heat input when the vessel is completely blocked in.

For example, in a vessel which cannot be full of liquid, the liquid vapour pressure at the maximum obtainable temperature might not exceed the vessel design pressure.

- D4.3.3 The design pressure of a vessel, the settings of the pressure relief device, any heat-off pressure sensor or temperature sensor and the pre-alarm sensor should be selected after considering the response time of the system including sensor, actuator and the process, and the relief device setting margin.

This can require an increase in the design pressure above that specified generally in BP Group [RP 46-1](#).

- D4.3.4 In addition to any automatic heat-off initiation, it should also be possible to initiate a heat-off system manually from the control room.

- D4.3.5 The actions taken on initiation of heat-off, will depend on outcome of the overpressure protection study but will typically include:-

- (a) Close valves in hot fluid supply lines.

- (b) Switch off heat input by electrical heating.
- (c) Stop stripping steam input to the vessel.
- (d) Stop the flow to fired heater re-boilers on fractionating column unless the process fluid is susceptible to coke formation.

Control valves which are designed to fail to the closed position may be used provided these are located such that they are not exposed to risk of damage from the hazard being protected.

D4.3.6 The effect of the heat-off actions on the heating system should be checked for possible secondary effects leading to over pressure or equipment damage which will require additional protection.

An example is due to stopping steam flow through superheater tubes in a fired heater.

D4.3.7 The effect of stopping feed streams to a vessel should be analysed considering all possible causes of over pressure. In assessing the ability of protection system to prevent over pressure of a vessel with blocked outlets, the analysis should take account of the different behaviour of a gas/liquid and vapour/liquid system. This analysis should determine if stopping the feed streams would increase the plant relieving rate and also if any equipment would be subject to over pressure. The analysis should assume that it is acceptable to stop the flow through a process heater on the feed stream.

Based on this analysis, it should be decided if the feed streams should be stopped by the heat-off system.

D5. EQUIPMENT TRIP

- D5.1 The requirement to trip equipment/machinery will depend on the risk assessment (refer section 4.10 of the main text). In general, manual facilities for shutdown will be required at a safe location local to the machine. Additional remote and automatic shutdown requirements may also have been identified.
- D5.2 As far as practicable and safe, other equipment should continue to operate but it should be protected against damage resulting from the shutdown. This may be by alarm and operator action within operationally acceptable time from the alarm signal, provided there are adequate back up facilities to prevent a major hazard, e.g. vessel over pressure, if the operator failed to take action.
- Where shutdown of other equipment is inevitable, then it should be shut down by the condition initiating the trip.
- D5.3 Standby machinery should not be started automatically when this could cause further hazard.

D6. OFFSHORE

D6.1 General

- D6.1.1 Additional Emergency Shutdown facilities are normally required for offshore applications in order to comply with statutory requirements applicable for the location of the installation.

The contents of this practice are not intended to supersede any Statutory Instruments and Guidance Notes for offshore installations but to supplement them with the particular requirements of BP. The shutdown system will normally consist of a number of interconnected levels which will include Emergency shutdown, production, plant and equipment levels. Red, post red, yellow and riser shutdowns described following are those emergency shutdown levels typically necessary to meet the requirements of such documents.

Reference should also be made to BP Group [RP 43-3](#) - Subsea Isolation Systems.

- D6.1.2 The required integrity of the Emergency Shutdown systems should be agreed prior to commencement of design.

Emergency shutdown functions necessary to satisfy statutory requirements are not normally defined as Category 1. Due to the importance of these systems, however, it may be decided that to meet the risk assessment requirements, an integrity and reliability is required that is higher than that provided by conventional Protective Instrument Systems.

- D6.1.3 Shutdown systems should be designed to be fail safe in operation except where it can be demonstrated that a greater hazard can result.



Where energise to trip systems are used, the design of the system will need to be such that the required integrity level is maintained.

The use of energise to trip can be considered for red shutdown in order to avoid spurious total facility power down. To achieve an acceptable integrity level, measures such as duplicate trip paths and condition monitoring may be required.

- D6.1.4 The specification of shutdown Systems for drilling operations requires special considerations and is excluded from this Recommended Practice. It is usual for the drilling area shutdown system to be separated from the installation shutdown system. It should be noted however, that manual initiation of the installation yellow shutdown should be possible from strategic locations in the drilling area.

D6.2 Emergency Shutdown Levels

D6.2.1 Red Shutdown

A red shutdown is defined as the highest level and is initiated manually on the decision to abandon the installation or in the event of a major emergency requiring isolation of all potential electrical sources of ignition.

A red shutdown should be initiated from manual push buttons located at the main control point for the installation and from other appropriate locations from where an emergency may be managed.

Consideration should be given to providing red shutdown buttons at lifeboat muster stations, radio room and other key locations, however, proliferation of such facilities should be avoided to minimise risk of spurious operation.

A red shutdown should initiate the following shutdown actions:-

- (a) Shutdown of all utilities and power supply systems except those emergency systems essential for life support, communication, navigation or evacuation.
- (b) Shutdown and isolation, of all production and associated test facilities.
- (c) Closure of all wellhead valves.
- (d) Opening of all automatic depressurisation valves.
- (e) Closure of all Down Hole Safety valves.
- (f) Closure of all riser ESD valves and sub-sea pipeline isolation valves.
- (g) Activate the Installation General Alarm .
- (h) Fire pumps which are already running should continue to operate.
- (i) Emergency lighting should remain energised.

D6.2.2 Post Red Shutdown System

Initiation of a red shutdown should make available the post red shutdown system. This system is to monitor the atmosphere in the vicinity of non certified electrical emergency systems and associated power supplies which remain energised following a red shutdown and shutdown that equipment in the event of detection of hazardous concentrations of gas.

Examples of emergency systems kept live after red shutdown are:-

- *General Alarm and Emergency Communications Equipment.*
- *Navigation Aids.*
- *Emergency Lighting.*
- *Diver Recovery and Life Support Systems.*
- *Fire Pumps.*

The post red system should provide the following functions:-

- (a) *Shutdown and isolation of non certified electrical emergency systems and associated power supplies on confirmed flammable gas in those areas. The isolation should be by equipment classified suitable for Zone 1.*
- (b) *Diesel driven fire pumps which are already running should continue to operate.*
- (c) *The starting of any electric start diesel driven fire pumps should be inhibited on confirmed detection of flammable gas in the area.*
- (d) *Non-certified electrically driven fire pumps should be shutdown and isolated on confirmed detection of flammable gas in the area.*

D6.2.3

Yellow Shutdown

A yellow shutdown is the second highest level of shutdown and should be initiated on detection of fire or loss of containment. Its function is to initiate shutdown, isolation and de-pressurisation of the process plant and to activate those emergency systems necessary to contain a potential emergency. This is normally achieved by activating the lower levels of the ESD system which comprise the process and unit shutdown systems.

A yellow shutdown should be initiated by the following signals:-

- (a) *Manual push buttons located at the main control point and at strategic points around the Installation.*
- (b) *Automatically from the fire and gas detection system, as determined by the risk assessment.*
- (c) *Automatically on loss of selected essential utilities such as electrical, pneumatic, hydraulic power or cooling water supplies.*

The manual facility for not normally manned or remotely controlled installations may require initiation via telemetry. Where used, the security of this transmission will require consideration to ensure integrity of shutdown is maintained.

A yellow shutdown should initiate the following actions:-

- (a) *Shutdown and isolation of all sections of production and associated test facilities. Liquid inventory should be retained in the process equipment.*
- (b) *De-pressurisation of the production system.*



- (c) Closure of all wellhead master and wing valves.
- (d) Closure of appropriate pipeline riser ESD valves.
- (e) Audible and visual alarm at the main control point.
- (f) Closure of down hole safety valves if a yellow shutdown has been initiated by confirmed fire detection in the well bay area.

D6.2.4 Pipeline Riser and Sub-sea Valve Emergency Shutdown System

The riser emergency shutdown and sub-sea isolation valves, where fitted, are required to close in the event of an emergency which could give rise to escalation of the incident due to loss of pipeline containment.

The valve and its actuating mechanism, so far as is reasonably practicable, should be protected from fire, explosion or impact.

The design of the ESD system should incorporate all necessary facilities to ensure the riser emergency shutdown valve and shutdown system can be inspected and tested including any statutory requirements that may exist. This should include periodic partial and total closure of the valve. There should be no method for overriding closure of the valve.

Riser and sub-sea isolation valves should be closed from the following:-

- (a) Manual push button located at the central control point and at strategic local positions.
- (b) A platform red shutdown.
- (c) Fire or gas detection in the vicinity of the riser valve or pig launcher/receiver area.
- (d) Loss of containment of the associated pipe-line.

There is currently no statutory requirement for a sub-sea isolation valve to be installed on each pipeline close to the installation. However, the formal safety assessment for each installation must consider the potential advantage of fitting one to achieve adequate integrity of the installation design.

Consideration should also be given to closure of riser ESD valves on an installation yellow shutdown unless it can be demonstrated that the integrity of the process plant can be maintained by other ESD valves, inboard from the riser valves. This should be determined by the formal safety assessment for the installation.

D6.2.5 Flare and Vent Extinguishing System

Consideration should be given to the provision of a system for the rapid extinguishing of flares and cold vents. Circumstances when a flame may need to be extinguished are:-

- (a) A well blowout.
- (b) Accidental release of hydrocarbons from the process where ignition from the flare could result in increased hazard.
- (c) Structural damage to the flare system.
- (d) Accidental ignition of cold vents.

Where provided, flare snuff should be initiated from dedicated manual push buttons located at the main control point and at strategic locations in the drilling and flare areas.

The decision whether to provide a flare and vent extinguishing system will depend on the measures available and the consequence of initiating such measures. The use of Halons for such systems is now actively discouraged, and in some areas may not be permitted, due to environmental impact.

Where provided, the system should extinguish all pilots and main burners on the flare system, and all cold vents.

The requirement for initiation of a yellow shutdown, followed by flare/vent extinguish, should be considered. Where included, the flare/vent extinguish should be initiated after a suitable time delay. The rate of decay of the flaring/venting flow rate will determine the delay time and the measures required to ensure effective flame extinguish.