HSE

Health and Safety Executive

Optimising hazard management by workforce engagement and supervision

Prepared by **Risk Support Limited**
for the Health and Safety Executive 2008

RR637
Research Report

HSE

Health and Safety Executive

Optimising hazard management by workforce engagement and supervision

Vladimir M Trbojevic
Risk Support Limited
88 Kingwood Road
London
SW6 6SS

Offshore oil and gas duty holders have recognised that a lack of skilled workforce, change to shorter working hours and increase in activity can lead to an erosion of health and safety unless balanced by significant increase in level of training and supervision. The way forward suggested in this report is based on:

a) improving comprehension of major hazards by the workforce; and

b) optimising the management processes such as balancing workforce competence and level of supervision.

By improving comprehension of major hazards the workforce itself can play a central role in safety case preparation by being involved in identifying real improvements in safety that are reasonable and based on the day-to-day grass-roots operational experience of various disciplines. Workforce involvement in optimising safety management processes not only increases the experience of the group of workers who can contribute to the process (contributory expertise), but also of other groups of workers who acquire interactional expertise. Safety optimisation can be applied to any process by challenging the existing situation along the lines ‘what more can we do’, or ‘how can we do it better’, etc. Evaluating complexity of protection systems is based on understanding the work that has to be done to maintain, control and operate protective systems, and the available competence.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the author alone and do not necessarily reflect HSE policy.

HSE Books

First published 2008

ACKNOWLEDGEMENTS

The author would like to thank the following companies for their participation in this work:

Hydrocarbon Resources Limited

ConocoPhillips (UK) Limited

CONTENTS

EXECUTIVE SUMMARY ..... **vii**

1 INTRODUCTION **1**

2 CONTROL OF RISK **4**

2.1 DEFINITIONS 4
2.2 BOW TIE METHODOLOGY 5
2.2.1 Introduction *5*
2.2.2 History of bow tie method *5*
2.2.3 Hazard identification *5*
2.2.4 Development of cause-consequence model *6*
2.2.5 Energising lines of defence *8*
2.2.6 Qualitative risk evaluation *9*
2.3 SOCIO-TECHNICAL APPROACH TO FAILURES 9
2.3.1 Introduction *9*
2.3.2 Types of failures *11*
2.3.3 Causes of failures *12*
2.3.4 Proposed failure scheme *14*
2.3.5 Proposed barrier model *15*
2.4 BARRIER RULE SET 15
2.4.1 Classification of barriers *15*
2.4.2 Primary and secondary barriers *19*
2.4.3 Barrier decay and failure modes *19*
2.4.4 Application suggestions *25*
2.5 BARRIER PARAMETERS 25
2.6 ACTUAL WORKFORCE INVOLVEMENT 28
2.6.1 Major hazard awareness workshops *28*
2.6.2 Improving safety management *29*
2.7 ADVANTAGES OF BARRIER APPROACH 31
2.7.1 Visualisation of hazard protection *31*
2.7.2 Visualisation of accident causation *32*
2.7.3 Safety case *34*
2.7.4 Contributing to improving resilience *35*

3 CONTROL OF RISK MANAGEMENT PROCESS **37**

3.1 APPROACH TO TOLERABILITY OF RISK MANAGEMENT PROCESS 37
3.1.1 Management of health and safety and control of major accident hazards *37*
3.1.2 Focus on risk management process *38*
3.2 OPTIMISING BALANCE BETWEEN COMPETENCE AND SUPERVISION 40
3.2.1 Introduction *40*
3.2.2 Approach *41*
3.2.3 Development of the model *44*
3.2.4 Rating of safety (criticality) *44*
3.2.5 Rating of complexity/competence matching *45*
3.2.6 Rating of supervision *46*
3.2.7 Convergence of judgments *48*
3.2.8 Demonstrating optimal balance between competence and supervision *49*

4 WORKFORCE INVOLVEMENT **51**

4.1 INTRODUCTION 51
4.2 IMPROVED COMPREHENSION OF MAJOR HAZARDS 51
4.3 IMPROVEMENT OF SAFETY BY INVOLVEMENT IN SAFETY CASE 52
4.4 IMPROVEMENT OF RISK MANAGEMENT PROCESSES 52
4.5 INVOLVEMENT IN SAFETY MANAGEMENT SYSTEM 53

4.6 IMPROVING SAFETY MANAGEMENT AUDITS 54

5 REFERENCES 55

APPENDIX A – WORKFORCE RESPONSE TO BARRIER APPROACH 58
APPENDIX B – EXAMPLES OF BOW TIES 60
APPENDIX C – CURRENT PRACTICE IN COMPETENCE ASSURANCE 77

EXECUTIVE SUMMARY

Introduction

Today's industrial sectors face a stark reality. Eroding health and safety threatens to become endemic due to the economic growth in all developed economies, labour shortage, the lack of skilled workers and the aging workforce. Safety performance is being severely compromised by an insufficiently skilled workforce and inadequate levels of training and supervision.

This study aims to reset the equilibrium between the level of workforce competence and the level of supervision required to improve safety performance to an acceptable level. This can be achieved by improving:

1. Understanding by the workforce of hazard management, and
2. The organisation and focus of supervision in order to restore an optimal balance between workforce competence and level of supervision.

Bow tie approach

The bow tie approach was utilised to present the major hazards of the facility in such a way as to facilitate workforce understanding of hazard management and their role in it. In this approach hazard is represented by a top event (realization of hazard) which can be triggered by one or several threats. The barriers are provided to protect the system from these threats, Figure i.

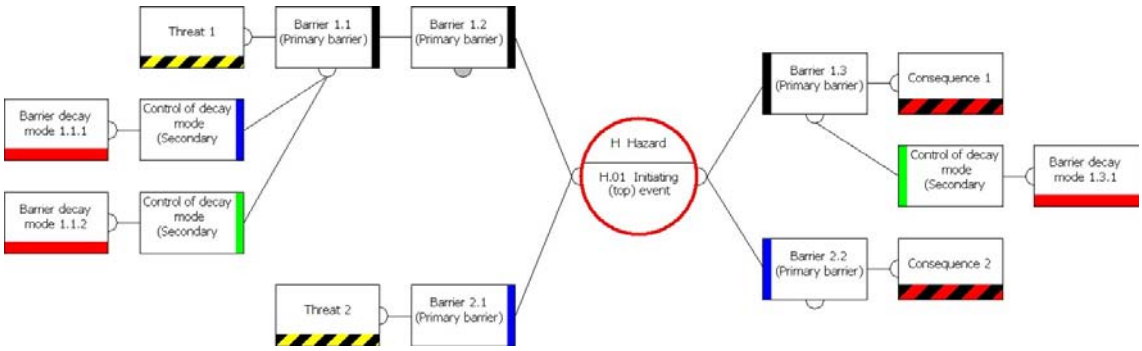


Figure i Bow tie

Optimising safety management processes

The objective is to achieve the optimal balance between workforce competence and supervision, the following observation is made. Balancing competence and supervision is just one of the processes within the safety management system. Opportunities for decay and erosion of the hazard protection system are many, from inadequate design, insufficient maintenance, unworkable procedures, conflicting goals, failure in communication, insufficient training, etc. While the monitoring and auditing procedures should be designed for a continuous improvement in reality these are often transformed into compliance audits. The improvements in overall safety level cannot be reached by monitoring and targeting annual safety indicators alone, but also requires improving processes of the system from which these indicators originate. Therefore an approach for optimizing the management process for balancing workforce competence and the need for supervision is developed in this study. The method

enables an organisation to demonstrate that so far as is reasonably practicable the optimal balance between competence and supervision can be achieved

Findings

The proposed approach has the potential for significant improvement of workforce involvement and understanding in the following areas:

Comprehension of major hazards

Visualisation of threat / barrier / initiating event / consequence systems in bow tie diagrams facilitates comprehension of hazard prevention and protection required for safe operations on an offshore facility. The interaction and interdependence between the primary barriers and their decay/failure modes and the secondary barriers are also visually displayed. Removing a barrier or a set of barriers for the purpose of maintenance can immediately indicate the possible weakening of the system.

The role of the barrier rule set developed in this study is important as it empowers the workforce to develop the bow tie diagrams themselves without relying on external specialists. The rule set facilitate channelling of the workforce experience, knowledge of facility specifics, of near misses, etc into better understanding of major hazards and possible improvements.

Safety case

The HSE has highlighted the central role that the offshore workforce can play in safety case preparation by being involved in the engineering task of identifying real improvement in safety, improvements that are reasonable from an engineering perspective that makes full use of the day-to-day and grass-roots operational experience of various workforce disciplines. The bow ties facilitate a more intimate participation of the workforce in the processes of hazard identification which forms the solid foundation on which the continuous safety improvement is built.

Operational competences

Involvement of the workforce in optimising safety management processes is essential for the following reasons:

1. The workforce involvement in optimising processes not only increases the experience of the group of workers which can contribute to the process (contributory expertise) and but also of other groups of workers who acquire interactional expertise. Interactional expertise facilitates the understanding of the overall issues related to the particular facility. This would in particular apply to identification of threats, underlying causes of failure, etc.
2. Evaluating complexity is based on understanding the work that has to be done on the barrier (to maintain, control or operate it) and the available and required competence. By understanding why and how something has to be done on the barrier, facilitates appreciation of the barrier function and its failure. This task increases not only contributory expertise, but also the interactional expertise as other workers learn how to conduct the analysis of a process without necessarily doing or understanding all the specifics of the process.
3. Understanding safety optimisation (the goal-setting approach to safety) serves as the basis for safety training. Safety optimisation can be applied to any process by challenging the

existing situation along the lines “what more can we do?”, or “how can we do it better”, “what can we change?”, etc.

Safety management system

Increased and focused information about the major hazard accidents, barriers, procedures and tasks should facilitate discussions, assessment and improvements of safety. This is in particular important with the human / organisational barriers such as Job Risk Assessments, Permit to Work systems, plans, manuals, etc. Both the workforce and the management can also visualise the importance of fundamental barriers such as management of change, procedural reviews, corporate audit, etc. The following areas of safety management which seem to be directly linked to the barrier approach, have the potential for improvement:

1. Raising safety issues and monitoring their handling by management. Visualisation of the distribution of responsibilities for barrier facilitates monitoring of their handling by the management and workforce.
2. Knowledge of major hazards and the facility experience empower the workforce to challenge the decisions made by management in their determination of the reasonable practicability of proposed improvement. It is envisaged that most of the improvements will be in systems of work, the way things are done, however improvement of technical barriers is by no means excluded.
3. Training – it is often the case that members of the workforce themselves are conscious of the need for further training, for maintaining and developing relevant skill, and may be concerned when there is inadequate provision for such training. It is essential that in such situations there is a system in place to raise training needs issues, to prompt the management to pursue these issues and to enable the workforce to monitor the progress of the issues and challenge any decisions or lack of management action as the need arises.
4. Organisational learning – near miss and accident investigation, best practice review, corporate audit, etc serve to update the existing experience pool which can be used for further safety improvements. Barrier model is can serve as depository of major hazards knowledge and as means of transfer of knowledge from the experienced workers to the newly employed.

Improved auditing

The proposed approach linking the major hazards, underlying causes of barrier decay/failure, complexity of safety critical tasks, barrier decay levels and the workforce provides more opportunity for proactive monitoring and consequently improved auditing system for the following reasons:

1. Most relevant barrier decay modes (underlying causes of failure) are identified and the secondary (fundamental) barriers are in place to detect latent conditions and strengthen the primary barriers. The reason for and the importance of monitoring of the barrier decay modes and the secondary (fundamental) barriers are visible and understood by the workforce.
2. Barrier decay level can be used to control the frequency of application of fundamental barriers such as audits.
3. Barrier decay level is also an indicator of barrier “robustness” which in the case of rapid decay and increasing frequency of audits can highlight the need to redesign or strengthen the primary barrier. Hence, rapid decay can be used as an indicator of the weakness of the primary barrier.

1 INTRODUCTION

This Joint Industry Project (JIP) is the result of a shared concern on how to improve workers' involvement in hazard management and deal with the lack of skilled workforce in the future. One of the results of the economic growth in all developed economies is labour shortage, the lack of skilled workers and the aging workforce. Lack of skilled workforce and change to shorter working hours inevitably leads to an erosion of health and safety and/or significant increase in level of training and supervision. This means that the established "equilibrium" between the level of competence of the workforce and the level of supervision by competent supervisors will be negatively affected. In order to achieve this goal a two pronged approach is proposed:

1. To improve understanding by the workforce of hazard management and thereby facilitate their effective involvement, and
2. To improve the organisation and focus of supervision in order to restore an optimal balance between workforce competence and level of supervision.

Workforce involvement in health and safety has been the focus of previous HSE sponsored research (HSE, 2000). This work has identified that companies approach the aim of greater workforce involvement a) by ensuring that management and employee roles specify their respective remits in identifying and resolving safety issues as well as implementing safety arrangements, and b) by undertaking a two-way communication process to elicit any concerns held by management and employees regarding the new arrangements. As the result of this and other studies companies have involved the workforce in risk assessments, created teams to identify and resolve health problems, involved employees in developing procedures, training packages, implemented participation in safety days, accident investigation, etc.

All of these and other measures have produced partial safety improvements and workers' involvement, mainly in the field of occupational safety as distinct from process safety. The analysis of large accidents (HSE, 2007a) indicated amongst others, organisational learning, memory and knowledge failures in relation to major accident prevention, inadequacies in providing management and employee competence, etc. Inspection of nearly 100 offshore installations (HSE, 2007b) found amongst other shortcomings that there is poor understanding across the industry of potential interaction of degraded non safety critical plant and utility systems with safety critical elements in the event of a major accident, that the role of asset integrity and concept of barriers in major hazard risk control is not well understood, poor performance in management systems has been further exacerbated by a workforce that is depleted in experience, etc. The reports from the HSE's inspectors point to poor procedures, lack of competence or lack of supervision as the main causes of process safety incidents often involving major hazards. It can be concluded that these issues share a common cause which is failing to deliver the appropriate knowledge to the work site (Miles, 2006). Improvements in the area of major hazards have been insufficient for several reasons:

1. Socio-technical systems (in which structural, equipment and human reliability depend on the management processes, organisation and the safety culture in which the organisation operates) are so complex that it is practically impossible for one or several persons to know the system intimately.
2. Complexity of failure propagation paths; the interaction between different failure modes of different components is neither straight forward nor intuitive. As the technical system design becomes more complex, attention cannot be limited to system failures resulting from one or two component failures. Such failures can result either from basic design

faults or from human failure to follow safety critical procedures, often because the purpose for these, i.e. what they protect, is not fully understood.

3. Insufficient knowledge and inadequate management procedures for linking and reinforcing the major hazards knowledge, trade/skill knowledge (competency) in operations and management and, local knowledge and experience (supervision) of such complex systems.

The approach proposed here is based on very simple propositions:

1. The process of management of major hazards in a socio-technical system has to focus on safety critical systems, barriers and procedures presented in a simplified and yet realistic manner, so that
2. The workforce can easily understand the main hazard issues and can recognise themselves as the "owners" of hazard barriers in their day-to-day tasks, and
3. That the essential underlying causes of barrier decay or failure are identified and displayed in an understandable form, their consequences clear, that the additional controls are in place to prevent these decay / failure modes, and that the responsibility or ownership of these controls can be traced back to management and organisation of the main safety critical tasks.

Therefore the first goal is to present the hazard model of the facility in such a way as to facilitate workforce understanding of hazard management and their role in it. The socio-technical hazard model will be developed using the bow tie approach. In the bow tie approach hazard is represented by a top event (realization of hazard) which can be triggered by one or several threats. The barriers are provided to protect the system from these threats. The bow tie representation can be viewed as bringing together in one view the two components of the hazard model that are usually handled in separate and distinct ways. These are a) the basic primary protection model, and b) the underlying incident causation and prevention model. The reason for this "artificial" subdivision is as follows:

The details of the hazard protection are typically treated in the safety case. However, explicit mapping of this information into the bow ties is not difficult. This model consists of threats, primary preventive barriers, top event, primary mitigation and protection barriers and consequences. The workforce in general is aware of this information from the safety case and safety briefings. Visualization of this information via bow ties contributes to easier and better understanding of barriers and their links to the workforce.

The details of underlying incident causation and prevention, consisting of barrier decay and failure modes and the secondary barriers targeting these modes and reinforcing the primary barriers are not explicitly defined in a safety case. However, the issues can be treated using the results of various human factors initiatives. The development of this part of the bow ties requires incorporation of the human, management and organizational factors (i.e. the underlying causes of failure) on the primary hazard protection barriers. In order to facilitate the understanding and incorporation of this information a barrier rule set will be developed. The **barrier rule set** will allow the workforce to identify the most relevant decay modes for each barrier and the most relevant secondary barriers for these decay modes. This information offers an insight into near miss and incident causation, and the role of the workforce and management in this process. It is also important because it facilitates explicit measurement of organizational performance which, if properly utilized, increases the resilience of the safety management system (SMS).

To achieve the second goal, i.e. to optimise balance between workforce competence and supervision, the following observation is made: balancing competence and supervision is just one of the processes within the safety management system. Furthermore, the opportunities for decay and erosion of the hazard protection system are many, from inadequate design, insufficient maintenance, unworkable procedures, conflicting goals, failure in communication, insufficient training, etc. The SMS monitoring and auditing procedures can identify weakness in the protection system and in general help in patching the system up. What is actually needed in parallel with monitoring and auditing, is the optimal design of the processes within the system. It would then be logical to expect that such an optimized management system will be more resilient to erosion and decay of the protection system. This observation is fortified by findings that, on the ground, in the work-space, the demonstration of safety is often separated in time from the management of safety and that a continuous improvement is transformed into compliance audits. Compliance audits are used to ensure compliance with the previously defined procedures and checklists in a way that resembles the quality management or "we check that we are doing what we are supposed to do". Questions such as "why is there non-compliance" or "is there a better way of doing things that would avoid non-compliances" are very seldom asked. A question "have the procedures been developed within the framework of goal-setting approach to safety" is almost never posed. Therefore the approach for optimizing the balance between workforce competence and the need for supervision will be developed by applying the goal-setting approach for maximizing safety to the safety management processes. The test for reaching the optimum of the management process will be based on as far as is reasonably practicable (SFAIRP) criterion (Health and Safety at Work etc Act, 1974). This will lead to demonstration of the achievement of the two main goals of the study, which are as follows:

1. To simplify the risk concept and ensure a sensible approach to risk management which will facilitate workforce involvement in hazard management, and
2. To demonstrate how all reasonable measures can be applied to achieve an optimal balance between workforce competence and the level of supervision needed.

2 CONTROL OF RISK

2.1 Definitions

Hazard is a physical situation, condition or material property that has the potential to cause harm such as sickness, injury or death to people, damage to property and investments, environmental damage, business interruption and loss of reputation. A container with flammable material is a hazard because it has the potential to cause fire and/or explosion; an installation operation consisting of lifting a module onto an offshore platform is a hazardous activity because it has the potential for dropping or releasing the module too fast causing damage to the platform.

Threat refers to the means by which a hazard may be realised (HSE, 1995). For example, hydrocarbon under pressure is a hazard for an offshore riser, while corrosion is one of the threats which could trigger the realisation of the hazards. A threat can be made actual, such as an object dropped on the riser causing a leak, or a barrier preventing the threat initiation can be breached, for example by disabling a pressure relieve valve.

Accident (initiating event, top event) is the realisation of the hazard and unintended departure from normal situation or point of loss of control in which some degree of harm is caused. The term initiating event is used in the offshore industry, while a top event denotes the event on the top of the fault tree and is synonymous to the initiating event. For example, hydrocarbon leak from a riser is an initiating event.

Consequence is the result that follows the realisation of hazard or degree of harm caused by an accident. This harm may be expressed in terms of injury or death to people, damage to the environment, loss of assets and reputation, etc.

Barrier (Oxford dictionary: *a fence or other obstacle that prevents movement or access*) in safety sense is a design feature. It may be physical or non-physical or a combination, and the intent is to prevent, control, mitigate or protect from accidents or undesired events. Examples of barriers are: a corrosion protection system is a barrier that protects the riser from corrosion, an emergency isolation valve limits the hydrocarbon inventory available to leak in the case of an incident, deluge system mitigates the effects of fires, an operator observing the pressure rise in a vessel can control the process by initiating blowdown, etc.

Barrier decay / failure mode indicates the departure of the barrier function from the design intent. It may result from decay in barrier function, a complete failure, or a removal of the barrier (Rimington, 2007). Examples of barrier decay are: a valve after certain time developing a leak, personnel training in emergency procedures allowed to lapse, etc. Examples of barrier failure is valve which fails to close on demand, instrument that stopped functioning, blocked deluge nozzles, etc. Example of removal of a barrier would be if an operator leaving the Control Room, etc. Barrier decay mode is also called “escalation factor” (SIPM, 1995).

Resilience is the characteristic of the safety management of process activities to anticipate and circumvent threats to its safety and production goals.

2.2 Bow tie methodology

2.2.1 Introduction

Due to the complexity of modern facilities, it is difficult for the operators to envisage all possible interactions if something were to go wrong. An offshore installation which is a socio-technical system for the purpose of risk analysis is currently mapped into mainly technical risk model. The human, management and organisational factors which are the major contributor to failures are treated outside the quantitative risk analysis (QRA). In this study the complete socio-technical system is mapped into the hazard protection model using different technique. This technique avoids using Boolean logic (e.g. yes/no, 1/0) to distinguish between an operational barrier and its failed state by introducing a state of "barrier decay" or weakened but not eliminated defences and thus allows modelling of underlying causes of barrier decay or failure. By avoiding quantification of risk, this technique is extended to mimic relationships between the threats, barrier systems, the workforce which controls and maintains these systems and the management. This approach is expected to be easily understandable by the workforce.

It has been accepted in safety practice that better understanding of the hazard protection model by the workforce would facilitate comprehensive engagement of the workforce into hazard management resulting in improved safety and the resilience of the safety management system. In order to engage the workforce in hazard management, the hazard model of operations is presented in the form of bow ties with barriers linked to people who operate the facility and who are responsible for maintaining the barriers. The barriers (risk controls) are the main handles for controlling the threats. In addition, knowledge of major hazards, facility operations and maintenance are embedded in barriers.

2.2.2 History of bow tie method

The first bow tie software called THESIS, was developed by Shell International Exploration and Production (SIEP, 1995) in the 1990's 6, based on the work by James Reason (1998). THESIS was designed to be used by the management and the workforce in collection and presentation of essential data needed to prepare a Health, Safety and Environmental Management System. Due to SIEP's requirement it is widely used for safety cases for the offshore drilling facilities. The approach was also used for risk analysis and the basis of the safety management system for marine operation in several ports in the UK (Trbojevic, 2001), and for operations of heavy lift and transport vessels (Trbojevic, et al., 2007). It was also used in the COMAH (HSE, 1999) safety reports for petro-chemical industry. Most of the usage is at the stage of hazard identification and collection of information. Resultant bow tie models have, in general, a large number of "barriers" and may give a false impression of high safety. In reality most of the barriers are not effective once the threat is realised and represent just existing safety practice in terms of procedures, notices, etc. This was an important reason for developing a rule set for the barrier usage which would better mimic the facility's protection systems.

2.2.3 Hazard identification

The starting point for this approach is hazard identification. Hazard identification should be undertaken with the workforce with the aim of ensuring understanding the threats that may be initiated to cause realization of hazards. This can be done by using a checklist, by critically rehearsing the activities and tasks on the site, and by brainstorming with the workforce to encourage participation and understanding. A diverse team experience is very beneficial. Therefore, the workforce is involved in activities / tasks and hazard identification. On existing installations most of this information should be available in the QRA. As the result of this exercise the hazards are mapped into initiating events.

2.2.4 Development of cause-consequence model

The next step is the development of cause-consequence model from the information obtained. In the bow tie approach the development of the causation part (or the left hand side of the bow ties) starts by listing all threats that can lead to an initiating event. The next step is to explore the barriers that already exist or could be put in path of these threats to prevent their initiation. Once the causation part is completed, the focus is on escalation from the initiating event to possible consequences. For each consequence a set of barriers exists or could be established which detect the accident, protect from or mitigate its consequences. A bow tie model for the sequence from threats to consequences is shown in Figure 1 (Risk Support, 2007).

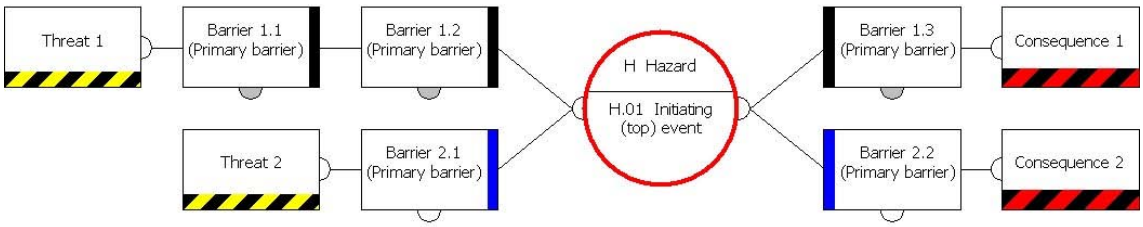


Figure 1 Hazard bow tie

The initiating event is denoted by a red circle in the middle of the bow tie, boxes with black/yellow stripes at the bottom are threats, boxes with black/red stripes are consequences, while the boxes with the vertical thick bar are barriers. As an example of barriers the following accident description is presented.

Crane Driver Error[1]

The lay-down area as designed was too small and was extended past the pipe shuttle but the part of the new area beyond the shuttle was not visible by the crane driver. This hazard was identified by designers and a closed circuit TV camera was placed on the crane jib looking down and the screen was in the crane cab. On the day of the accident a camera was not working and the part is on order. A rule was introduced that a banksman must be present at all

[1] Text in blue italic letters indicate description of accident

times during lifting and a second rule that there must be no more than two persons on the lay-down area at one time.

A bow tie for this accident is very simple: a threat in this case is poor design of the lay-down area, initiating event is lowering (dropping) the load and the preventive barrier (on the left hand side) is a banksman who is guiding the crane driver. On the right hand side the barrier is a permit to work system which has to ensure that there are no more than two workers in the lay-down area[2].

It has been mentioned that a barrier can decay, perform inadequately or fail. Barrier decay or failure modes express deterioration of the barrier functions. A technical barrier like a blast wall can fail if the explosion overpressure exceeds the design overpressure. An operator (barrier) can also fail if the operator leaves his post, violates the procedure, fall asleep, etc. A procedural barrier such as permit to work system can decay if there is too much paper work, or if there is a lack of safety culture, or if carrying out tasks and procedures is not monitored. This is shown in the continuation of the accident description.

Crane Driver Error (cont.)
The banksman confirms to the crane driver that there were two people working in a basket A on the lay-down area. They were out of the view of the crane driver. The banksman is called away (removed barrier!). Two more people working for a different company go to work in a basket C on the lay-down area in the view of the crane. The crane driver sees two people in a basket C and assumes these were the two he has been told about (failure of the permit to work barrier). He makes a lift and the load is dropped onto basket A and onto the two people originally on the lay-down area. One is killed.

This accident took place because both barriers (banksman and permit to work system - PTW) were breached and there were no controls for the barrier decay modes. For example, "absent banksman" and the control "stop lifting operation", and "inadequate compliance monitoring" (regarding PTW system) with the control "procedural review", etc.

Graphical representation of this accident is presented in Figure 2. The boxes without thick vertical bars represent the barriers that were not in place. The boxes with the red horizontal bar

[2] Text in black italic letters indicates the approach to accident from the point of view of barriers

represent barrier decay/failure modes and the boxes next to decay/failure modes are secondary barriers which were not in place (hence there is no thick vertical bar in those boxes).

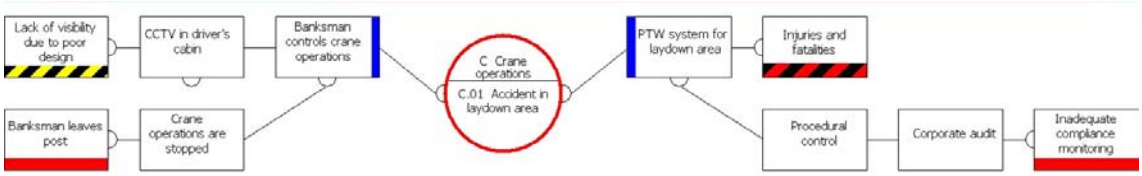


Figure 2 Barriers and barrier decay modes

It should be noted that barriers "CCTV in driver's cabin", "crane operations are stopped", "procedural control" and "corporate audit" do not have a vertical bar in the barrier box to indicate that the barriers were non-existent.

2.2.5 Energising lines of defence

Having mapped all identified initiating events into bow ties and incorporated all existing and newly identified barriers, the organisation for safety can be carried out. This means that a set of safety critical tasks is identified, the purpose of which is to ensure that barriers are operational at all times. This is typically an iterative process and it is carried out in parallel with identification and provision of barriers. The reason why the process is iterative is that, in general, the safety management system and its procedures do not focus on the barriers the same way as the bow ties. However, it is possible to link the barriers to the corresponding task or set of tasks. This is shown in Figure3. In the bottom row of each barrier there is a post indicator of a person (e.g. E1, O1, etc) responsible for the barrier and the task or set of tasks the purpose of which is to ensure its proper operation (e.g. A.01.01, A.02.02, etc).

In this way, common mode failures such as having one person in charge of all barriers along a threat path can be avoided. This approach allows the workforce to see clearly the distribution of responsibilities, the potential consequences of barrier erosion or failure to execute that task, and to become "risk owners".

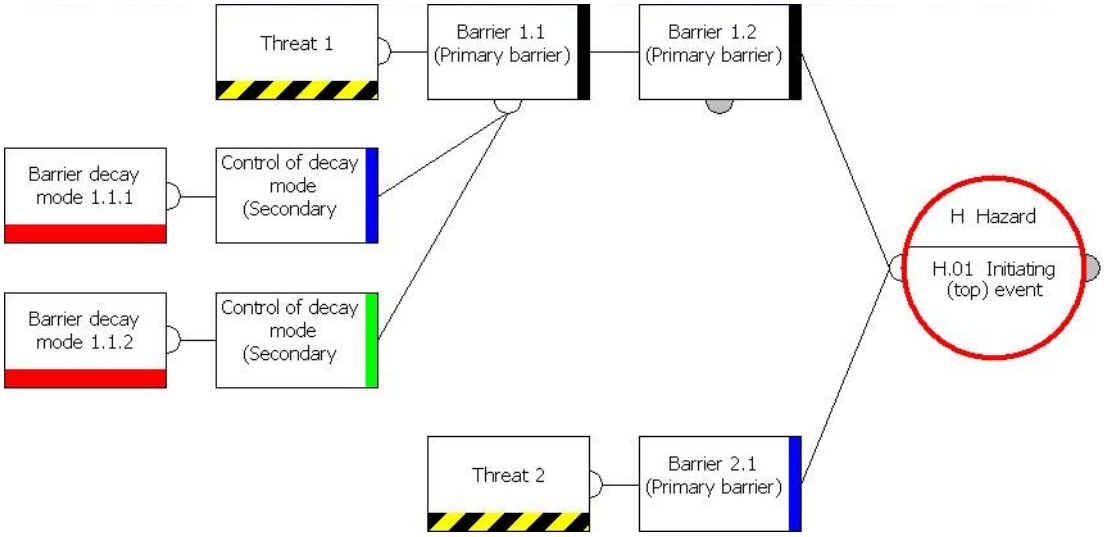


Figure 3 Linking hazard protection to personnel activities

2.2.6 Qualitative risk evaluation

For the sake of completeness, the extension of the bow tie model to the qualitative risk model is described here as well. Qualitative risk assessment requires the following steps:

1. The judgment is made about the likelihood and the severity of each consequence (of each event) without reference to the barriers. A risk matrix type approach can be utilized for this purpose, and the risk (combination of likelihood and severity) can be assessed on a three point scale, for example, low, medium and high.
2. Risk is assessed against risk acceptance criteria. The criteria are based on the minimum number of barriers required for each risk level. For example, the condition for the low level of risk would require the minimum of one effective barrier for each threat and one barrier for each consequence, for the medium level it would be the minimum of two barriers for each threat and one barrier for each consequence, and so on. The "effective" barrier is the barrier which can prevent the threat realization, attenuate it, or mitigate the effects of hazard realization. The criteria can be further extended by requiring, for example, that all barrier decay modes are provided by the suitable controls, i.e. secondary barriers which should prevent these modes, etc.

The purpose of this risk model is to focus the minds on the effective and important barriers and at least in a judgmental way show the change in the qualitatively evaluated risk if a barrier is removed and the number of barriers fall below the acceptance condition.

2.3 Socio-technical approach to failures

2.3.1 Introduction

An overview of failures is presented here with the following main objectives:

1. To facilitate the identification of the barriers with the potential to prevent and protect from failures
2. To identify barrier decay modes and consider the types of secondary barriers that would prevent barrier decay or failure.

In the last 30 or so year it has became clear that most of the causes of failures could be traced back to a combination of one or more of human error, inadequate design, poor maintenance, degradation of working practices, inadequate training, poor supervision, excessive working hours, poor safety management, and so on, or what is called human, management and organizational factors. Major accidents for which some of the above mentioned factors were implicated were: Three Mile Island (1979), Chernobyl (1986) in the nuclear industry; Piper Alpha (1988) in the offshore industry; Herald of Free Enterprise (1987), Clapham Junction (1988) in the transport industry; Bophal (1984), Texaco Refinery, Milford Haven (1994), Texas City Refinery (2005) in the chemical industry (Kletz, 2006). The main approaches that have been applied to analyse, estimate and reduce human, management and organizational error in industrial systems are as follows:

1. Traditional safety engineering focuses on the human factors that give rise to accidents and emphasises behavioural modification as risk reducing measure. Behavioural modification can be achieved through motivation, education or punishment.
2. Human factors engineering / ergonomics focuses on the mismatch between human capabilities and the demands of the system as the main causes of human error. Hence the

risk reducing measures include workplace and job design, human-machine interface design, improvement of the physical environment and optimisation of the workload.

3. Cognitive systems engineering focuses on the analysis of work practice, structure, purposes and constraints in order to design the process and technology for human-system integration. It assumes that people impose meaning on the information they receive, and that their actions are directed to achieving some explicit or implicit goal. The approach is considered as most comprehensive for evaluating the underlying causes of errors. It is also particularly applicable to planning and handling abnormal situations.
4. Socio-technical systems consider that human and technical performance is influenced by organisation and management of the industrial activities, by the safety culture and by external factors such as regulations, market pressures, political pressure, etc, Reason (1998), HSE (1992b).

The socio-technical systems approach has been adopted in this study. This model is based on recognition that many different factors influencing operator error or equipment failure operate at different levels in a system. These levels are determined according to proximity to the actual occurrence of error in the front line task or failure in safety equipment, from the close to the most remote level, as shown in Figure 4, (HSE, 1992b). The levels are explained briefly below.

Level 5: System climate

This is the climate within which a particular organisation operates, such as the economic and regulatory climate. At this level the organisation and management can be affected by factors outside the boundary of the system over which they have direct control, e.g. by economic pressures. Any company managing hazards should be aware of these and have mechanisms for dealing with such important influences. An obvious one would be the way in which an organisation keeps itself updated on current guidance and regulations. A company's safety culture plays an important role in it approach and commitment to safety.

Level 4: Organisation and management

This level refers to organisational and management structures and objectives, standards, targets, priorities, programmes, strategies, policies, etc., operating within a particular organisation. It defines the safety policy and goals and sets in place the organisational systems, structures, roles and responsibilities by which this is achieved and maintained, both in the short and long term. This should not be a static process as it can be expected that organisational learning will take place.

Level 3: Control, communication and feedback processes

In order to achieve the safety goals of the organisation, there is a need to have control, communication, coordination and feedback processes to ensure that the system operates according to its intended goals. It is also necessary to determine whether deviations from goals are occurring and need correcting. Therefore this level addresses the ways in which control, communication, coordination, and information dissemination occur within the organisation and the processes by which appropriate feedback relating to deviations from system goals are acquired, communicated and acted upon.

Level 2: Operator reliability

Codes, procedures, tools, instructions, etc., are examples of external constraints within which personnel are required to operate. In addition, the ability of personnel to meet task demands will depend on intrinsic personal factors (skills, knowledge, motivation, etc.). This level addresses the match between personnel competencies and the task support provided.

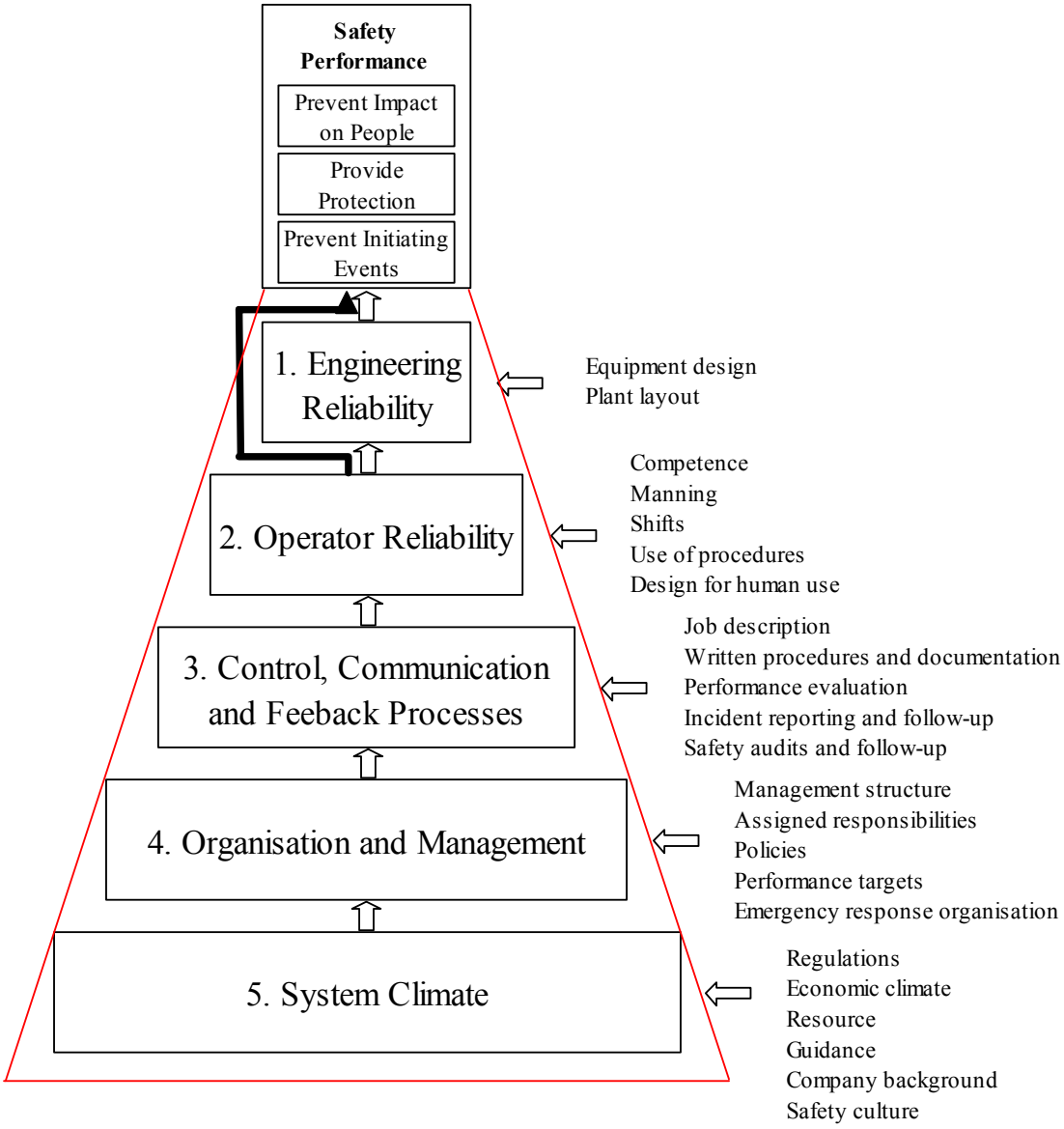


Figure 4 Socio-technical pyramid

Level 1: Structural and mechanical reliability
This level refers to the design and maintenance of the plant or system. It only includes those aspects of the design and maintenance the failure of which could lead directly to an initiating event, given a triggering condition.

2.3.2 Types of failures

There are in general two types of failure or human error:

1. Direct or active failures / errors the effects of which tend to be felt immediately, for example, containment failure leading to the release of hazardous material, operator failure to initiate manual shut down on detection of the release of hazardous material, etc.
2. Passive failures / errors where error occurrence is separated in time from its effects. James Reason (1998) uses the term "latent conditions" which comprise, for example, poor design, insufficient maintenance, inadequate training and supervision, unsuitable

procedures, etc. Passive failures / errors can stay dormant in the system and need a trigger to cause an accident. A "trigger" is usually a combination of active failure or some external factors which manage to penetrate several layers of defences (Reason, 1998).

2.3.3 Causes of failures

The research programme on the contribution of human error and socio-technical failures to pipework failure frequencies carried out for the Health and Safety Executive (Hurst et al., 1991) led to the development of the failure classification scheme used to analyse about 500 reported incidents involving failure of fixed pipework on chemical and major hazard plants. The objective of the classification scheme was to make a distinction between human error and other direct or immediate cause of failure and the underlying causes of failure of the socio-technical system. The results of this analysis show that 90% of the analysed incidents could have potentially been prevented by suitable preventive mechanisms which in theory are within the scope of management control.

The list of direct and underlying causes of failure and preventive mechanisms from this approach are presented in Table 1. This failure classification scheme should be viewed as three-dimensional with the direct causes of failures along the vertical axis, and the base or route (underlying) causes and the preventive mechanism along two horizontal axes applying to each of the direct causes.

Table 1 Direct and root causes of failure (Hurst et al., 1991)

Direct Causes of Failure	Base or Root Cause of Failure	Recovery (Preventive) Mechanisms
Corrosion	Natural causes	Not recoverable
Erosion	Design	Hazard study
Vibration	Manufacture / assembly	Human factors review
Defective pipe or equipment	Construction / installation	Task checking / testing
External loading	During normal operations	Routine checking / testing
Impact	Maintenance	Unknown recovery
Overpressure	Unknown origin	
Temperature	Sabotage	
Wrong equipment	Domino	
Operator error		
Unknown		
Other		

The Tripod approach developed by Reason (1998) within the socio-technical framework is based on three main elements. The first element is execution of an unsafe act (operator error, violation, etc.) within a hazard space which can trigger safety management actions such as training and motivation. If the unsafe act causes the breach of the existing defences on the facility, an incident may occur which is the second element of Tripod approach. Defences are usually associated with inspection and maintenance so breach of defences triggers investigation of the latent conditions that may have contributed to the event. Latent conditions such as poor design, lack of supervision, undetected maintenance failures, unworkable procedures, incomplete training, and so on, may be present for a long time before they combine with local circumstances and active failures (unsafe acts) to breach system defences (Reason, 1998). In

the Tripod approach these latent conditions are categorised into eleven General Failure Types (GFT) and an audit method is established for identifying and managing these. The General Failure Types (GFTs) are as follows:

1. Hardware (HW)
2. Design (DE)
3. Maintenance management (MM)
4. Procedures (PR)
5. Error enforcing conditions (EC)
6. Housekeeping (HK)
7. Incompatible goals (IG)
8. Organisational (OR)
9. Communication (CO)
10. Training (TR)
11. Defences (DF)

Tripod is mainly intended as an audit or evaluation tool to evaluate the shortfalls in the safety management system. The level of presence of GFTs can be interpreted as the level of "safety health" of a system.

The classification scheme based on the analysis of hydrocarbon leaks in the offshore oil and gas industry identifies the immediate (direct) and the underlying causes of failure (HSE, 2003a). The list of these causes from that report is presented in Table 2. The immediate causes of releases correspond to levels 1 and 2 in the socio-technical pyramid in Figure.4, while the underlying causes correspond to the levels 3 to 5.

Table 2 Immediate and underlying causes of failure

Direct Causes of Failure	**Underlying Causes of Failure**
Corrosion (internal)	Inadequate compliance monitoring
Corrosion (external)	Inadequate risk assessment
Erosion	Inadequate design
Fatigue / Vibration	Inadequate procedures
Incorrect installation	Inadequate competency
Operator error	Inadequate supervision
Degradation of material properties	Incorrect material specification / usage
Procedural violation	Inadequate task specification
Inadequate isolation	Excessive workload
Blockage	Outdated information / data
Inadequate procedures	Incorrect installation
Defective equipment	Inadequate maintenance
	In adequate communication
	Inadequate inspection/condition monitoring

2.3.4 Proposed failure scheme

Previously described failure schemes were designed to facilitate accident analysis (Hurst, et al., 1991), (HSE, 2003a), and for auditing the safety management system (reason, 1998). The purpose of the failure scheme proposed here is to proactively facilitate identification of a) barriers preventing and protecting from the direct causes of failures, and b) barriers preventing the underlying causes of socio-technical system failures. Term "proactively" is used here to denote the main aim to make the barriers preventing the underlying causes of socio-technical system failure visible to the workforce and managers.

The starting point for the proposed scheme is the historical accident data in the offshore oil and gas industry, Table 2 (HSE, 2003a). The scheme is then extended so that it could target perhaps yet undetected or unrecorded direct and/or underlying causes of failure. In particular certain underlying causes of failure were added to this list such as incorrect material specification/usage, incorrect equipment specification / usage, design changes/damage during operations, inadequate plans or criteria, lack of safety culture, etc. The emphasis was on operational failures, and typical management and organisational failures such as inadequate goals and strategies, poor management functions and overview, resource allocation, co-ordination of work, organisational learning and/or knowledge, and so on, were omitted. It is assumed that such management and organisational failures would have a) a secondary effect on the operational risks, and b) could be accounted for by considering management and organisational hazards. The list of direct and underlying causes of failure is presented in Table 3. The scheme in Table 3 was developed for the purpose of analyzing a few accidental events in the offshore oil and gas industry. These are typically hydrocarbon leaks, dropped loads, boat collision, etc. Consequently the list of failures is not exhaustive. Further extension of this list may be required for wider applications.

Table 3 Direct and underlying causes of failure

Direct Causes of Failure	Underlying Causes of Failure
Corrosion (internal)	Inadequate design
Corrosion (external)	Incorrect material specification / usage
Erosion	Incorrect equipment specification / usage
External loading	Incorrect installation
Impact	Inadequate commissioning
Overpressure	Design changes / damage / add-ons
Vibration / Fatigue	Inadequate testing
Temperature	Inadequate (poorely controlled) maintenance
Structural defect	Inadequate inspection
Material defect/degradation	Inadequate plan / criteria
Defective equipment	Inadequate procedures
Failure to operate on demand	Inadequate compliance monitoring
Operator error	Inadequate supervision
Procedural violation	Inadequate task specification
Procedure not followed	Insufficient training / competence
Error during maintenance	Inadequate communication
	Demanning / Staff turnaround
	Lack of safety culture
	Excessive workload
	Outdated information / data
	Violation
	Erosion of vigilance
	Time, economic, external pressure

2.3.5 Proposed barrier model

The proposed barrier model linking the direct and underlying causes of failure is presented as a bow tie diagram in Figure 5.

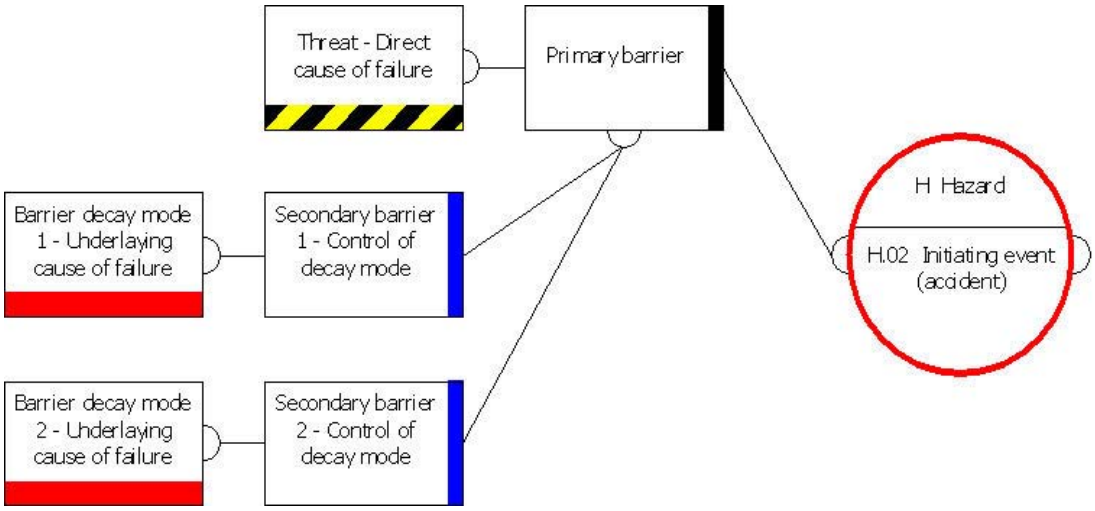


Figure 5 Barrier model

In the bow tie approach if a barrier decay mode (underlying cause of failure) is identified, then the control (secondary barrier) for that decay mode should be specified as well. There could be several possible barrier decay modes (underlying causes of failure) which will need to be matched by corresponding secondary barriers (decay mode controls), as depicted in Figure 5. It should be noted that the barrier decay modes (underlying causes of failure) are primarily caused by management and organizational factors.

The key benefit of using bow ties now becomes clear. The purpose of this approach is to identify the relevant barrier decay modes and the secondary barriers which are associated with the management and organization of the hazardous facility. If this approach were to be applied to risk quantification, by "inverting bow ties" into fault and event trees, the problem of judgmental quantification of failures related to organization and management factors would arise. The reason for this is very simple – there are no data for human and organisational failures. Consequently the quantification is based on expert judgment.

An example of such an approach is given in the Norwegian Barrier and Operational Risk Analysis (BORA) project (Haugen et al., 2007). The benefits of such quantification are far from obvious as it may introduce more uncertainties in an already uncertain estimate of risk. On the other hand, in the bow tie approach, just flagging out management actions and procedures which aim to prevent the underlying causes of failure is beneficial.

2.4 Barrier rule set

2.4.1 Classification of barriers

A good review of barrier definition, classification and performance was given by Sklet (2006). Widely used classification of barrier functions lists prevention, control and mitigation as the main functions, IEC:61508 (1998), IEC:61511 (2002), ISO:13702 (1999). In the ARAMIS project (Salvi and Debray, 2006) four safety functions are identified as follows: avoidance

(suppressing all potential causes of accidents by changing the design), prevention (reducing probability of an event or attenuating its consequences), control (controlling limiting deviations from the normal and emergency situations) and protection (protection from consequences of an event).

Furthermore barriers are classified as physical and non-physical, ISO17776 (2000), hard and soft defences (Reason, 1998), technical or human factors-organisational systems (Svenson, 1991). Classification of barrier systems proposed by Sklet (2006) is shown on Figure 6.

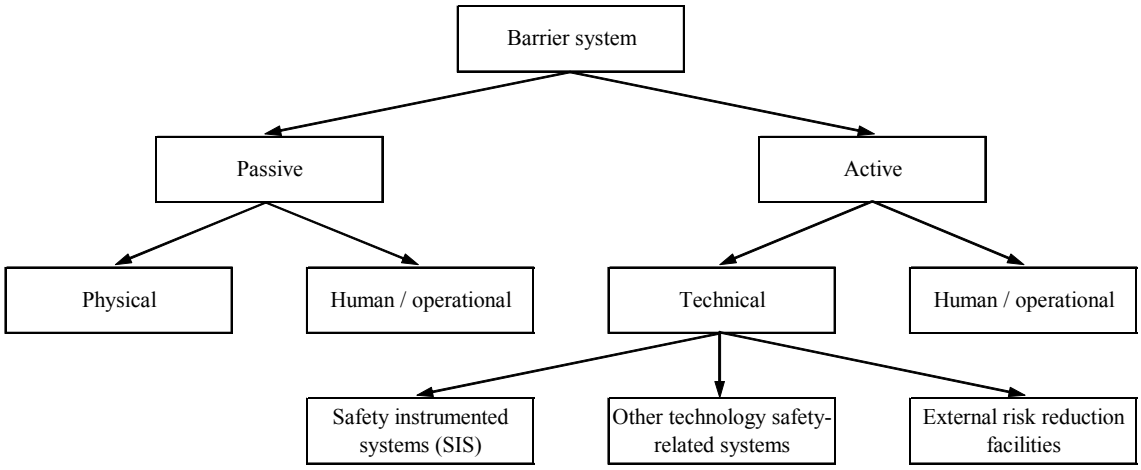


Figure 6 Classification of safety barriers (Sklet, 2006)

Often quoted classifications of barriers was compiled by Hollnagel (1999) and reproduced in Table 4.

Table 4 Barrier systems and barrier functions (Holnagel, 1999)

Barrier System	Barrier Function	Example
Material, physical	**Containing** or protecting. Physical obstacle, either to prevent transporting something from the present location (e.g. release) or into present location (penetration)	Walls, doors, buildings, restricted physical access, railings, fences, containers, tanks, valves, rectifiers, etc.
	Restraining or preventing movement or transportation	Safety belts, harnesses, fences, cages, restricted physical movements, spatial distance (gulfs, gaps), etc.
	Keeping together. Cohesion, resilience, indestructibility	Components that do not break or fracture easily, e.g. safety glass.
	Dissipating energy, protecting, quenching, extinguishing	Air bags, crumple zones, sprinklers, scrubbers, filters, etc.
Functional	**Preventing** movement or action (mechanical, hard)	Locks, equipment alignment, physical interlocking, equipment match, brakes, etc.
	Preventing movement or action (logical, soft)	Passwords, entry codes, action sequences, preconditions, physiological matching (iris, fingerprint, alcohol level), etc.
	Hindering or impeding actions (spatial-temporal)	Distance (too far for a single person to reach), persistence (dead-man-button), delays, synchronisation, etc.
Symbolic	**Countering**, preventing or thwarting actions (visual, tactile interface design)	Coding of functions (colour, shape, spatial layout), demarcations, labels & warnings (static), etc.
	Regulating actions	Instructions, procedures, precautions / conditions, dialogues, etc.
	Indicating system status or condition (signs, signals and symbols)	Signs (e.g., traffic signs), signals (visual, auditory), warning, alarms, etc.
	Permission or authorisation (or the lack thereof)	Work permit, work order.
	Communication, interpersonal dependency	Clearance, approval, (on-line or off-line), in the sense that the lack of clearance etc., is a barrier.
Immaterial	**Monitoring**, supervision	Check (by oneself or another aka visual inspection), checklists, alarms (dynamic), etc.
	Prescribing: rules, laws, guidelines, prohibitions	Rules, restrictions, laws (all either conditional or unconditional), ethics, etc.

For the purposes of this project barriers are classified according to the judgment about the effectiveness of a barrier in case of a threat initiation. A three-point scale of effectiveness (high, medium, low) is proposed based on the following types of the barriers:

1. **Technical barrier** (effectiveness is high) is the barrier which can prevent hazard escalation, attenuate the hazard, mitigate its consequences or reduce its likelihood. If a technical barrier were to fail than the threat would be transmitted to another technical barrier, and so on, before realization of hazards (reaching the initiating event); the same applies for further escalation from the initiating event to consequences (Figure 1). The following sub-categories are also identified:

- **Technical active barrier** which performs on demand, for example emergency shut-down valve, deluge system, stand-by vessel, etc.
- **Technical passive barrier** which performs all the time, for example blast/fire wall, pressure vessel, pipe, etc.
- **Technical control barrier** is a barrier which activates other prevention or mitigation barriers, for example gas/fire detection system, early warning radar system, etc. This type of barrier cannot stop hazard escalation by itself but can initiate other barriers to do that.

2. **Human/Organisational (H/O) barrier** (medium effectiveness) is a barrier that contributes to the control of the process or activity. This type of barrier can reduce the likelihood of initiating event by reinforcing barriers or preventing their decay, but once the threat is initiated it cannot, in general, prevent its transmission nor reduce consequences. Typical sub-groups are as follows:
   - **Organisational (procedural) barrier**, for example inspection and monitoring, controlling instruments, procedural control, permit to work systems, job risk assessment, etc.).
   - **Human (operator) barrier**, for example operator control, supervision, walk rounds etc.

3. ***Fundamental barrier*** *(low effectiveness close to event) is a barrier the action of which* is separated in time from the threat initiation and hazard realization. However fundamental barriers are very important and effective in contributing to the system safety by checking for the weaknesses in the system and the underlying causes of failure. The following sub-groups can be identified:
   - **Fundamental procedural barrier**, for example design review, commissioning review, procedural review, operational review, competence assurance, etc.
   - **Fundamental human barrier**, for example, good health of workforce, etc.

This classification is presented in Figure 7.

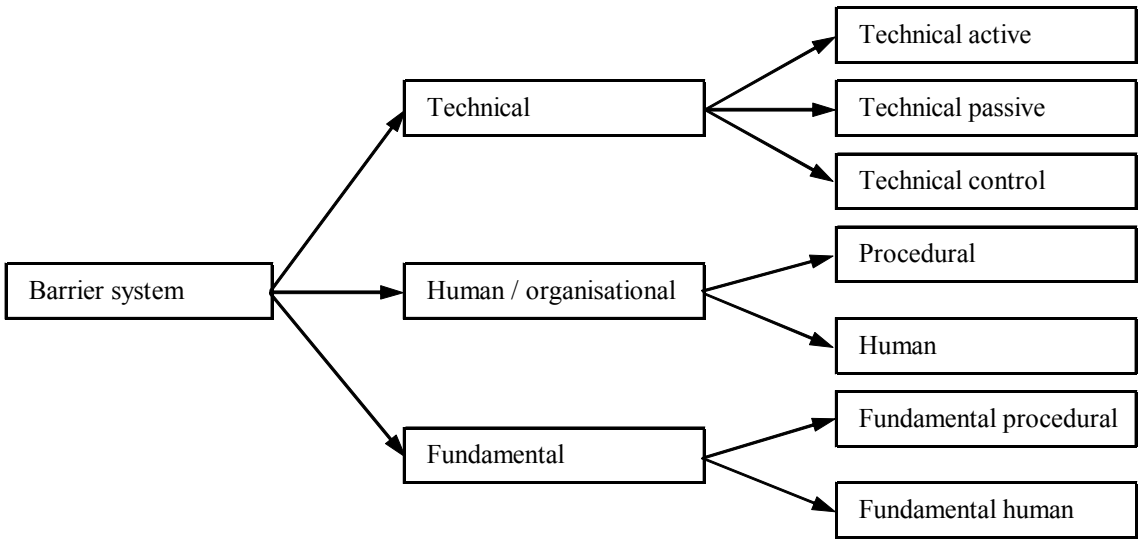


Figure 7 Proposed barrier classification scheme

2.4.2 Primary and secondary barriers

While the function of the primary barrier is to eliminate, prevent, reduce, mitigate or control threat transmission and escalation of the realised hazard, the function of the secondary barrier (control of barrier decay mode) is to prevent the barrier decay, erosion or failure: the primary means of preventing and controlling hazards are primary barriers, while secondary barriers are fortifying the primary barriers. The following rule set can now be established:

1. Primary barriers are:
   - Technical active barriers (e.g. shut-down valves, deluge system, etc.)
   - Technical passive barriers (e.g. fire wall, blast wall, containment, separation, etc.)
   - Technical control barriers (e.g. fire and gas detection, alarms, etc),
   - Organisational (procedural) barriers (e.g. inspection and monitoring, etc.),
   - Human (operator) barriers (e.g. process control operator, etc.).

2. Secondary barriers:
   - Human (operator) barriers (e.g. supervision, etc.)
   - Fundamental (procedural) barriers (e.g. design reviews, operational reviews, competence assurance, etc.).
   - Fundamental human barriers (e.g. good health, etc.)

2.4.3 Barrier decay and failure modes

The overriding priniciple for assigning the barriers decay/failure modes was that only the most relevant modes should be defined. The criteria for a "relevant decay mode" were based on the near miss and accident experience of several offshore operators. In this way repetition of the same secondary barriers was minimized. The rationale behind this is that each secondary barrier (mostly of fundamental type) besides targeting a particular decay mode, will also be able to prevent other related underlying causes of failure/decay. The advantage of this approach is to improve reliability and energise the socio-technical system with the minimum number of controls, thus keeping the size of the bow ties at reasonable level.

Another aim was to avoid vacuous argument or statements of the obvious, for example that for a given human barrier the decay/failure mode is human error, instead the most relevant underlying cause is given, such as excessive workload, erosion of vigilance, inadequate task specification, etc.

The matrix of primary and secondary barriers and the underlying modes of failure (barrier decay modes) is presented in Figure 8. The way in which this matrix can be used is illustrated on the following example.

Large Motor Fire on an Offshore Platform
The procedure for starting the large motors requiring separately driven cooling fans was for a person in the Control Room (separate from the motors) to start the motors and check that the indicator saying "motor cooling fan" was on, and for another person to be by the motors and check if the cooling fans were turning (these were driven by separate motors). In addition there was the (large) motor temperature alarm indicator in the Control Room.

This means that the procedure to avoid motor overheating (threat) was for person A in the Control Room to switch on the fans and check the indicator, and for person B in the Motor Room to confirm that fans are working. The first barrier in this system is human/organisational procedural (operator A switches on the fans and checks the indicator) which corresponds to

"operator control" primary barrier in Figure 8. The second primary barrier of the same type (operator B in Motor Room confirms that fans are working) is also "operator control". The third primary barrier is a motor temperature indicator which corresponds to "detection barrier" in Figure 8.

Considering the "operator control" barrier in Figure 8 and moving along the same row towards the right and the first red field with letters "DM" (decay mode) and then up the same column to the underlying causes of failure, in this case it is "inadequate task specification", the next "DM" in the barrier row corresponds to "insufficient training/competence", the next one is "inadequate communication", and the last underlying cause of failure is "excessive workload".

Large Motor Fire on an Offshore Platform (cont.)
On the day of the accident, workforce was very busy and the fans were being repaired. A person in the Control Room started the motors, but could not find another person to send to the Motor Room to confirm that fans were working. A person in Control Room checked that the indicator "motor cooling fan" was on and did not do anything else. The indictor for motor cooling fan was indicating that there is power to the fans and not that they are working. Motor temperature alarms were cancelled as they would indicate high temperature and unnecessary stoppage of the motors, so the practice was to ignore these. After a while the motor caught fire.

In this case the second barrier (operator B in Motor Room confirms that fans are working) and the third barrier (motor temperature alarms) were disabled, i.e. non existent. In fact the whole situation could be interpreted as a failure of the Permit to Work system, which is very seldom analysed. Besides the failure in global safety management of the facility, the operator A in the Control Room should have known that he was violating the procedure by having two barriers disabled and should not have switched the motors. It seems that he was not aware of the "barriers" and their functions indicating a lack of competence, and that his task was not properly specified i.e. he had insufficient knowledge about the motor, fan and their control systems or explanation about the role of the second person.

Choosing these two barrier decay modes (underlying causes of failure) and going down along their respective columns to the blue field with letters "SB" (secondary barrier) and then left towards the barriers, for the "inadequate task specification" one comes to the secondary barrier of the fundamental type "procedural review", and for the "insufficient training / competence" to the secondary barrier "operational (best practice) review". Those two secondary barriers that could have prevented this accident.

The condensed information presented in Figure 8 is shown in an expanded form in Table 5.

The barrier rule set in Figure 8 has been derived on the basis of several initiating events and it therefore is not complete. In order to make it live and dynamic it should be:

1. Adjusted to be facility and organisation specific,
2. Improved by proactive monitoring of latent conditions caused by decay/failure modes and their controls, and
3. Updated from lessons learned from incidents and near-misses.

	Barriers	Underlying Cause of Failure / Barrier Decay Modes																								
		Inadequate design	Incorrect material specification / usage	Incorrect equipment specification / usag	Incorrect installation	Inadequate commissioning	Design changes / damage / add-ons	Inadequate testing	Inadequate (poorly controlled)	Inadequate inspection	Inadequate plan / criteria	Inadequate procedures	Inadequate compliance monitoring	Inadequate supervision	Inadequate task specification	Insufficient training / competence	Inadequate communication	Demanning / Staff turnaround	Lack of safety culture	Excessive workload	Outdated information / data	Violation	Erosion of vigilance	Time, economic, external pressure
Technical	Containment	DM	DM			DM	DM		DM	DM														
	Shields / guards / separation	DM	DM			DM	DM		DM	DM														
	Additives	DM		DM	DM		DM	DM	DM															
	Energy release (safety valve)							DM	DM															
	Isolation	DM		DM	DM			DM	DM															
	Mitigation	DM		DM	DM			DM	DM															
	Detection / Portable gas detectors	DM		DM				DM	DM						DM									
	Stand-by vessel								DM								DM					DM	DM	
	Radar Early Warning System								DM								DM						DM	
Human / Organisational	Inspection & Anomaly reporting and management										DM	DM		DM	DM	DM								DM
	Maintenance										DM			DM	DM	DM								
	Condition monitoring (e.g. corrosion)										DM	DM		DM	DM	DM								DM
	Permit to work (PTW) system												DM		DM				DM					
	JRA / Plan / Manual / Work preparations / Systems of work											DM	DM			DM	DM							
	Control of all crane lifting												DM	DM				DM						
	Operator control														DM	DM	DM			DM				
	Walk rounds										DM	DM		DM	DM	DM							DM	DM
	Procedural control												DM	DM		DM			DM	DM				DM
	Supervision														SB	SB	SB		DM	DM		SB	SB	DM
Fundamental	Management of change						SB											SB	SB		SB			
	Procedural review							SB	SB	SB		SB			SB		SB				SB			
	Design review (HAZOP, etc.)		SB	SB																	SB			
	Construction / commissioning review	SB	SB		SB		SB																	
	Operational review (best practice)	SB		SB		SB	SB		SB	SB	SB					SB		SB			SB			SB
	Competence assurance											SB		SB										
	Corporate audit												SB											
	Third Party Verification					SB																		

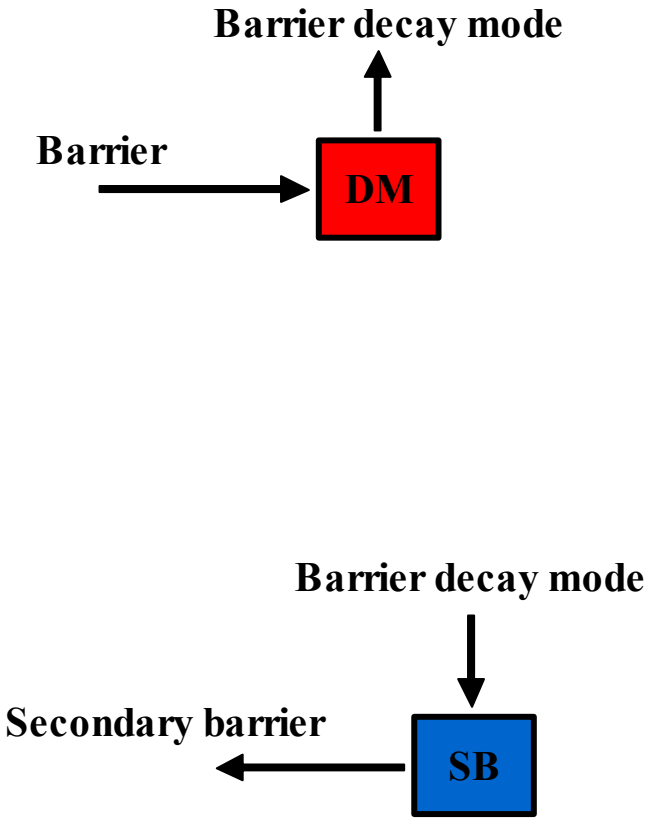


Figure 8 Barriers and barrier decay modes

Table 5 Barriers, decay/failure modes and their controls

No.	Barrier	No.	Underlying Cause of Failure (Barrier Decay/Failure Mode)	No.	Secondary Barrier (Control of Barrier Decay/Failure Mode)
1	Containment	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect material specification / usage	1	Design review (HAZOP, etc.)
				2	Construction / commissioning review
		3	Inadequate commissioning	1	Operational review (best practice)
				2	Third Party Verification
		4	Design changes / damage / add-ons	1	Management of change
				2	Construction / commissioning review
				3	Operational review (best practice)
		5	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
		6	Inadequate inspection	1	Procedural review
				2	Operational review (best practice)
2	Shields / guards / separation	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect material specification / usage	1	Design review (HAZOP, etc.)
				2	Construction / commissioning review
		3	Inadequate commissioning	1	Operational review (best practice)
				2	Third Party Verification
		4	Design changes / damage / add-ons	1	Management of change
				2	Construction / commissioning review
				3	Operational review (best practice)
		5	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
		6	Inadequate inspection	1	Procedural review
				2	Operational review (best practice)
3	Additives	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect equipment specification / usage	1	Design review (HAZOP, etc.)
				2	Operational review (best practice)
		3	Incorrect installation	1	Construction / commissioning review
		4	Design changes / damage / add-ons	1	Management of change
				2	Construction / commissioning review
				3	Operational review (best practice)
		5	Inadequate testing	1	Procedural review
		6	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
4	Energy release (safety valve)	1	Inadequate testing	1	Procedural review
		2	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)

Table 5 Barriers, decay/failure modes and their controls (cont.)

No.	Barrier	No.	Underlying Cause of Failure (Barrier Decay/Failure Mode)	No.	Secondary Barrier (Control of Barrier Decay/Failure Mode)
5	Isolation	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect equipment specification / usage	1	Design review (HAZOP, etc.)
				2	Operational review (best practice)
		3	Incorrect installation	1	Construction / commissioning review
		4	Inadequate testing	1	Procedural review
		5	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
6	Mitigation	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect equipment specification / usage	1	Design review (HAZOP, etc.)
				2	Operational review (best practice)
		3	Incorrect installation	1	Construction / commissioning review
		4	Inadequate testing	1	Procedural review
		5	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
7	Detection / Portable gas detectors	1	Inadequate design	1	Construction / commissioning review
				2	Operational review (best practice)
		2	Incorrect equipment specification / usage	1	Design review (HAZOP, etc.)
				2	Operational review (best practice)
		3	Inadequate testing	1	Procedural review
		4	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
		5	Inadequate task specification	1	Supervision
				2	Procedural review
8	Stand-by vessel	1	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
		2	Inadequate communication	1	Supervision
				2	Procedural review
		3	Violation	1	Supervision
		4	Erosion of vigilance	1	Supervision
9	Radar Early Warning System	1	Inadequate (poorly controlled) maintenance	1	Procedural review
				2	Operational review (best practice)
		2	Inadequate communication	1	Supervision
				2	Procedural review
		3	Erosion of vigilance	1	Supervision
10	Inspection & Anomaly reporting and management	1	Inadequate plan / criteria	1	Operational review (best practice)
		2	Inadequate procedures	1	Procedural review
				2	Competence assurance
		3	Inadequate supervision	1	Competence assurance
		4	Inadequate task specification	1	Supervision
				2	Procedural review
		5	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		6	Time, economic, external pressure	1	Operational review (best practice)

Table 5 Barriers, decay/failure modes and their controls (cont.)

No.	Barrier	No.	Underlying Cause of Failure (Barrier Decay/Failure Mode)	No.	Secondary Barrier (Control of Barrier Decay/Failure Mode)
11	Maintenance	1	Inadequate plan / criteria	1	Operational review (best practice)
		2	Inadequate supervision	1	Competence assurance
		3	Inadequate task specification	1	Supervision
				2	Procedural review
		4	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
12	Condition monitoring (e.g. corrosion)	1	Inadequate plan / criteria	1	Operational review (best practice)
		2	Inadequate procedures	1	Procedural review
				2	Competence assurance
		3	Inadequate supervision	1	Competence assurance
		4	Inadequate task specification	1	Supervision
				2	Procedural review
		5	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		6	Time, economic, external pressure	1	Operational review (best practice)
13	Permit to work (PTW) system	1	Inadequate compliance monitoring	1	Corporate audit
		2	Inadequate task specification	1	Supervision
				2	Procedural review
		3	Lack of safety culture	1	Management of change
14	JRA / Plan / Manual / Work preparations / Systems of work	1	Inadequate procedures	1	Procedural review
				2	Competence assurance
		2	Inadequate compliance monitoring	1	Corporate audit
		3	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		4	Inadequate communication	1	Supervision
				2	Procedural review
15	Control of all crane lifting	1	Inadequate compliance monitoring	1	Corporate audit
		2	Inadequate supervision	1	Competence assurance
		3	Demanning / Staff turnaround	1	Management of change
				2	Operational review (best practice)
16	Operator control	1	Inadequate task specification	1	Supervision
				2	Procedural review
		2	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		3	Inadequate communication	1	Supervision
				2	Procedural review
17	Walk rounds	1	Inadequate plan / criteria	1	Operational review (best practice)
		2	Inadequate procedures	1	Procedural review
				2	Competence assurance
		3	Inadequate supervision	1	Competence assurance
		4	Inadequate task specification	1	Supervision
				2	Procedural review
		5	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		6	Erosion of vigilance	1	Supervision
		7	Time, economic, external pressure	1	Operational review (best practice)
18	Procedural control	1	Inadequate compliance monitoring	1	Corporate audit
		2	Inadequate supervision	1	Competence assurance
		3	Insufficient training / competence	1	Supervision
				2	Operational review (best practice)
		4	Lack of safety culture	1	Management of change
		6	Time, economic, external pressure	1	Operational review (best practice)
19	Supervision	1	Lack of safety culture	1	Management of change
		3	Time, economic, external pressure	1	Operational review (best practice)
20	Management of change				
21	Procedural review				
22	Design review (HAZOP, etc.)				
23	Construction / commissioning review				
24	Operational review (best practice)				
25	Competence assurance				
26	Corporate audit				
27	Third Party Verification				

2.4.4 Application suggestions

The main aim of the barrier rule set is to facilitate the use of bow ties by the workforce for the graphical representation of the hazard protection and accident causation models. In addition, the subsequent guidelines may be useful when applying the rule set for the primary barriers, barrier decay/failure modes and their controls (secondary barriers):

1. Primary barriers must correspond to the reality, i.e. they must either physically exist on the facility (technical barriers) or must be in use (applied) in the form of procedures or operator controls (human / organizational).
2. For each primary barrier a set of relevant decay modes is specified, out of which only a few may be applicable. If a same type of barrier is in place for several threats, then different decay modes may be applied to each of the barriers in order to trigger different secondary barriers.
3. When choosing secondary barriers (decay/failure mode controls) for the particular underlying cause of decay/failure, there is usually no need to apply all controls, but the most specific to the failure. For example, if the "operational (best practice) review" is triggered once or twice for one barrier, it will apply to all procedures which are related to that barrier. This will keep the size of the bow ties at reasonable level which facilitates easier understanding.
4. When linking a barrier to safety critical tasks (required to maintain, control or operate the barrier) which should ensure that barrier is operational at all times and to the person who is responsible for the task, care should be taken for distribution of responsibilities so that persons who maintain, inspect, control, etc. barriers can take the ownership of their reliability and availability. In this way a common mode failure, e.g. having one person for several barrier related task, is avoided.

2.5 Barrier parameters

For the purpose of this study two most important barrier parameters are: effectiveness and complexity. These two parameters are described as follows:

1. **Effectiveness** – describes the level or prevention, attenuation, mitigation or control of the threat of the hazard being released. In Section 2.4.1 three levels of effectiveness were mentioned: high for technical and some human / organizational barriers, medium for some human / organizational barriers and low for fundamental barriers.

2. **Complexity** – denotes the level of complexity of maintaining, controlling or operating a technical barrier, or controlling or making operational the procedural barrier. For a technical barrier level of complexity takes into account the complexity of the tasks to maintain, control or operate the barrier and the required knowledge and experience. For a procedural barrier the level of complexity is associated with the complexity of procedural tasks, quality of procedural information, and the required knowledge and experience to carry out the tasks. It should be noted that the level of complexity is a "condensed" rule regarding the required level of competency of the team that has to perform certain set of tasks. Again a three point score is used to define the level of complexity of maintaining the barrier as high, medium and low. Clearly, for a high level of complexity, the high level of competence is required. In general there could be two solutions for one complexity level - one with high team competency and less supervision and the other with lower team competency and more supervision.

For the sake of completeness of the barrier rule set two more barrier parameters are identified but not used in this study. These are:

3. **Probity** – applies to fundamental barriers and denotes the quality, independence, etc of the barrier, i.e. review, corporate audit, etc.

4. **Decay level** – decay in safety performance influences the period between application of fundamental barriers, similarly to the mean test interval of the equipment. It applies to fundamental procedural barriers most of which are reviews and audits and for which the repetitiveness (frequency) of application depends on the measured level of barrier decay. Measuring level of decay of procedural barrier is not an easy task. It should be based on monitoring deviations from the specified procedures, the quality delivered by the procedures, comparison with the best practice in industry, etc and then deciding on how many deviations and of which severity should trigger barrier repetition.

The adopted rating scheme for the barriers is based on three levels (high, medium and low). The following simple rule set has been applied for the rating of effectiveness and complexity:

1. Technical passive barriers (containment, blast/fire wall, etc.) – are the preventive barriers and therefore are associated with high effectiveness. Maintenance of such barriers is considered to be associated with low level of complexity.
2. Technical active barriers (ESD valves, deluge system, etc,) – are attenuation/mitigation barriers and their effectiveness can be rated as high. The complexity level of their upkeeping is assessed as medium.
3. Technical control barriers (fire/gas detection, stand-by vessel, etc.) – intuitively should be as effective as the barriers which they activate, therefore the effectiveness is high, while their complexity ranges from medium to high.
4. Human/Organisational procedural barriers (inspection, maintenance, condition monitoring, etc.) – are effective in reducing the frequency of threat initiation but not effective once the threat is initiated. It therefore seems logical to assign medium level of effectiveness. The complexity related to some of the barriers like maintenance, inspection and anomaly reporting, condition monitoring is high, while for Permit to Work system, control of crane lifting it is medium.
5. Human/Organisational operator barriers range from high effectiveness for operator control, medium for supervision, to low effectiveness for walk rounds. The range of complexity levels is also wide from high for operator control, medium for supervision, to low for walk rounds.
6. Fundamental barriers – these have no effect once the threat is initiated but can significantly improve the procedural barriers (and safety management all the way up to technical barriers). Consequently the level of effectiveness is low. Level of complexity is high for barriers such as competence assurance, design, construction, and commissioning review, and medium for the other fundamental barriers.

It should be noted that the barrier rating should be done by eliciting the considered judgments of a team of people from different disciplines and the workforce. This would facilitate the evolution and convergence of judgments which may differ at the start of the process. Barrier rating is important because it helps to focus on most effective barriers, i.e. barriers that can prevent, attenuate and mitigate the consequence of an accident and it can improve the maintenance of barriers which depending on the task complexity and competence of the workforce, may require more or less supervision.

An example of barrier rating is presented in Table 6 where the red fields denote high level (H), yellow the medium level (M) and green the low level (L) rating.

Table 6 Rating of barriers

Type		Barrier	Effectiveness	Complexity
Technical	Passive	Containment	H	L
		Shields / guards / separation	H	L
		Additives	H	L
	Active	Energy release (safety valve)	H	H
		Isolation	H	H
		Mitigation	H	H
	Control	Detection / Portable gas detectors	H	H
		Stand-by vessel	M	M
		Radar Early Warning System	M	M
Human / Organisational	Procedural	Inspection & Anomaly reporting and management	M	H
		Maintenance	M	H
		Condition monitoring (e.g. corrosion)	M	H
		Permit to work (PTW) system	M	M
		JRA / Plan / Manual / Work preparations / Systems of work	M	M
		Control of all crane liting	M	M
	Human	Operator control	H	H
		Walk rounds	L	L
		Supervision	M	M
Fundamental	Procedural	Managemnt of change	L	M
		Procedural control	L	M
		Procedural review	L	M
		Design review (HAZOP, etc.)	L	H
		Construction / commissioning review	L	H
		Operational review (best practice)	L	H
		Competence assurance	L	H
		Corporate audit	L	M
		Third Party Verification	L	M

2.6 Actual workforce involvement

2.6.1 Major hazard awareness workshops

Barrier (bow tie) approach is a useful tool in communicating major hazards information to the workforce. In general, the hazard identification is the natural starting point and the workshop with the workforce is the best source of information. In the offshore oil and gas industry in the UK there is general awareness of hazards through the safety cases and safety briefings, so that this first step can be omitted. One of the best way for raising the workforce involvement with major hazards is to start with the very basic hazard protection model containing just a few primary (technical) barriers. Simple bow tie models are very suitable for presenting the definitions, the approach and basic mapping of hazards into initiating events.

This is can be followed by elicitation of information about the other threats and primary barriers by asking questions such as "are there any other threats that could lead to this initiating event", "are there more barriers in place of these threats?" or "what more do you do which is directly safety related?". Such a workshop yields the complete information on the threats, primary barriers and consequences.

The next step is to investigate barrier decay/failure modes and their controls (secondary barriers). In general, recalling the previous near misses and incidents helps kick start the brainstorming process. However, if such information is not available for the particular facility/industry, this process may take a long time and easily diverge. This was one of the main reasons for the development of the barrier rule set. It should be noted that the rule set has been tested in modelling of a few initiating events for several operators and may require some extension for other initiating events.

Some companies were not confident that their workforce would understand the bow ties, and some others approached the communication of major hazards differently, thinking the bow tie presentation would confuse the workforce. However, the managers that were exposed to the bow tie approach believed that it would be easily understood and accepted by the workforce.

The workshop experience indicated that the bow ties were easy to understand. Due to insufficient time there was little discussion on the barrier rule set (which barrier decay/failure modes are more relevant), but general agreement that it had the potential to greatly facilitate the process of completing the barrier model. In fact few people found that some of the barrier decay modes explained the cause of some near misses.

The questionnaire was developed to allow the measurement of the understanding of the workshop and collect the comments and ideas from the workforce and the management. The results of the workforce response to the barrier approach are presented in *Appendix A*. The responses from offshore safety representatives were given separately from the platform management. Interestingly, the workforce was more positive and more understanding of the barrier approach than the management. They also had some ideas about using bow ties in job risk analysis, etc. The management was sceptical that the workforce would understand the barrier approach.

The previous experience (Trbojevic, 2001 and 2007) of working with the workforce indicated that the development of the bow ties in parallel with the personnel safety critical tasks was the most natural and beneficial. The main reason for this was that where there was no proper safety management system in place it was easier to develop the "process" model (day-to-day activities and tasks) and the bow tie (safety) model in parallel. In fact development of the bow tie model was sometimes driving (eliciting) personnel tasks not mentioned before and vice versa. Some

new tasks (not mention at the start) were pointing to new threats that had to be incorporated into the bow tie model.

The offshore experience was that the development of the activity model was either impractical or too time consuming, and therefore an attempt was made to link the hazard protection (bow tie) model to safety management system procedures. It is for those reasons that the barriers and the procedures are a less sharply defined.

2.6.2 Improving safety management

In parallel with rating of barriers the workforce should also be involved in discussion, contributing, assessing, improving all barriers but in particular human / organisational procedural, operator and fundamental barriers. This is shown in Table 7 where the barriers are listed in the column on the left and the actual workforce involvement processes (for an operator) are given in the top row. The "x" in Table 7 present an assumed test for the focus of the safety processes. The table can also be interpreted as a template for audit of workforce involvement. Such a template should also be linked to the workforce training matrix.

Table 7 Workforce involvement with barriers

Type		Barrier \ Actual Workforce Involvement	Safety through knowledge	Safe/Unsafe act auditing (SUSA) Culture chage workshop	SUSA Observation Workshops	Safety improvement feedback process	Information gathering on new legislation, developments in the fields of safety, etc.	Offshore Safety and Environmental Meetings (one per shift rotation)	Daily Operations Team briefings	Shift handovers	Safety Representatives Committee Meetings	Wash-up meetings following exercises and drills to test Emergency Plans	Toolbox Talks	HAZOP reviews	SIL reviews	Major Hazard Risk Reviews	Planning and liaison meetings with major contractors	Management of Environment, Safety & Health (MESH)	Inciddent investigation reviews	Construction workpack revirews	Construction workpack revirews
Technical	**Passive**	Containment	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Shields / guards / separation	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Additives	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
	Active	Energy release (safety valve)	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Isolation	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Mitigation	x			**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
	Control	Detection / Portable gas detectors	x	**x**	**x**	**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Stand-by vessel	x	**x**	**x**	**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
		Radar Early Warning System	x	**x**	**x**	**x**		x	x	x	x	x	x	x	x	x		x	x	x	x
Human / Organisational	**Procedural**	Inspection & Anomaly reporting and management	x	**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Maintenance		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Condition monitoring (e.g. corrosion)		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Permit to work (PTW) system		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		JRA / Plan / Manual / Work preparations / Systems of work		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Control of all crane liting		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
	Human	Operator control		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Walk rounds		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Supervision		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
Fundamental	**Procedural**	Managemnt of change		**x**	**x**	**x**		x	x	x	x	x	x	x		x		x	x	x	x
		Procedural control		**x**	**x**	**x**								x		x		x	x	x	x
		Procedural review		**x**	**x**	**x**								x		x		x	x	x	x
		Design review (HAZOP, etc.)					x							x		x	x	x	x	x	x
		Construction / commissioning review					x									x	x	x	x	x	x
		Operational review (best practice)		**x**	**x**	**x**	x									x		x	x	x	x
		Competence assurance		**x**	**x**	**x**	x									x	x	x	x	x	x
		Corporate audit				**x**	x									x		x	x	x	x
		Third Party Verification					x										x				

2.7 Advantages of barrier approach

2.7.1 Visualisation of hazard protection

The main uses of the bow tie (barriers) approach are as follows:

1. For brainstorming with the workforce to obtain the list of threats and the barriers to guard from these threats, for example, by asking the question "given this hazard (e.g. sour gas release), how could this be brought about?".
2. For the visualisation of the links between the hazard model and the safety management system and the workforce, once the hazard model (threats, barriers, top event, barriers and consequences) is assembled.

One event from such a model is shown in Figure 9 depicting the left hand side (causation part) of the sour gas release from a riser.

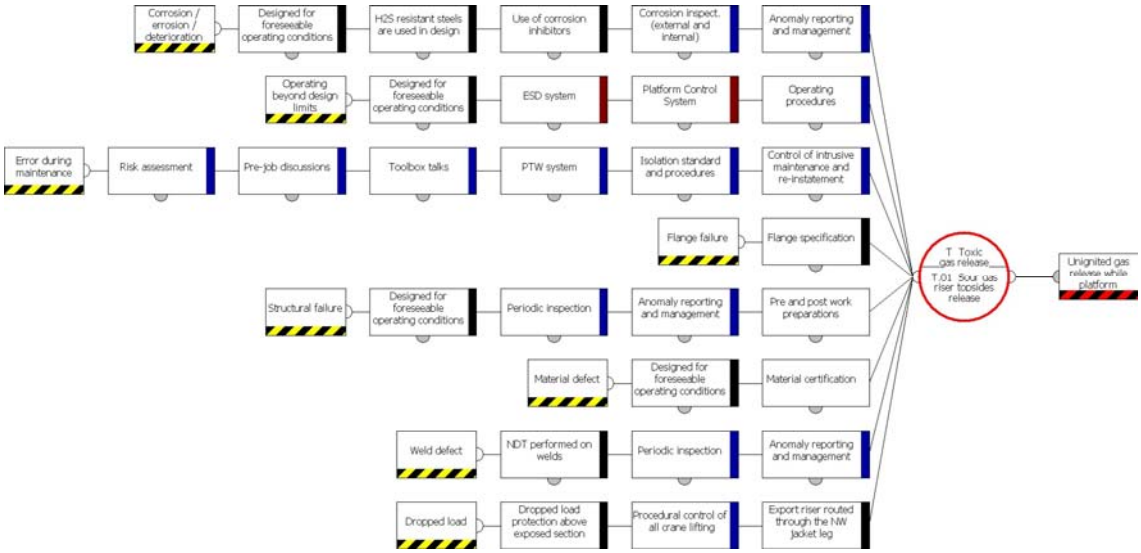


Figure 9 Bow tie for gas release

A barrier risk model explicitly displays the information about the threats and available protection from these. In fact it visually displays the information on major hazards and their triggers (threats) and the facility specific information on protection systems and practices.

Disabling the barrier(s) for maintenance or any other reason leads to reduced protection from threats or a shorter route from a threat to an initiating event. If barriers are disabled then the decision needs to be made about continuing the operation and/or supplying some additional protection. This decision making can be risk/barrier based, for example, the risk is qualitatively evaluated based on the likelihood of consequences (neglecting barrier effects at this stage), and assessed against the criteria specifying the minimum number of barriers for each risk level, Section 2.2.6. Expanding on the previous description, a combination of technical and procedural barriers could be prescribed, as follows: for the low risk level the criteria could prescribe as a minimum, one technical and one procedural barrier for each threat and one barrier for each consequence (and a control for each identified barrier decay/failure mode); for the medium risk level, the acceptance could be based on an increased number of barriers, for example, two technical and a procedural barrier or one technical and three procedural barriers, and so on.

Another way of doing this would be to mark barriers which are essential for safe operations, the removal of which would require additional protection, and barriers the removal of which requires raised alertness. In this way, taking a barrier out of the operation would signal if the risk is acceptable or not or if extra protection needs to be implemented. Incident investigation should follow the barrier scheme which may have to be reviewed after a near miss or incident

The essence of the barrier model is that it is simple and therefore easily understood. A "simple" model means that for each initiating (top) event there is a number of threats, consequences and a reasonable number of barriers, for example, the bow tie in Figure 9.

2.7.2 Visualisation of accident causation

It is important that a causation part of the barrier model is not too complicated like, for example, some fault trees in the nuclear industry. Once the barriers are presented and understood, the expansion of the bow ties showing barrier decay/failure modes can commence. The proposed rule set linking barriers to decay/failure modes and their controls is expected to:

1. Facilitate further application of the barrier approach,
2. Allow the workforce to understand the importance of underlying causes of barrier decay/failure and their role in this process,
3. Improve safety trainings, job risk assessment (JRA), etc.
4. Contribute to foresight and avoidance of accidents.

More complex systems can be presented by the second layer of bow ties. For example, a threat can be treated as an initiating event in itself, which means that a threat can be represented by an additional bow tie which would have only the left hand (causation) side. Such a bow tie would serve as an input to the main bow tie.

Partial expansion of the bow tie for gas release (Figure 9) showing some of the barrier decay/failure modes is presented in Figure 10. More examples of bow ties for offshore marine operations, riser release and dropped loads are presented in *Appendix B*.

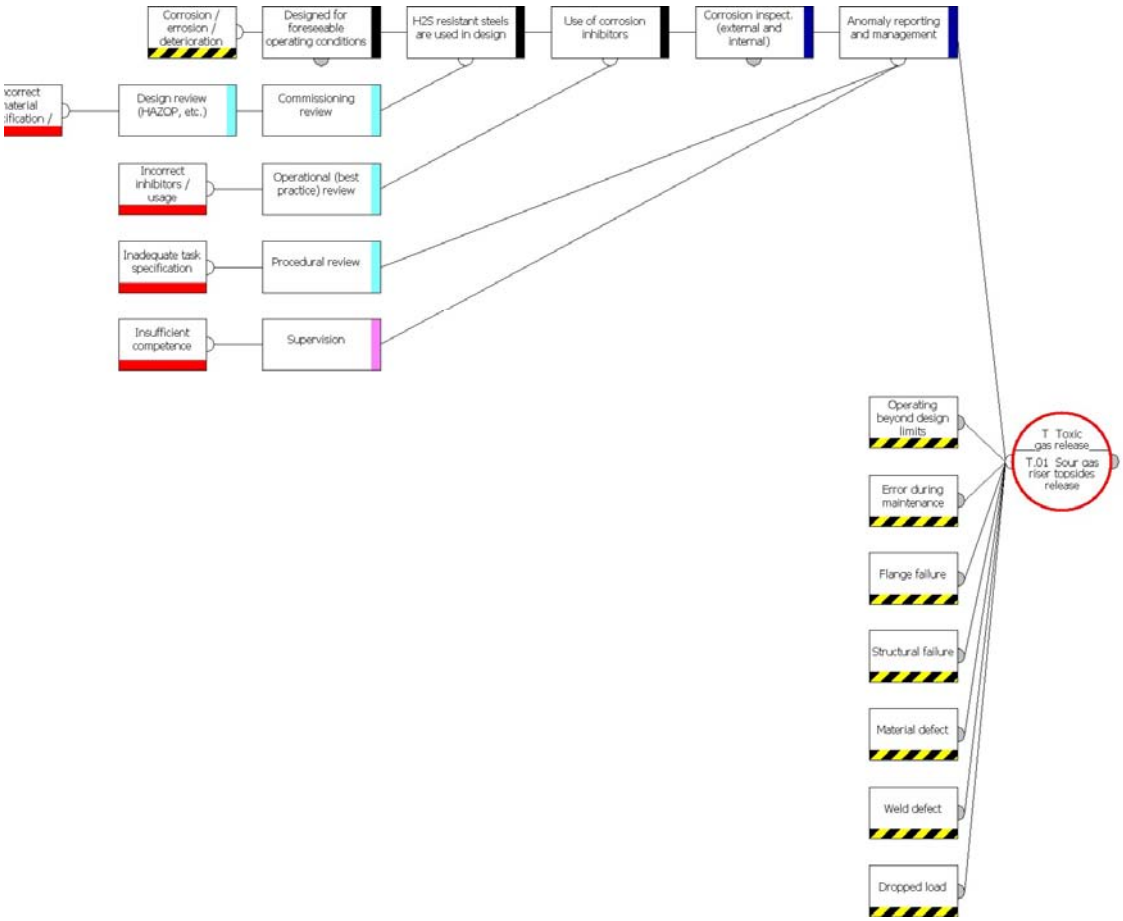


Figure 10 Barrier decay / failure modes

A clear example of simple barriers being breached is the Herald of Free Enterprise accident:

Herald of Free Enterprise, 1987

On 6 March 1987 the cross-channel roll-on-roll-off ferry Herald of Free Enterprise sank soon after leaving the port of Zeebrugge, with the loss of 186 passengers and crew. The vessel sank because the large inner and outer bow doors, through which vehicles enter and leave, had been left open and water soon rose the few metres necessary for it to enter the ship. The water moved to one side and caused the ship to roll onto its side and settle on the sandbank. The accident investigation found that:

1. *The crew member responsible for shutting the doors, after finishing cleaning the car deck, had a short break.*
2. *It was also found that he was not on the car deck before the ship set sail and that he was asleep during his break*
3. *The other crew members expected him to close the doors because he was scheduled to close them.*
4. *Before the ship dropped moorings the First Officer should have stayed on the car deck to make sure the doors were closed, but trying to stay on the schedule he left the car deck and went to the bridge before the doors were closed.*
5. *From his position on the bridge the captain was not able to see the bow doors clearly, leading him to assume that they were closed. However, even leaving the doors open*

alone should not have caused the ship to capsize, which in this case was due to the reduced clearance between the doors and the water line.

6. *The loading ramp at Zeebrugge was too low to reach the upper deck at high tide. To clear the gap, the captain filled the ballast tanks to lower the ship, but forgot to deballast it afterwards. The clearance between the bow doors and the waterline was 2.5 m.*
7. *As the ship was under way in shallow waters, the clearance was reduced to 1.5 m due to squatting.*
8. *When the ship reached 18 knots the bow wave was high enough to engulf the bow doors.*
9. *The final factor was that the ship was designed to allow vehicles to drive in and out easily, without watertight compartments which could have prevented sinking. This was due to the repeal of the Act of 1865 requiring all iron vessels over 100 tons to have divided hulls (Kletz, 2006).*

Looking from the perspective of barriers it follows:

1. Technical barrier: Hull - had two latent conditions: a) design changes without bulkhead for easy car access and egress leading to unforeseen result, and b) ship was designed with clam doors instead of visor doors visible from the bridge.
2. Technical barrier (missing) - Failure to provide warning lights or CCTV to be able to check the doors from the bridge.
3. Human and Organisational barrier (removed): The responsible crew member closes the doors - The crew member responsible for closing the doors failed to do so.
4. Human and organisational barrier (removed): The First Officer checks that bow doors are closed – Failure to check that the doors were closed; this was due to external (schedule, economic) pressure.
5. Human and organisational barrier: Preparation for sailing - Failure to prepare the ship for sailing and recognise the ship's vulnerability in manoeuvring when not properly ballasted for the voyage.

In addition it was obvious that the distribution of responsibilities was not clear and that the underlying causes of barrier decay or failure were not identified and a fundamental barrier was not provided to reinforce the primary barriers, which all indicates inadequate safety management.

2.7.3 Safety case

The main purpose of the safety case is to demonstrate that, in relation to major accident events, all reasonably practicable controls have been identified and implemented in order to ensure that risk is As Low As Reasonably Practicable (ALARP). The bow tie approach fits well with the safety case and its big advantage is that it facilitates the process of reducing all the hazards so far as is reasonably practicable including hazards resulting from human/organizational failures. The bow tie, in effect, gives a structure for analyzing and demonstrating compliance with standards of good practice in countering **all threats**. The structure imposes discipline in assessment replacing intuition and experience, and permits a constructive dialogue to take place. The safety demonstration may comprise the following two steps:

1. Barrier model for the major accident hazards, describes all foreseeable threats that can be initiated to lead to hazard realization, i.e. initiating (top) events, and how these could escalate to various consequences. In addition there is a combination of primary technical barriers, and human / organisational and fundamental (secondary) barriers which reinforce the primary barriers. The requirement that all reasonable controls are in place becomes visible. This approach facilitates an improved focus of the Safety Management System (SMS) on the maintenance and upkeeping of the barriers.

2. Furthermore the barrier model can be linked to the day-to-day activity model of the personnel on a facility, Figure 11 which will ensure that the responsibilities for the barriers are distributed, that barriers are linked to processes that ensure their proper operation and maintenance, and that performance criteria and standards are prescribed for all barriers. The model could be extended to account for management hazards in which case it becomes the foundation of the SMS. Such a model requires only a depository of the existing procedures to provide a road map for the major hazards and installation specific information, the information of the required trade/skills, maintenance, supervision, specific reviews, etc in a simple visual form. In Figure 11 post indicators of the responsible persons and the procedures corresponding to the barriers are given at the bottom of the barrier boxes.

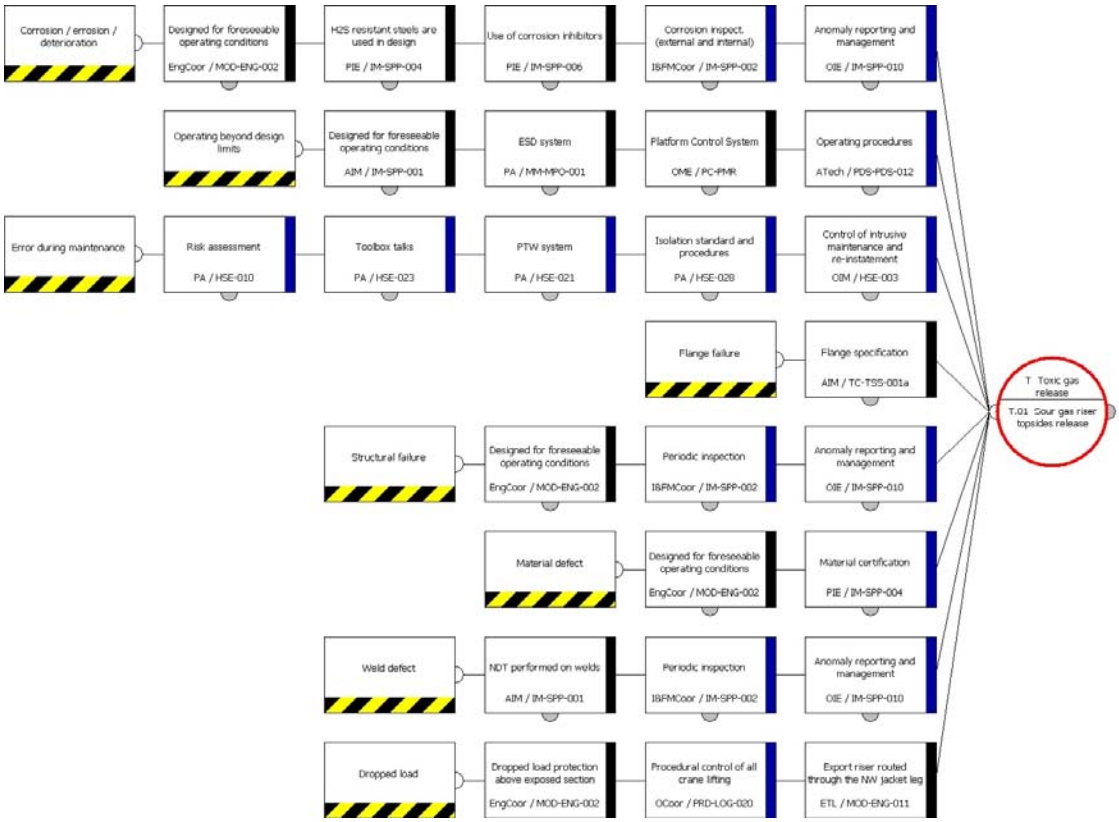


Figure 11 Bow tie SMS model

2.7.4 Contributing to improving resilience

Among many aspects that make a safety management system resilient, the important one is the predictability of threats. Predictability in this context does not mean that it can be predicted when the event will occur, but that its occurrence is foreseeable. The designers of offshore oil and gas installations anticipate not only the severity of hazard realization, but also its credible return period, for example, the air gap beneath a jacket platform in Gulf of Mexico is designed for a 100-year wave.

Ron Westrum identifies two types of foresight required for resilience (Resilience Engineering, 2006):

1. The first comes from learning from the past and present experience. This includes evaluation, learning and dissemination of industry generic and facility specific incident data, and keeping alive existing knowledge. This type of foresight is demonstrated in the primary barriers that target direct threats.
2. The second type of foresight is associated with processing of "faint signals". These can include symptomatic events, suspected trends, gut feelings, and intelligent speculation (Resilience Engineering, 2006). In the proposed approach a certain number of the so called "faint signals" may be detected from the barrier decay /failure modes and their controls.

Latent conditions caused by the barrier decay/failure modes can, in general, be detected by their controls. It is the absence or inadequate control of these modes that is more difficult to detect. Such information can be distilled from incident and near-miss reports and the controls reinstated or reinforced. Frequent repeat of particular latent conditions usually indicates problems on the higher level of procedures or processes which then may require a re-design. Optimisation of the design of safety management processes is dealt with in Section 3.

It is worth emphasising again that important information required for predictability of threats may be found in the primary barriers, decay/failure modes and secondary barriers. Moreover this information can be understood and generated by the workforce to improve the resilience of the system. Assuming that all reasonable primary barriers are in place, the resilience of the system can be improved by the effective secondary barriers.

3 CONTROL OF RISK MANAGEMENT PROCESS

3.1 Approach to tolerability of risk management process

3.1.1 Management of health and safety and control of major accident hazards

The basis of health and safety regulation in the UK is the Health and Safety at Work etc Act (1974). The Act requires those who conduct undertakings (generally employers) to ensure, so far as is reasonably practicable, (SFAIRP), the health, safety and welfare of their employees, of self-employed persons under their control, and of third persons (generally, the public). In addition, these general duties are supplemented by regulations applying to different risk areas (e.g. electricity, major hazards, hazardous substances etc), which set more specific goals and standards. The regulations are supported in turn by codes of practice, or other guidance drawn up by or with the help of industry, which set out good practice. Regulations may of course, where necessary, include specific instructions; but in general the aim is one of "goal-setting", allowing duty-holders flexibility as to the means of complying. The hierarchy of instruments is therefore as follows:

1. HSWA,1974,
2. Regulations,
3. Approved codes of practice (ACOPs) setting out good practice. These may either be attached to regulations or may stand independently,
4. Guidance and advice
5. Research which has non statutory standing but it moves the knowledge base forward by showing what is practical.

The HSWA system implies a dialogue between duty holders and an informed regulator, both in creating national standards and in improving particular situations. The burden of proof on the duty holder is defined by a "demonstration on balance of probabilities", rather than by "proof beyond reasonable doubt" (the condition used in the criminal law). The term "reasonable practicability" implies that cost can be taken into account in relation to risk reduction. However, SFAIRP cannot be pleaded as a defence in a failure to observe good practice, since accepted good practice is, almost by definition, always "reasonably practicable". The SFAIRP defence can only arise where good practice is unclear, or does not fully cover a given situation, or where an inspector is seeking to persuade a duty-holder to move forward from "good" to "best" practice as technology changes. The term "as low as reasonably practicable" (ALARP) is identical in meaning to SFAIRP, but is applied particularly where risk can be analysed and, in principle, may be quantified.

3.1.2 Focus on risk management process

The safety case regime in the UK requires the demonstration, starting from the current good industrial practice, that all necessary measures are in place to reduce and control the risk so far as is reasonably practicable (SFAIRP). This process embodies a continuous goal-setting process, where the goal is safety improvement. The term continuous is used here to imply an on-going process of safety improvement which could be triggered not only by the advances in technology, management control, experience and the best industrial practice, but also the process of monitoring and rectifying the weaknesses in the system.

Once the safety case is submitted and accepted reliance is mainly on the Safety Management System (SMS) to ensure that the facility is managed safely and that continuous improvement in safety is ongoing. This means that all technical, human / organisational and fundamental barriers necessary to reduce and control the risks should be implemented, maintained and kept in fully operational state. The acceptance of the safety case implies that risks are at an ALARP level assuming that the main technical barriers are in place for all threats and their effectiveness will be assured by the SMS. Insufficiency of the safety case therefore requires a focus on human and organizational factors. Typical weaknesses in the SMS can be directly linked to human/organizational barrier decay/failure modes and their controls (fundamental barriers) and these weaknesses should be the target for continuous improvement. As mentioned before, in practice the goal of continuous improvement degrades into compliance audits over time. So when deviations are recorded they are treated as non-compliances instead of focusing on their underlying causes and/or on the improvement of activities and procedures in order to avoid those.

It should also be noted that the latent conditions caused by the decay and erosion of barriers will always be present in the system. Even if these are picked up, treated and system patched up accordingly, their number will oscillate after implementing changes and improvement from a trough to a crest after certain barrier decay time. It is therefore logical to assume that if the processes within the SMS were to be optimized, then the number of latent conditions would be reduced. Such an optimized SMS would be more resilient to the decay and erosion of technical, and human / organisational barriers. In other words the improvement in overall safety level cannot be reached by monitoring and targeting annual safety indicators, but also requires improving the processes of the system from which these indicators originate.

One could also take a legal perspective by asking “should the optimisation approach, i.e. the principle of ensuring that all necessary measures are in place to reduce and control the risks and ensure the health, safety and welfare of the workforce, be also applied to the development of the SMS and its processes?”.

Drawing an analogy, an offshore facility for which ALARP process is applied at the design stage (where the focus is mainly on technical barriers), will have better safety performance, than if it were applied only at the operational stage (when design changes are seldom practical). Therefore, the processes and procedures (which control risks) designed with all necessary measures to reduce the risks from the start, will perform better and be more resilient to decay and failure, than the processes and procedures which just have to ensure compliance with predetermined templates.

It is not reasonable to expect that the safety will stay at the level demonstrated in the safety case or improve, just by having the SMS and patching it up with compliance audits, regardless of the quality of the processes developed within the SMS. It is therefore proposed to apply a risk based approach to further challenge and optimise a process in SMS. Inspiration for this idea came from an attempt to broaden the concept of tolerability doctrine (HSE, 1992a) to embrace

the tolerability of the process leading to risk reducing measures whose tolerability is based on adherence to process standards (McQuaid, 2007).

The following example demonstrates the importance of having proper design and functioning of the safety processes.

Formosa Plastics in Illinois, USA
Massive explosion resulting in death of five workers and the loss of the plant occurred when an operator overrode a critical valve safety interlock on a pressurised vessel making polyvinyl chloride.

On the day of the accident, an operator on the upper level of the reactor building was washing out a reactor with a water blaster. He should have gone to the lower level to open two valves on the reactor he was cleaning – a reactor bottom valve and the lower drain valve. The worker made an error after descending the stairwell to the lower level and turned to a different cluster of reactors and went to a vessel he evidently thought was the one he had started cleaning. It was a wrong reactor. He opened the drain valve, but the reactor bottom valve would not open. To prevent an accidental release, that valve was fitted with a safety interlock which prevented it from opening when the reactor was pressurised. However, instead of seeking further information on why the bottom valve would not open, he attached an air hose that provided the pressure needed for the override – a procedure intended to be used only in an emergency. When the valve opened, the highly flammable vinyl chloride immediately sprayed onto the floor and vapour filled the area. Vinyl chloride detection alarms sounded in the area. The supervisor and operators attempted to slow the release by relieving the reactor pressure. Just as the supervisor made an attempt to get to the bottom level via an external stairwell, the vinyl chloride vapour exploded.

The investigation found that the operators had time to evacuate the production building after the alarms had sounded; however they were not adequately trained for immediate evacuation. In addition, the systems and procedures put in place by the company were insufficient to minimise the potential for human error.

From the point of view of barriers this was the situation:

1. Clustering of the reactors in packs of four should have been treated as a latent (design) error, and the reactors should have been either painted differently or some other means of identification should have been in place (design process failure).
2. By-passing the safety interlock at the bottom valve is the overriding of the barrier (violation).
3. Operator's competence was insufficient (barrier decay)
4. Permit to work system or job safety analysis sheet barrier was absent (all necessary measures were not in place).
5. Workforce involvement in major hazard management and learning from the previous experience was non-existent (insufficient training and competence assurance; failure to analyse near misses and disseminate the information).
6. Corporate audits did not yield results (process decay).
7. Safety culture in the company was subjugated to the production pressure (process decay).

Formosa Plastics in Illinois, USA (Cont.)
The company was aware of the possibility of massive release of vinyl chloride but decided that the existing safety interlock was sufficient to prevent a serious accident. In 2003 an operator in the company's plant at another location opened the bottom valve on a wrong reactor releasing 8,000 pounds of vinyl chloride into the atmosphere. In 2004, an operator on the plant where

this accident occurred, bypassed a bottom valve safety interlock releasing a significant amount of vinyl chloride. After that incident, the company determined that additional controls were needed on the interlock. However, the company did not act quickly enough and the fatal explosion occurred just two months later.

The company did not recognise that all necessary measures were not in place for it to operate safely.

Optimization of the safety management processes requires that the main components of the SMS to be designed to dynamically improve safety so far as is reasonably practicable. The term "dynamically" implies that this process is ongoing. The main components of the SMS in this context are all types of barriers, and all processes, procedures, activities and tasks that ensure workforce competence, supervision, training, reviews, audits, etc. required for operation and maintenance of these barriers. In other words, when designing an SMS the focus should be on properly optimized safety that will also ensure optimized production performance. It is the principle of reducing the risk (and loss of production) so far as is reasonably practicable which ensures the convergence/optimisation of both the safety and production systems.

This process of optimizing the balance between competence and supervision by embodying all necessary measures to improve safety will be formulated here. The focal point for this is the barrier model. Barrier effectiveness in conjunction with threat potential offers an indication of the level of safety while the complexity of tasks for maintaining, controlling and operating a barrier should be matched by the appropriate personnel competence. Therefore all information is available at the starting point and the idea is to combine this information in a way to ensure that risks are minimised.

In the language of safety practitioners, this means to employ the Tolerability Doctrine (HSE, 1992a), or to apply all necessary measures to the process of balancing competence and supervision taking into account possible deterioration of barriers due to direct and underlying causes, with the aim to developing the process which will facilitate achieving the optimal balance between competence and supervision.

3.2 Optimising balance between competence and supervision

3.2.1 Introduction

A brief overview of the current practice related to competence assurance is given in *Appendix C*. The proposed approach has the potential to tackle most of the recommendations identified in the report "Competence assessment for the hazardous industries" (HSE, 2003b) which are listed below together with the comments related to the suitability of the proposed approach (in italics):

1. The full scope of safety critical tasks, such as process upsets and shutdowns should be covered by competence assessment. Bow ties present the link between major hazards, threats, barriers, safety critical tasks, possible accidents and unwanted consequences.
2. A wider application of risk assessment for the purpose of identifying and prioritising safety critical tasks for which competence need to be assessed. ***Safety critical tasks related to direct control of the process or to the upkeeping, control and operation of the barriers and the responsibilities for those tasks are visible in bow ties***.
3. Ensuring that NVQ syllabus clearly denotes the major hazard consequences of tasks and the safety role of equipment and is tailored to the needs of the site. ***Proposed balancing between threat potential, barrier effectiveness, task complexity, available and required competence and supervision directly complies with this recommendation***.

4. Wider considerations of the potential for skills to decay or become outdated, and therefore the need to consider effective reassessment system for people carrying out safety related tasks, such as adopting "check and train" process for staff, perhaps linking this to existing schemes such as annual reviews. ***This is accounted for by the fundamental barriers (probity and decay, Section 2.5) but is outside the scope of this study***.

3.2.2 Approach

Balancing competence and supervision can be viewed as providing the sufficient interaction between the different sources of knowledge required for task completion in a high hazard environment Miles, 2006). The knowledge requirements can be broadly categorized into three groups: a) major hazards knowledge, b) competence (trade/skill knowledge) and c) supervision (experience and local/facility knowledge), as shown in Figure 12.

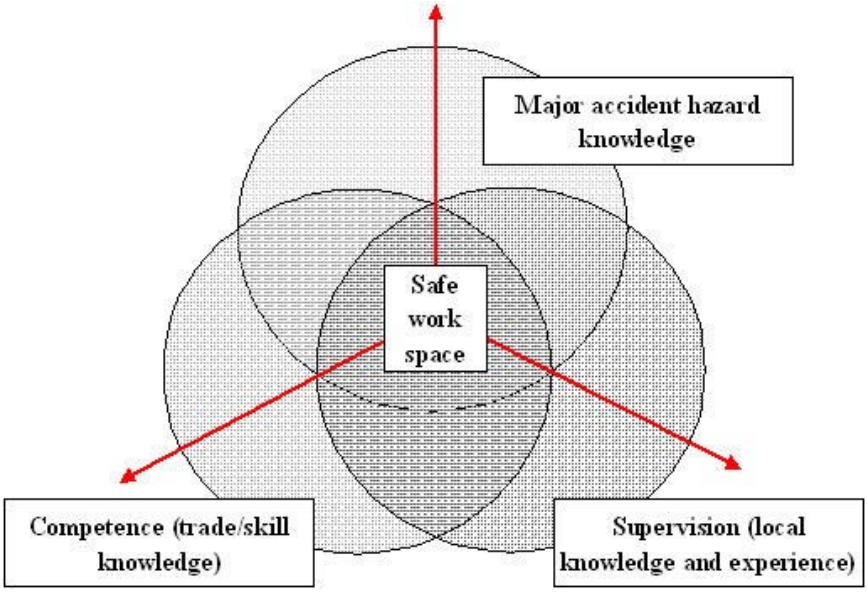


Figure 12 Knowledge requirement for a safe work space

For the sake of simplicity each circle in Figure 12 is assumed to move along its axis (shown in red) with the centrifugal (away from the centre) movement denoting decreasing knowledge transfer and decreasing safety at work space. An ideal situation of three circles coinciding would clearly be not reasonably practicable. The aim in practice is to achieve the sufficient interaction between the knowledge sources for the work space to be as safe as is reasonably practicable. If the competence were to decrease, for example due to new shift, then its circle would move outwards decreasing safety at the work place. To compensate this situation supervision would need to be increased, i.e. its circle would move inwards, and so on.

The approach adopted for optimising the balance between competence and supervision is within the framework of risk analysis. Risk based approach is considered a useful tool to identify combinations of several factors such as barrier effectiveness, task complexity, available competence, supervision, etc in the search for an optimal solution. Such optimal solution will at the same time deliver the sufficient knowledge for the safe workspace.

The main steps of the approach are shown in Figure 13. In a standard risk analysis after identifying the hazards and mapping those into representative initiating events, the frequency

estimation and the consequence analysis outputs are combined into a risk measure or a profile, which is then assessed against risk acceptance criteria. In this approach frequency estimation is replaced by estimation of the potential for barrier decay (rating of matching complexity and competence), and consequence analysis is replaced by estimation of criticality assessment (safety rating). The approach is described in the subsequent paragraphs.

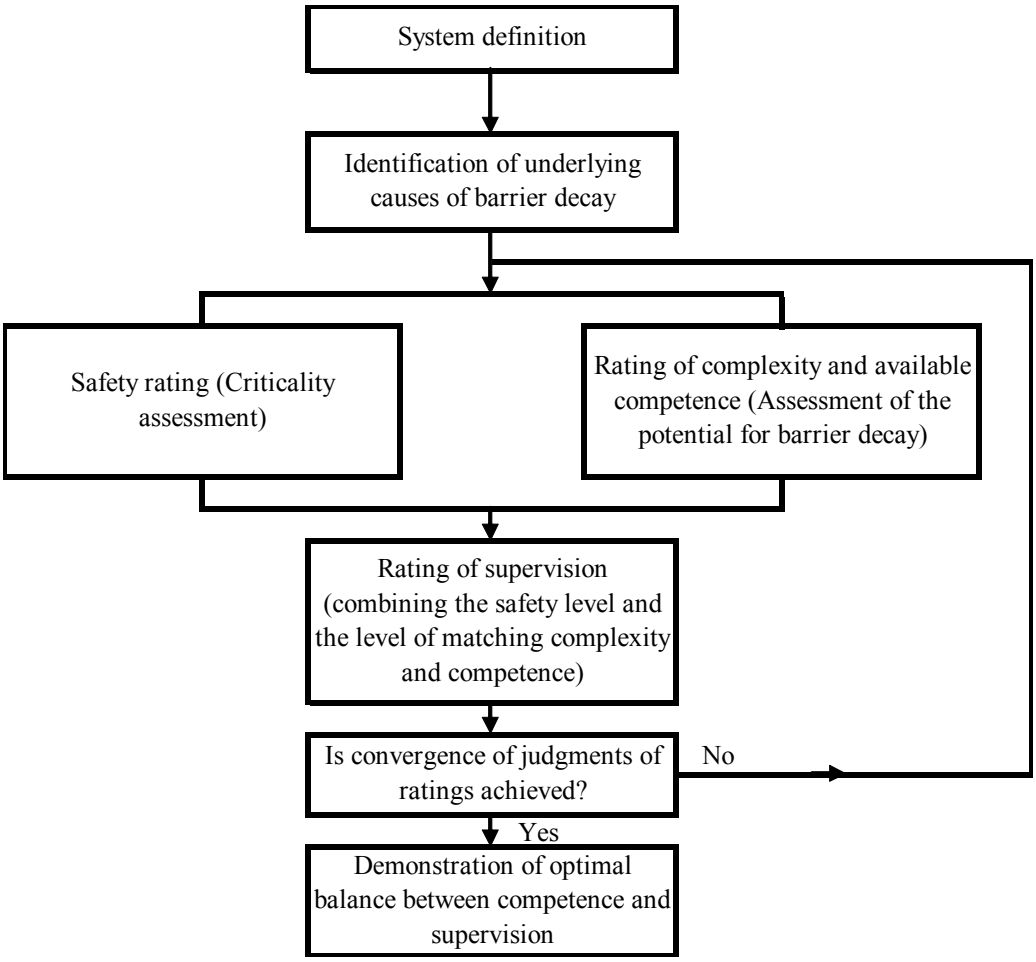


Figure 13 Risk based scheme for balancing competence and supervision

System definition

The system to be analysed is the process of balancing the personnel competence and the level of supervision. The main components of this process are as follows:

- Threat potential,
- Barrier effectiveness,
- Complexity of the procedure(s) and tasks required to maintain, operate and control the barrier during operations. Procedure(s) and tasks are related for example, to the maintenance of a technical barrier, or to following a control procedure, or to activity such as lifting, etc.
- Available competence is related to the person or a team of people who will perform the above tasks.
- Supervision is associated to on the job training, supervising, checking, etc. the person or the team performing the required set of tasks.

It should be noted that this approach is **barrier oriented** and that optimal balance between the available competence and supervision has to be determined for each barrier as a function of the above listed parameters.

Identification of underlying causes of barrier decay

Identification of underlying causes of barrier decay mainly due to the management and organisational failures is analogous to "hazard identification". The underlying causes of failure in this approach are represented by different combinations of mismatch or discrepancy between the main components of the "system" which could erode the integrity of the barriers. Term mismatch is used to denote underlying causes of decay or failure of the barrier socio-technical system. These are:

- Mismatch between threat potential and the barriers in place (insufficient or non-effective barriers in place of the high threat potential).
- Mismatch between the required competence and the complexity of a task related to barrier control and upkeeping (e.g. complex tasks and insufficient competence).
- Operating with less supervision than necessary (insufficient knowledge or information about competence and task complexity, insufficient supervision due to other reasons, etc.).
- Operating with inadequate competence and inadequate supervision (insufficient overall knowledge, production pressure, etc.); this in fact should be recognized as a violation.
- Operating with unknown (untested, uncertain) competence and/or supervision (new shift, new workforce, etc.)

Rating of safety

The term "rating of safety" (or criticality assessment) is used here instead of consequence analysis as in a standard risk analysis. Safety level refers to the match between threat potential and barrier effectiveness. Therefore, the "high" safety level corresponds to the low threat potential and high barrier effectiveness, the "appropriate" safety level corresponds to the same levels of threat and barrier effectiveness, and "low" safety level corresponds to high-medium and medium-low levels of threat and barrier effectiveness, respectively. Reciprocal of the level of safety would be level of criticality. Hence, the low safety level corresponds to a high criticality level, and vice versa.

Rating of matching of complexity and available competence

Mismatch between task complexity and the available competence has the potential to cause barrier decay/erosion. For example, if personnel with insufficient competence carry out complex tasks related to maintaining, controlling, operating, etc on the barrier, there is a possibility that errors or omissions could be made that will lay dormant in the system creating the latent conditions.

These latent conditions may combine with local circumstances or some other failures to cause barrier malfunction that may trigger threat initiation (Reason, 1998). Deciding on this propensity for the manifestation of underlying causes of failure could be loosely associated with assigning a probability or frequency in risk analysis. Adopting a three point scheme, for example low, appropriate and high, then a "low" level of matching (or slight mismatch) would correspond to higher probability of barrier decay/erosion than an "appropriate" matching level, and so on.

Rating of supervision

Rating of supervision is analogous to risk summation and denotes the combining of the judgments of safety level assessment and of the level of matching complexity and competence in order to indicate the required level of supervision. In other words, combining the level of safety and the judged potential for underlying causes of failure determines the required level of supervision.

Convergence of judgments

Rating of barrier effectiveness, complexity of tasks, available competence and supervision is based on judgments of various workforce disciplines and management. The initial variation or even divergence of views is quite common due to different perceptions of all parameters that play part in the assessment. Therefore revisiting the process of rating makes a good sense and leads to convergence of judgements which in itself is an optimising process.

Demonstrating optimal balance between competence and supervision

For three levels of supervision the conditions requiring remedial measures are developed. These conditions lead to the reduction of the potential for actuation of underlying causes of failure and to optimal balance between competence and supervision. A rule set, inspired by the Tolerability Doctrine HSE, 1992a), has been developed which aims to decrease the level of supervision to the standard (broadly acceptable level). The level of effort for the remedial measures is proportional to the level of supervision, i.e. the higher the level of supervision, the higher effort and cost are required to reduce it.

3.2.3 Development of the model

In the proposed risk model the level of supervision is determined by two key components a) level of safety of the barrier, and b) level of matching task complexity and personnel competence. The details of the model and how to establish the model components, i.e. the safety level and the complexity/competence matching level are described in detail in subsequent paragraphs.

3.2.4 Rating of safety (criticality)

The first step in establishing the risk model is to determine the **safety level** of the threat-barrier system. The level of safety has two components a) threat potential and b) the barrier effectiveness. Barrier effectiveness describes the level of prevention, attenuation, mitigation or control provided by the barriers (Section 2.5). The level of safety can be assessed on the basis of the 3 x 3 risk matrix shown in Figure 14.

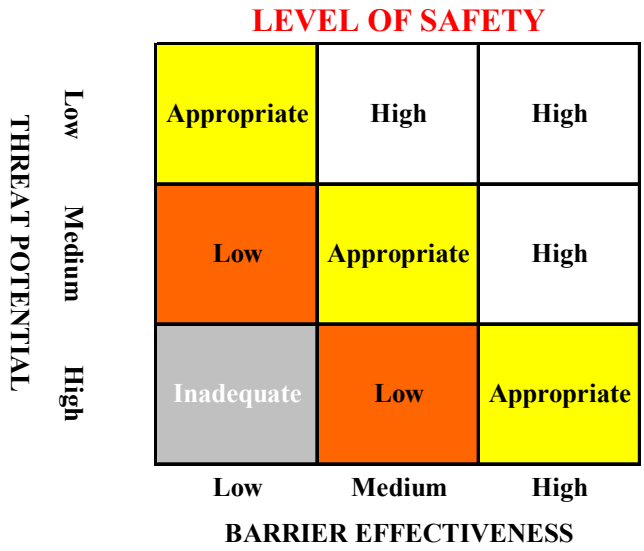


Figure 14 Rating of safety

When the threat potential is matched by the barrier effectiveness (both are judged to be on the same level) then the level of safety (defense) is assessed as "appropriate" (this applies when these two levels are low-low, medium-medium and high-high). When the level of threat potential is judged as greater than the barrier effectiveness, there are two possibilities. In the first case, i.e. medium-low or high-medium, the level of safety is "low". The second case is when the threat potential is high and the barrier effectiveness is low, and this case is defined as "inadequate". In this case logic of the barrier should be re-examined:

- Is this barrier really needed, i.e. what is its purpose or could this be done by another barrier?
- If it is needed, what can be done to improve its integrity?, etc.

It should be noted that the focus of the approach is on a single barrier at a time and a situation of an inadequate level of safety will be very rare, and it would not invalidate the original ALARP test in the safety case, but could point out that the barrier is superfluous. The decision whether to improve such a barrier or remove it altogether should be done in consideration of the complete threat-barrier system, i.e. looking at other barriers protecting from the same threat.

3.2.5 Rating of complexity/competence matching

The next part of the risk model determines the level of matching the barrier complexity and the available workforce competence. The resultant complexity / competence matching level is the combination of barrier complexity and the available workforce competence. Barrier complexity describes the **complexity of procedure(s) and tasks required to maintain, operate and control the barrier and keep it functional and operational** (Section 2.5). It is reasonable to assume that high complexity level requires a high competence level for this matching to be appropriate, and similarly medium complexity level requires at least the medium competence level, and so on. It follows that the matching level is inadequate for high complexity and low available competence. For the high level of complexity and the medium level of competence, the matching is low, Figure 15.

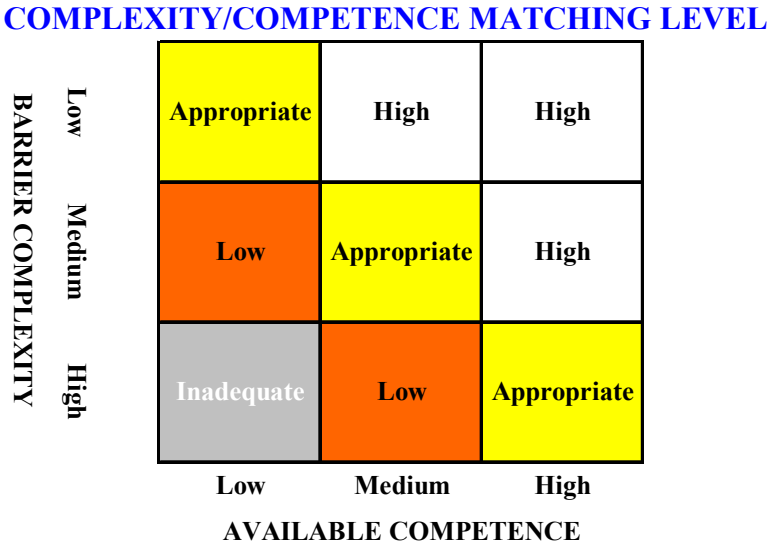


Figure 15 Rating of complexity and available competence

There are three levels of competence/complexity matching: low, appropriate and high. Low level of matching can still be made acceptable by increased supervision.

The "inadequate" level is the special case of high complexity of tasks and/or procedures and a low or insufficient level of competence. This situation is not allowed and the short-term remedial measure is to provide the supervisors to the team (competence of which was assessed as low), which in fact would move this case (along horizontal axis, Figure 15) to the low level of matching complexity and competence. The medium-term measure would be to improve competence.

3.2.6 Rating of supervision

In this step the rating of supervision is determined. The supervision is a function of the **safety level** and the **level of complexity/competence matching**. For the high level of safety and the high level of complexity/competence matching, the level of supervision is standard or normal. For the appropriate level of safety and the corresponding level of complexity/competence matching the level of supervision is cautionary. The same level of supervision applies for high/low and low/high levels of complexity/competence matching and safety, respectively. For a low level of safety and appropriate matching of barrier complexity / competence level and vice versa, the resultant level of supervision is interventionist supervision. The matrix for this evaluation is shown in Figure 16.

Standard (normal) level of supervision denotes the situations where there is sufficient safety margin. For example, take the high complexity/competence match and appropriate level of safety – this is a situation where the available competence is a level higher that the complexity of tasks for the given safety level. If the high complexity/competence level is matched by the high level of safety for which the barrier effectiveness is a level higher than the threat level, then safety margin is increased further. Safety margin in this context indicates that there is sufficient knowledge, experience and supervision to minimize possible deviations of errors in task execution.

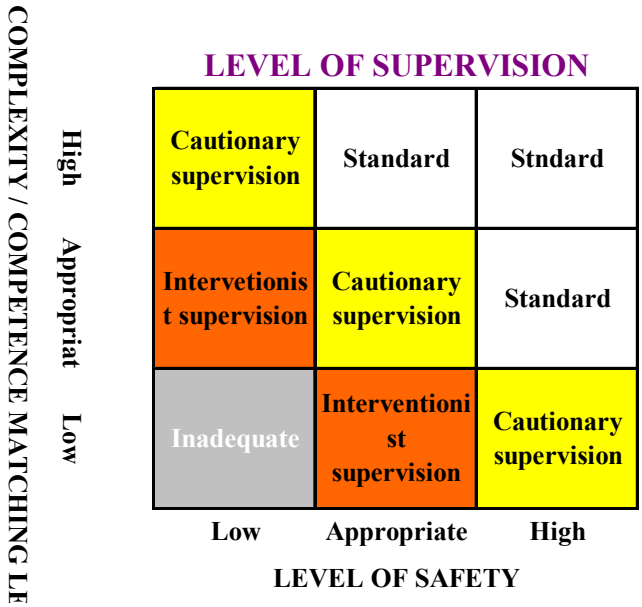


Figure 16 Rating of supervision

It follows that in situations where the levels of complexity/competence matching and safety level are matched, i.e. either both are the same, or one is a level up and the other is a level down or vice versa, there is no safety margin. Consequently, the corresponding cautionary supervision implies that some precautions need to be implemented, for example, like increased frequency of auditing performance of tasks and adherence to procedures.

The interventionist supervision (low matching of complexity/competence and appropriate level of safety, or vice versa) implies a situation where safety can be jeopardized. Hence the term "interventionist supervision" which is somewhere "between increased frequency of auditing and doing it oneself".

The situation of low level of complexity/competence matching and low level of safety is inadequate. This is intolerable situation and it means that the job/tasks cannot be executed.

3.2.7 Convergence of judgments

The described approach is based on judgments about threat potential, barrier effectiveness, complexity of tasks, available competence and supervision. It is quite usual to expect an evolution in judgments during the progression of the analysis. Therefore it makes a good sense to either perform the assessment again or revisit parts of the assessment.

Similar practice was applied to risk assessment of the construction to installation phases of large gravity base offshore structures. This type of risk assessment focuses on the engineering operations which are very structure-specific, and for which a database of operator active or recovery failures is very sparse, and hence it relies heavily on expert judgment. The approach adopted for risk reduction in those situations (Trbojevic et al., 1994) was based on two steps (a) the reduction of uncertainties by which risk reduction was achieved by means of "improved evidence", followed by (b) risk reduction based on the identified remedial measures of engineering, logistics or management type.

The re-assessment in this case cannot be treated as the reduction of uncertainties, but as the Bayesian[3] updating which offers the improvement in uniformity and confidence of the judgments made. The main aim of the iteration is to compare judgments made for similar barriers, similar levels of safety, similar complexity and competence levels, based on the gained experience, and correct any discrepancies. It is also essential to involve the workforce in this assessment.

The typical areas that may require revision are as follows:

1. Threat potential to which a barrier is exposed – in many cases this information is available in the safety case, but also for many hydrocarbon leak events the fault tree describing the causation part and therefore the threats may not have been developed.

2. Barrier effectiveness – the three point scale makes this rating easier, but judgment about human and organizational barriers needs to be made explicit and open to scrutiny and needs to involve the workforce.

---

[3] Frequently used interpretation of probability suggested by Bayesian theory, which holds that the concept of probability can be defined as the degree to which a person believes a proposition.

3. Complexity of procedures and tasks required to maintain the barrier, control it and keep it operational, etc. – this rating requires judgments from various workforce disciplines. In the case of human and organisational barriers there might be more differences in judgments since the comprehension by the workforce of why the tasks are required and the consequences of omitting a step is not often checked.

4. Competence – rating is required for the team of people, and therefore the averaging and subjectivity may cause differences in judgments.

5. Supervision – it is expected that the competence of supervisors is quite high, however in some cases the supervisors act more as project managers than experts, hence a source for different judgments.

3.2.8 Demonstrating optimal balance between competence and supervision

The main aim at this stage is the demonstration that, so far as is reasonably practicable, the optimal balance between competence and supervision has been achieved. The goal-setting approach for improvement in safety has been present in all key steps of this approach as follows:

Rating of safety - Three levels of safety high (white), appropriate (yellow) and low (red) are identified, Figure 14. The high level is considered acceptable, while the appropriate and low levels are considered tolerable for the time being if the further improvements are not reasonably practicable. It should be recognized that there is a duty to continue to investigate the scope for improvement of barrier rating through technological advances for technical barriers and improvements in the procedures for human and organizational barriers.

Rating of the matching between complexity and competence – Again there are three levels of matching: high (white), appropriate (yellow) and low (red), Figure 15. The high rating is acceptable, while the appropriate and low rating is tolerable in the same sense as for rating of safety. The scope for improvement of this parameter is obvious because the competence level can always be improved. On the other hand the judgment about procedure and task complexity is inevitably subjective and is influenced by the competence of the assessors and their view on complexity with respect to the workforce. Complexity may also change, for example new equipment may be simpler to maintain, control and operate, or the procedures and tasks can be simplified.

Optimising supervision – Three levels of supervision can be interpreted in a goal-setting sense along the lines of the Tolerability Doctrine as shown in Figure 17. The Tolerability Doctrine definitions are on the left hand side, while the supervision levels are given on the right hand side in Figure 17. The supervision acts to reduce the potential for activation of underlying causes of failure which in turn depends on the level of matching the competence and complexity and the level of safety. Given that these latter factors have been rigorously assessed, the resultant level of supervision will fall into one of three regions as follows:

1. Unacceptable region – where matching of complexity and competence and the level of safety are both low and there is therefore no level of supervision that would suffice for safe operation. The required procedure and tasks should not be executed.

2. Tolerability region – where the level of supervision can be tolerated for the time being but with a duty to seek improved safety through increased supervision and risk reduction measures such that::

- interventionist supervision (somewhere between increased auditing and doing the work oneself) requires these actions to continue until their cost becomes grossly disproportionate to the benefits achieved, or
- cautionary supervision (increased auditing) requires actions unless their costs would significantly exceed the improvements gained.

3. Broadly acceptable region – where the level of supervision is standard and the improvements are introduced in parallel with the improvements in the Safety Management System)

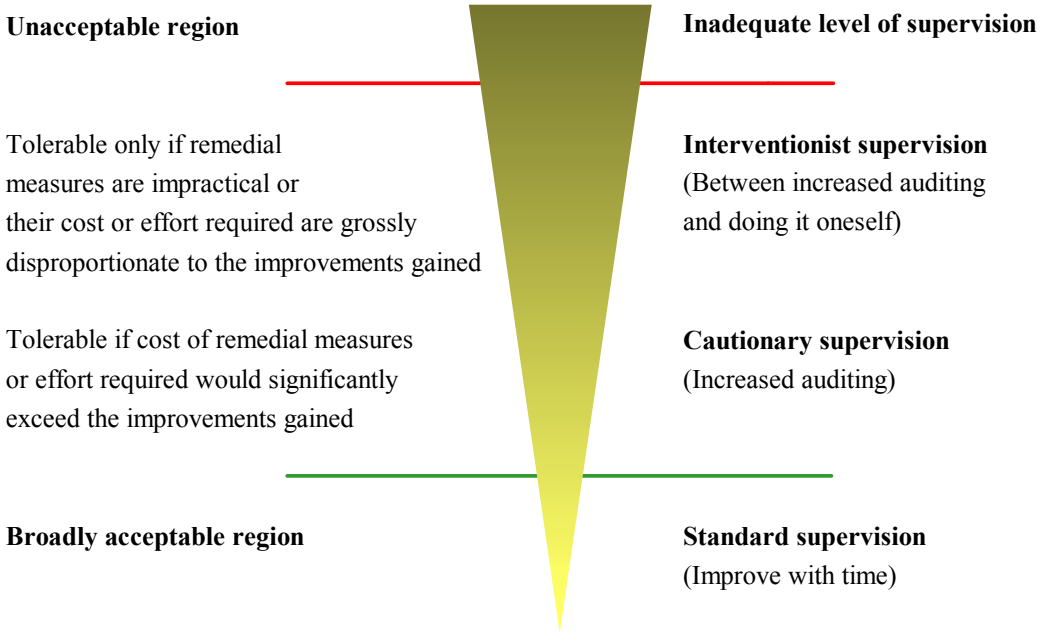


Figure 17 Assessing the level of supervision

The overall imperative is the need for continuous improvement in safety of operations to be sought. The level of supervision complements and supports good operating practice where there is a demonstratable matching of the level of safety and the competence/complexity profile. The scheme presented above is proposed as a means to address this challenge and to display the results in a transparent manner.

4 WORKFORCE INVOLVEMENT

4.1 Introduction

The bow tie approach has the potential for significant improvement of workforce involvement in the following areas:

1. Comprehension of major hazards,
2. Involvement in safety case,
3. Safety management processes,
4. Safety management.

4.2 Improved comprehension of major hazards

Visualisation of threat / barrier / initiating event / consequence systems in bow tie diagrams facilitates comprehension of hazard prevention and protection required for safe operations on an offshore facility. The interaction and interdependence between the primary barriers and their decay/failure modes and the secondary barriers are also visually displayed. Removing a barrier or a set of barriers for the purpose of maintenance can immediately indicate the possible weakening of the system.

By some assessment the Brazilian rig P-36 that sank in the Atlantic had at least eight barriers removed or faulty before the fatal accident happened. This indicated that there was a lack of knowledge of the overall system and absence of a graphical scheme which could have displayed erosion of safety by the removal of barriers.

Better understanding of hazard prevention and protection contributes to increased knowledge of major hazards and potential accidents. Since the barriers are associated with the equipment (technical) or with procedures and /or tasks, focusing on barriers also provides better insight into the level of complexity of their control and maintenance. Therefore improved understanding of barriers and their maintenance/control contributes to improving facility specific (local) and trade/skill knowledge.

The role of the barrier rule set is important as it empowers the workforce to develop the bow tie diagrams themselves without relying on external specialists. The rule set facilitate channeling of the workforce experience, knowledge of facility specifics, of near misses, etc into better understanding of major hazards and possible improvements.

An example of the lack of proper information and knowledge is given in the description of the gas leak accident by the Norwegian initiative Working together for Safety (Samarbeid for Sikkerhet).

Gas leakage on Tordenskjold platform

The incident happened in 2005. An area operator during walk rounds noticed a bubble gas leak on a pressure gauge on an instrument pipe. She tries to stop the leak by tightening the pipe connection. While the operator was holding the pipe with one hand and applying pressure to the connection, the pipe twists and the leak got bigger. Gas pressure was in excess of 150 bar and risk of explosion was great. There have been similar incidents in the same company before, but during the accident investigation none of the interviewees mentioned the previous incident. The accident analysis found the that the actuating factor was that work was being conducted without the plan, work permit or safe job analysis, that work on pressurised equipment should

not be carried out without necessary permission, and that small unplanned jobs are the frequent cause of incidents and accidents that could have been avoided had the system been followed. The recommendations followed the improvement loop:

1. *Plan – job should have been planned*
2. *Do – Job should have been started by a phone call to the Control Room. This could have resulted in an overview of the procedure for the job.*
3. *Act – Next step is to evaluate the job. Did the job go as planned?*
4. *Improve – Evaluate recommendations for safety improvement.*

What is interesting with this example is the procedural way of thinking, basically emphasising a failure to learn from previous similar incidents and which procedures have been breached, for example work on pressurised equipment, unplanned job, failure to get a work permit, failure to check with the Control Room, etc. This incident analysis is the product of a quality management system where the focus is on the procedures which have to be followed. So one recommendation was if in doubt about the procedure, just ask. Interestingly the need to know the reason or the specifics of the process has not been mentioned. There is also a statement that "work permit is required where the normal barriers are taken out of service".

In a bow tie approach which is barrier-focused, an operator would have been aware of the barriers related to that particular process equipment and the specifics such as high pressure and the purpose of instrumentation. The operator should have also been aware of the responsibilities for the related barriers and if out of his scope should have immediately reported it. On the other hand, the operator on duty was responsible for that particular equipment and should have known what to do, either to isolate the pressure gauge and try to tighten the fittings, or to report to the Control Room.

4.3 Improvement of safety by involvement in safety case

A central purpose of a safety case is an examination of the adequacy of existing safety measures for avoidance, prevention, control and mitigation of major accidents. Such an examination entails consideration of potential further safety measures that could, on grounds of engineering safety, be put in place. This consideration should, in order to be consistent with a precautionary approach to safety, err on the side of safety when making decisions about the reasonable practicability of potential further measures. Current practice is for a safety case to include a significant amount of theoretical analysis that is relatively inaccessible to all but the risk assessment community specialists.

The HSE has highlighted the central role that the offshore workforce can play in safety case by being involved in the engineering task of identifying real improvement in safety, improvements that are reasonable from an engineering perspective that makes full use of the day-to-day and grass-roots operational experience of various workforce disciplines. The bow ties facilitate a more intimate participation of the workforce in the processes of hazard identification which forms the solid foundation on which the continuous safety improvement is built.

4.4 Improvement of risk management processes

Involvement of the workforce in optimising safety management processes is essential for the following reasons:

1. The workforce involvement in optimising processes not only increases the experience of the group of workers which can contribute to the process (contributory expertise) and but also of other groups of workers who acquire interactional expertise (Collins, 2006). Interactional expertise facilitates the understanding the overall issues related to the particular facility. This would in particular apply to identification of threats, underlying causes of failure, etc.
2. Evaluating complexity and competence is based on understanding the work that has to be done on the barrier (to maintain, control or operate it) and the available and required competence. Understanding why and how something has to be done on the barrier facilitates appreciation of the barrier function and its failure. This task can also elicit potential differences between the design intent and the operational experience or misconceptions between the designers and operators. This task increases not only contributory expertise, but also the interactional expertise as other workers learn how to conduct the analysis of a process without necessarily doing or understanding all the specifics of the process.
3. Understanding safety optimisation (the goal-setting approach to safety) serves as the basis for safety training. Safety optimisation can be applied to any process by challenging the existing situation along the lines "what more can we do?", or "how can we do it better", "what can we change?", etc.

4.5 Involvement in safety management system

Increased and focused information about the major hazard accidents, barriers, procedures and tasks should facilitate discussions, assessment and improvements of safety. This is in particular important with the human / organisational barriers such as Job Risk Assessments, Permit to Work systems, plans, manuals, etc. Both the workforce and the management can also visualise the importance of fundamental barriers such as management of change, procedural reviews, corporate audit, etc. The following areas of safety management which seem to be directly linked to the barrier approach, have the potential for improvement:

1. Raising safety issues and monitoring their handling by management. Visualisation of the distribution of responsibilities for barrier facilitates monitoring of their handling by the management and workforce.
2. Challenging the decisions made by management in their determination of the reasonable practicability of proposed improvement. It is envisaged that most of the improvements will be in systems of work, the way things are done, however improvement of technical barriers is by no means excluded.
3. Training – it is often the case that members of the workforce themselves are conscious of the need for further training, for maintaining and developing relevant skill, and may be concerned when there is inadequate provision for such training. It is essential that in such situations there is a system in place to raise training needs issues, to prompt the management to pursue these issues and to enable the workforce to monitor the progress of the issues and challenge any decisions or lack of management action as the need arises.
4. Organisational learning – near miss and accident investigation and the fundamental barriers such as operational review, best practice review, corporate audit, etc serve to update the existing experience pool which can be utilised for further safety improvements. Barrier model is can serve as depository of major hazards knowledge and as means of transfer of knowledge from the experienced workers to the newly employed.

4.6 Improving safety management audits

The audit systems are designed to assess the main elements of safety management, for example, policy, organisation, planning and implementation, measuring performance, audit and reviewing system (HSE, 1997). The audit quality depends on the competence of an auditor who makes judgement on the adequacy of the safety management system by comparison of the results against a relevant standard or benchmark. Key performance indicators usually include assessment of the degree of compliance with safety requirements, identification of areas where the safety system is inadequate, assessment of the achievement of specific objectives and plans, accident and incident data accompanied by analysis of both the immediate and underlying causes, trends and common features, etc.

Performance indicators can be reactive and proactive (Reason, 1998). Reactive performance indicators, commonly in use, are based on the analysis of causes and effects of incidents and accidents. The quality of reactive indicators depends on the depth of the analysis of underlying causes of incidents and accidents.

Proactive performance indicators have a diagnostic role and can be used before an event to assess the safety health of the system. These indicators focus a) on defences (barriers) in order to check for "holes" or barrier decay, and b) organisational latent conditions and weaknesses. In general, the proactive indicators are rarely utilised and in this area the ingenuity of an auditor is required.

The proposed barrier approach linking the major hazards, underlying causes of barrier decay/failure, complexity of safety critical tasks, barrier decay levels and the workforce provides more opportunity for proactive monitoring and consequently improved auditing system for the following reasons:

1. Most relevant barrier decay modes (underlying causes of failure) are identified and the secondary (fundamental) barriers are in place to detect latent conditions and strengthen the primary barriers. The reason for and the importance of monitoring of the barrier decay modes and the secondary (fundamental) barriers are visible and understood by the workforce.
2. Barrier decay level can be used to control the frequency of application of fundamental barriers such as audits.
3. Barrier decay level is also an indicator of barrier "robustness" which in the case of rapid decay and increasing frequency of audits can highlight the need to redesign or strengthen the primary barrier. Hence, rapid decay can be used as an indicator of the weakness of the primary barrier.
4. Due to comprehension and visibility of the primary barriers, their decay modes and the corresponding secondary barriers, the monitoring of the barrier decay and the application of secondary (fundamental) barriers can performed by the workforce (self monitoring).

5 REFERENCES

Collins, H. et al. (2006). *Experiments with Interactional Expertise*, KES, School of Social Sciences, Cardiff University, Cardiff CF10 3WT. For publication in Studies in History and Philosophy of Science, 37A, 4, December.

Haugen, S., Seljelid, J., Sklet, S., Vinnem, J.E., Aven, T. (2007) BORA – Operational risk analysis – Total risk analysis of physical and non-physical barriers, H3.1 Generalisation Report for NFR/HSE/OLF, Rev. 1, 31 January.

Health and Safety at Work etc Act 1974, SI 1974/1439, The Stationery Office 1974 ISBN 0 11 141439 X.

Hollnagel, E. (1999) *Accident analysis and barrier functions*, in Accidents and barriers project TRAIN, Version 1.0, February.

HSE (1992a) *Tolerability of risk from nuclear power stations*, HMSO 1988 and 1992, ISBN 0 11 886368 1.

HSE (1992b) Organisational, management and human factors in quantified risk assessment – Report 1, CRR No. 33/1992, L.J. Bellamy and T.A.W. Geyer (ed. J.C. Williams), Technica, London.

HSE (1995) Generic Terms and Concepts in the Assessment and Regulation of Industrial Risks, Discussion Document.

HSE (1997) Successful health and safety management, HSG65, HSE Books, ISBN 0 7176 1276 7

HSE (1999) A guide to the Control of Major Accident Hazards Regulations, HSE Books, 1999, ISBN 0 7176 1604 5.

HSE (2000) Examples of effective workforce involvement in health and safety in the chemical industry, CRR 291/2000.

HSE (2003a) Offshore Hydrocarbon Releases Statistics and Analysis, 2002, HID Statistics Report, HSR 2002 002, February.

HSE (2003b) *Competence assessment for the hazardous industries*, Prepared by Greenstreet Berman Ltd, Research Report 086.

HSE (2007a) *Development of a working model of how human factors, safety management systems and wider organisational issues fit together*, Prepared by White Queen Safety Strategies & Environmental Resources Management, Research Report, RR 543

HSE (2007b) *Key programme 3 – Asset integrity inspection*, Hazardous Installation Directorate Offshore Division, Interim Final report, October.

Hurst, N.W., et al. (1991) A Classification Scheme for Pipework Failures to Include Human and Socio-Technical Errors and their Contribution to Pipework Failure Frequencies, Journal of Hazardous Materials 26, 159-186.

IEC:61508 (1998). Functional safety of electrical / electronic / programmable electronic safety-related systems. International Electrotechnical Commission, Geneva.

IEC:61511 (2002). Functional safety – safety instrumented systems for the process industry sector. International Electrotechnical Commission, Geneva.

ISO:13702 (1999). Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines. International Organisation for Standardisation, Geneva.
ISO:17776 (2000). Petroleum and natural gas industries – Offshore production installations – Guidance on tools and techniques for hazard identification and risk assessment. International Organisation for Standardisation, Geneva.

Kletz, T. (2006) *Learning from accidents*, Third edition, Gulf Professional Publishing.

McQuaid, J. (2007) Personal communication.

Miles, R.W. (2006). Managing a safe workplace during change: a knowledge approach to competence and risk management, OD 3.6.

Reason, J. (1998) Managing the Risks of Organisational Accidents, Ashgate Publishing Ltd., Aldershot.

Resilience Engineering (2006) Eds. Erik Hollnagel, David D. Woods and Nancy Leveson, Ashgate Publishing Ltd., England.

Rimington, J (2007) Personal communication.

Risk Support Limited (2007) Active Bow Tie – A tool for displaying hazard analysis and for improving and energising safety management, Version 1.7, July.

Salvi, O. and Debray, B. (2006) A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive, Journal of Haz. Materials, 130, 187-199.

SIPM (1995) *THESIS – HSE Manual*, EP 95-0323, 1 November.

Sklet, S. (2006) *Safety barriers: Definition, classification, and performance*, Journal. of Loss Prevention in the Process Industries, 19 (2006) 494-506.

Svenson, O. (1991) The Accident Evolution and Barrier Function (AEB) Model Applied to Incident Analysis in the Processing Industries. Risk Analysis, Vol. 11, No. 3, 499-507.

Trbojevic, V.M. (2001) *Linking Risk Assessment of Marine Operations to Safety Management in Ports*, 6th Biennial Marine Transportation System Research and Technology Coordination Conference, Washington DC, 14-16 November.

Trbojevic, V.M., Gudmestad, O.T., Rettedal, W.K. (2007) *Influence of organisational factors on risk analysis of marine operations*, ESREL 2007, Stavanger, Norway, 25-27 June.

Trbojevic, V.M., Bellamy, L.J., Gudmestad, O.T., Rettedal, W.K. (1994) *Methodology for the Analysis of Risks During the Construction and Installation Phases of an Offshore Platform*,

Special Issue: “Safety on offshore process installation: North Sea”, J. Loss Prev. Process Ind., Volume 7, Number 4.

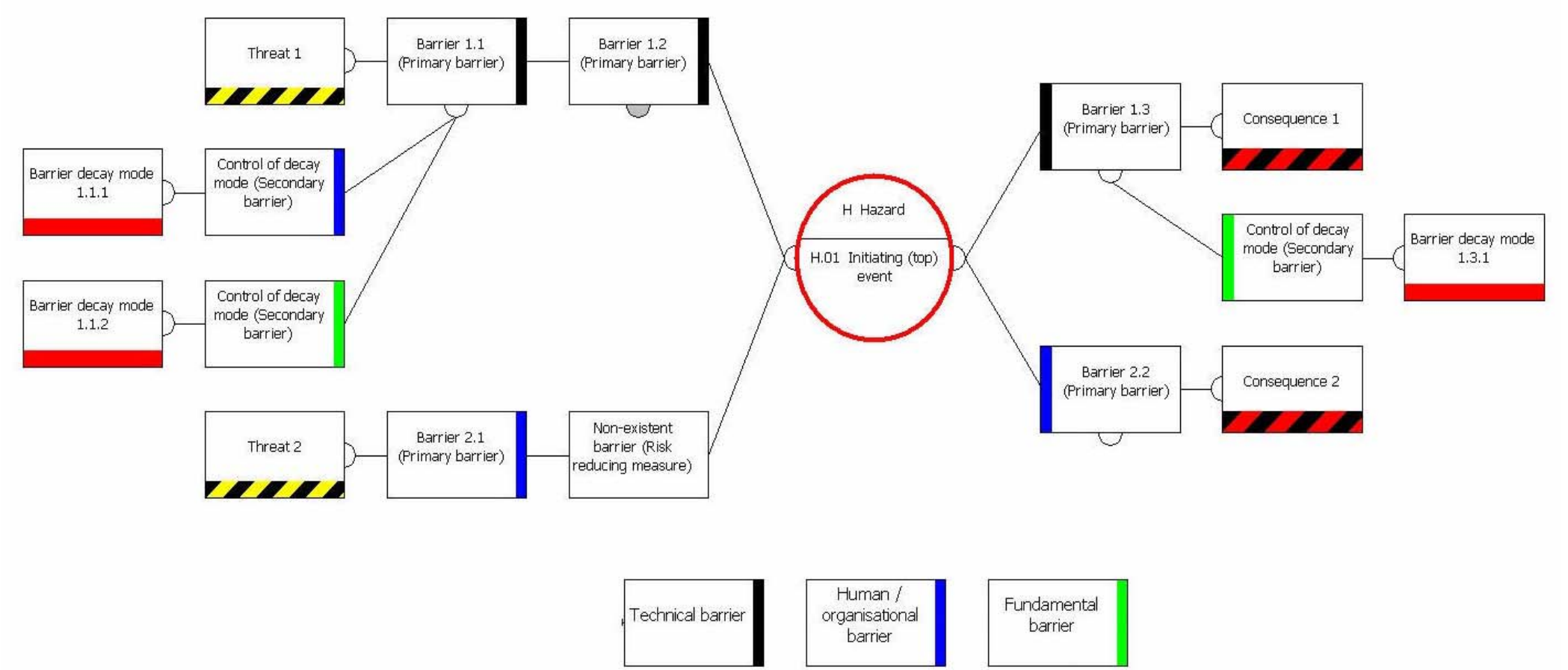
Working together for Safety, http://www.samarbeidforsikkerhet.no/

APPENDIX A – WORKFORCE RESPONSE TO BARRIER APPROACH

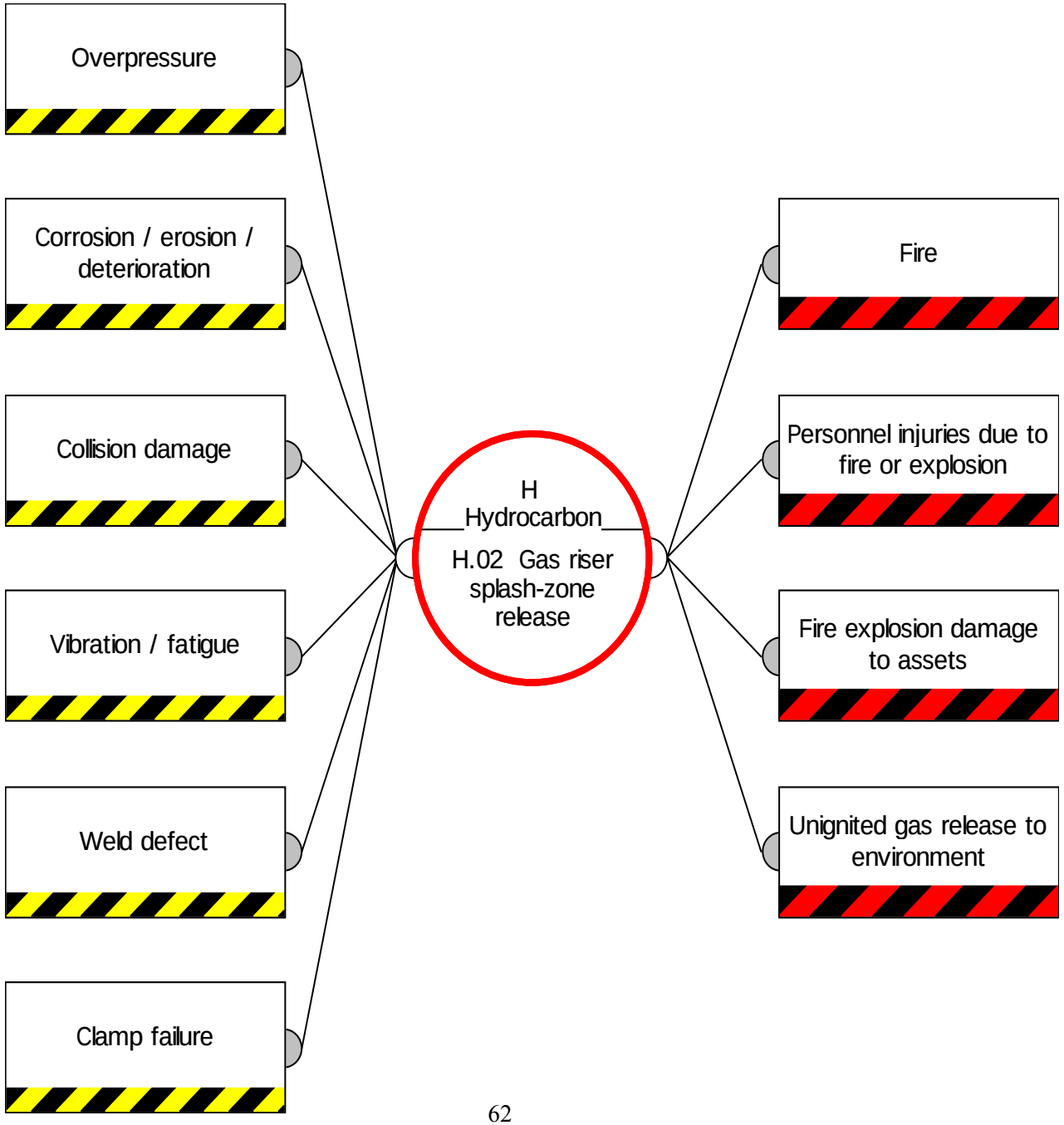
Questionnaire	13 Offshore Safety Reps	5 Management
	Positive answers are indicated with numbers	**Positive answers and indicated with numbers**
Did you find this approach helpful in understanding hazard management?	12 ; not really	5 ;
How would you improve this approach?	Present the process of obtaining bow ties; use visio/video?; Take more time to cover presentation; Change slide format; Better handouts and in colour;	Differentiate between "soft" hazards and "hard" hazards (soft = people & procedures, hard = design); Slightly simpler approach; Table top review against our procedures; Simplify it if possible;
How would you use this approach?	Task planning; Reinforcing the message that people arte involved and that the failures could result from more than one person; At safety meetings; match the procedures to each of the barriers; Could be used for raising permits; Review existing systems; During risk assessment; Large screen to increase viewing area;	HAZOP / HAZID; Risk assessment; When doing a risk assessment; Fault / failure investigation;
Did you find this presentation easy to understand?	9 ; Not at all; Too much detail as sheets led to too much "rustling of paper" background noise as people attempted to follow slides on screen with A3 sheets; Difficult to follow and switching between the handouts and listening was difficult; Could add to day-to-day management systems; Having the handouts was a great benefit as the content on page on screen was difficult to see;	Yes & no - for the workforce to grasp the concept fully they need a comparison between current method / QRA and how this approach "involves" them and not just a scientist; Hard to follow with handouts; Very easy, good presentation; Yes; Hard to follow A3 sheets; No, not enough time;
Any suggestions on how this presentation could be improved?	Make slides readable; More details; Take more time and get the handouts before the presentation; More details;	Better slides / explanation; Improve quality of the slide show and do away with the A3 sheets; Increase time;
Are there any other applications where this approach could be helpful (for example, Job Risk Analysis, PTW system, etc)?	Risk assessment;	Job planning; Yes to our systems; All types of investigations;

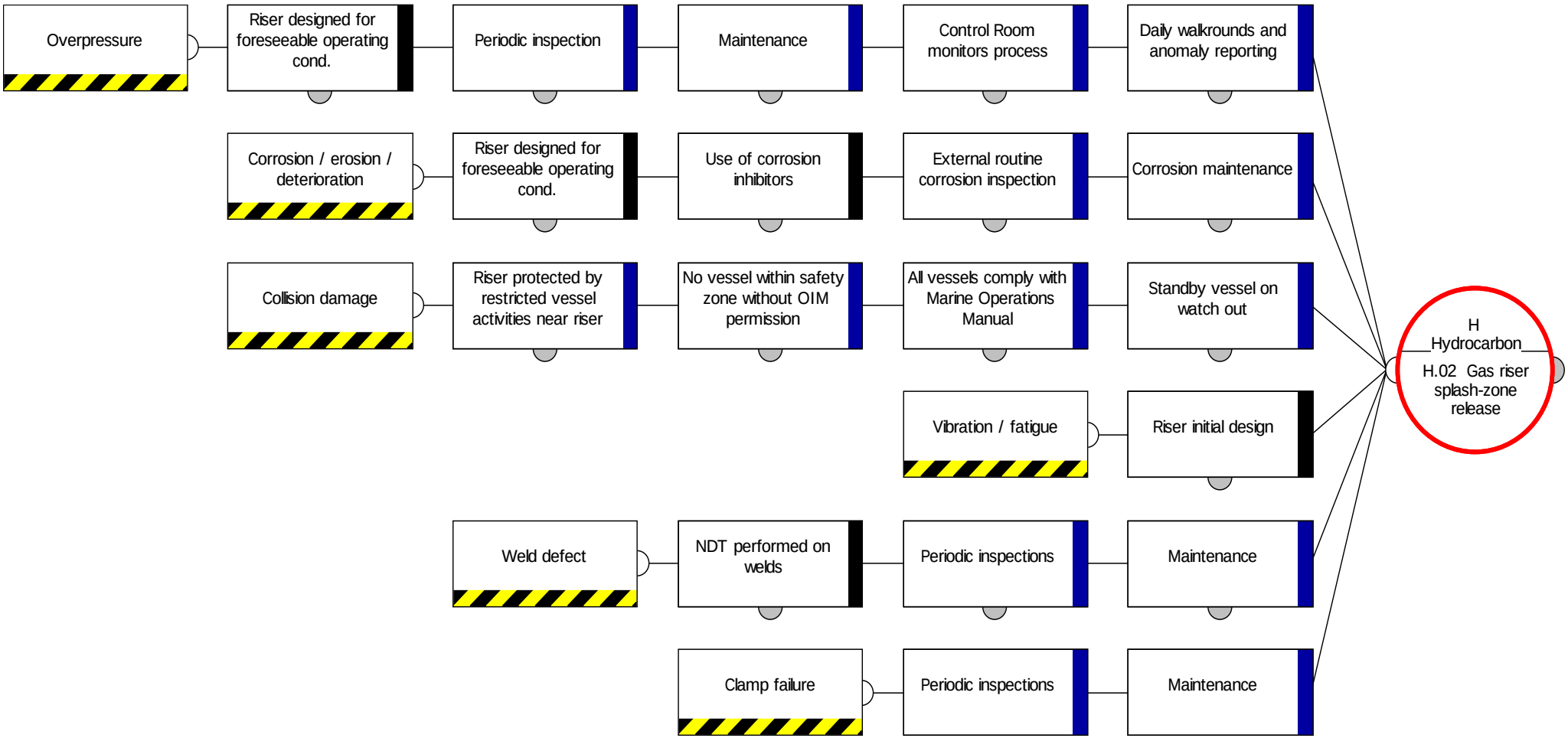
APPENDIX B – EXAMPLES OF BOW TIES

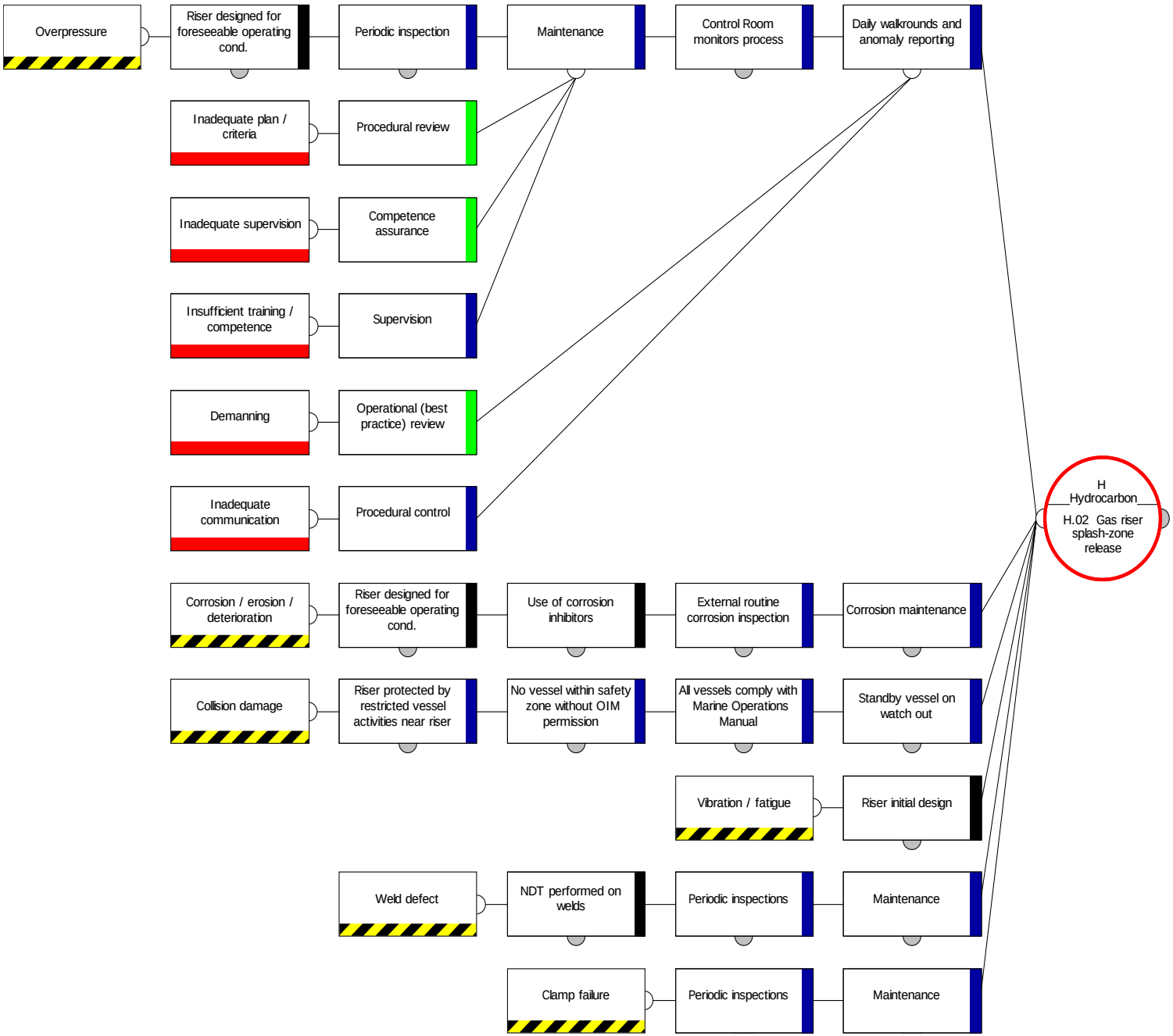
Active Bow Tie[3] Notation

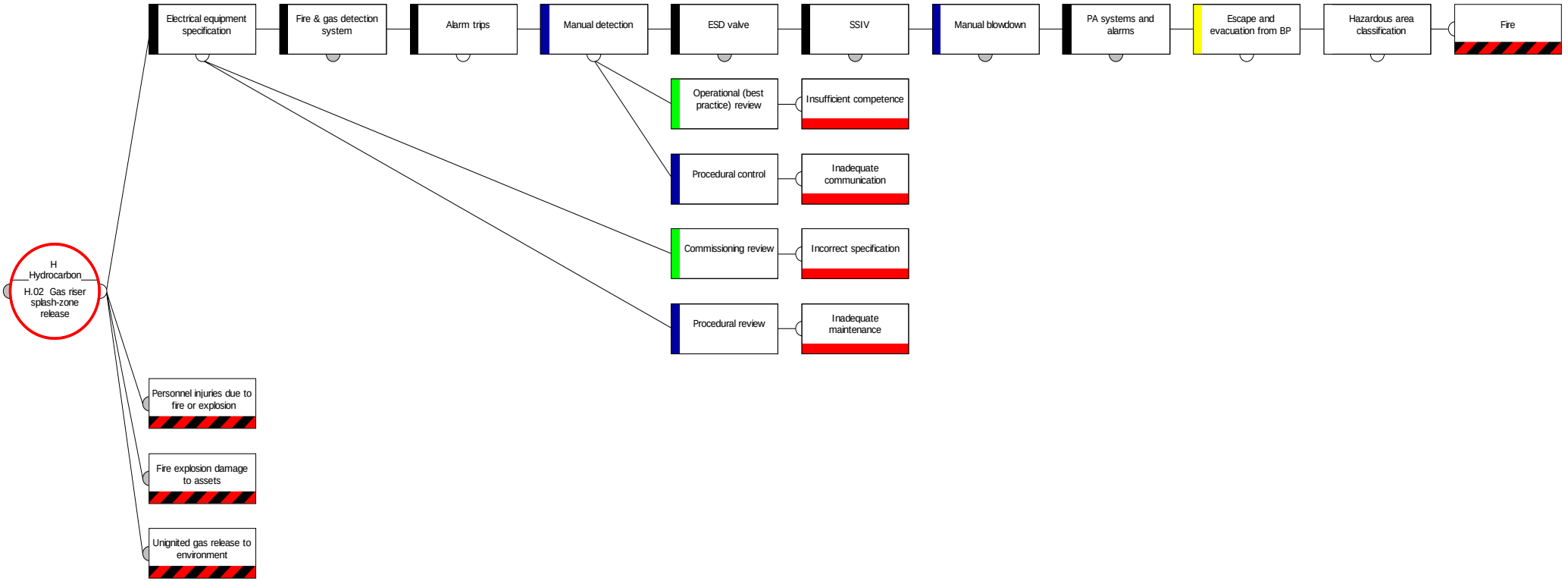


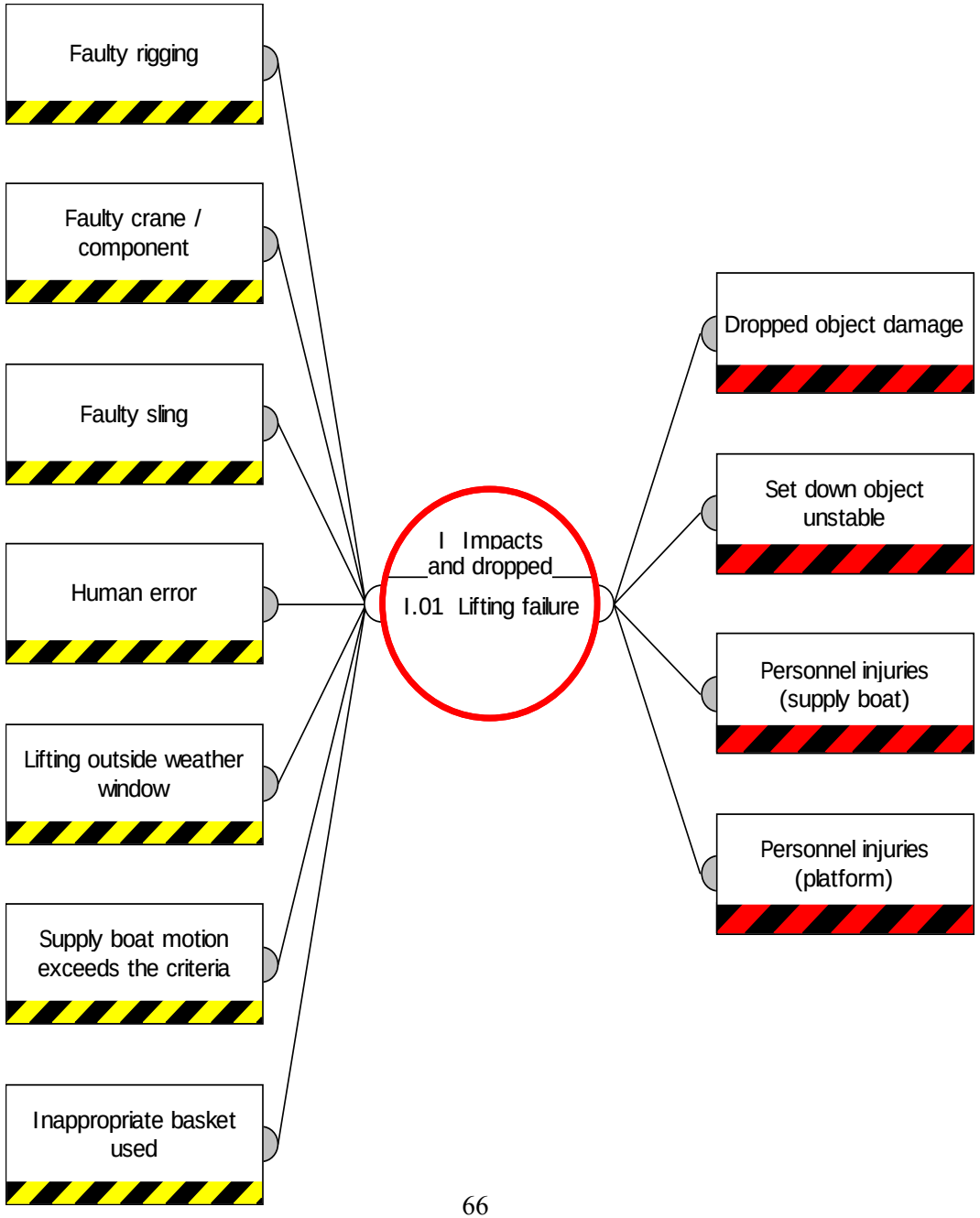
[3] Risk Support Limited, Active Bow Tie – A tool for displaying and improving hazard analysis and energising safety management, Version 1.7, July 2007

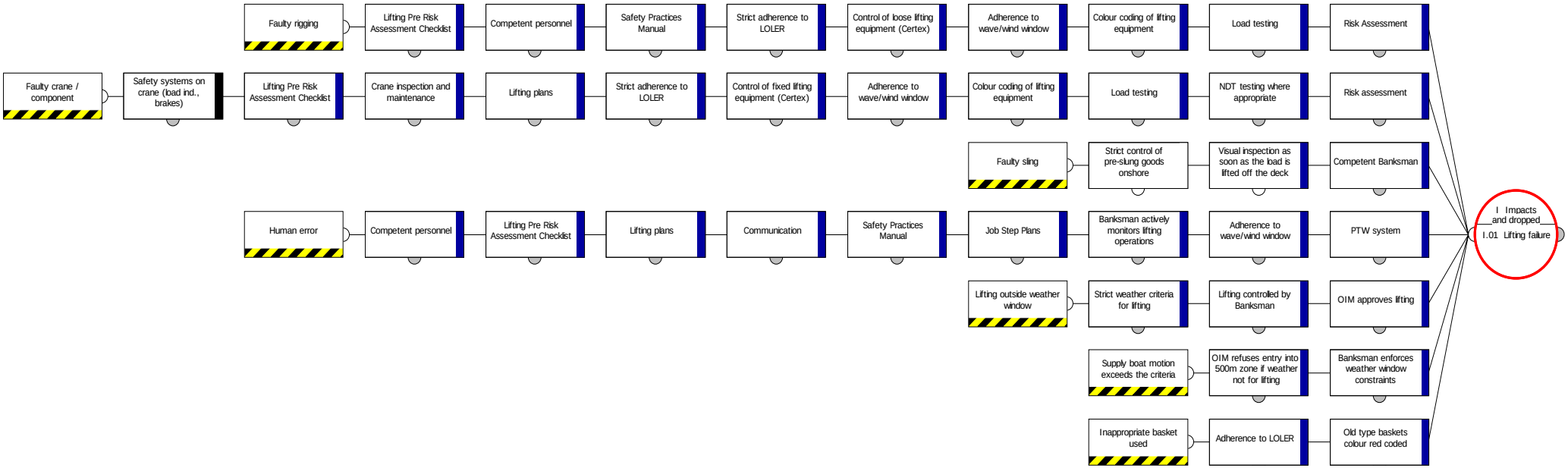

Overpressure
Corrosion / erosion / deterioration
Collision damage
Vibration / fatigue
Weld defect
Clamp failure
H
Hydrocarbon
H.02 Gas riser splash-zone release
Fire
Personnel injuries due to fire or explosion
Fire explosion damage to assets
Unignited gas release to environment

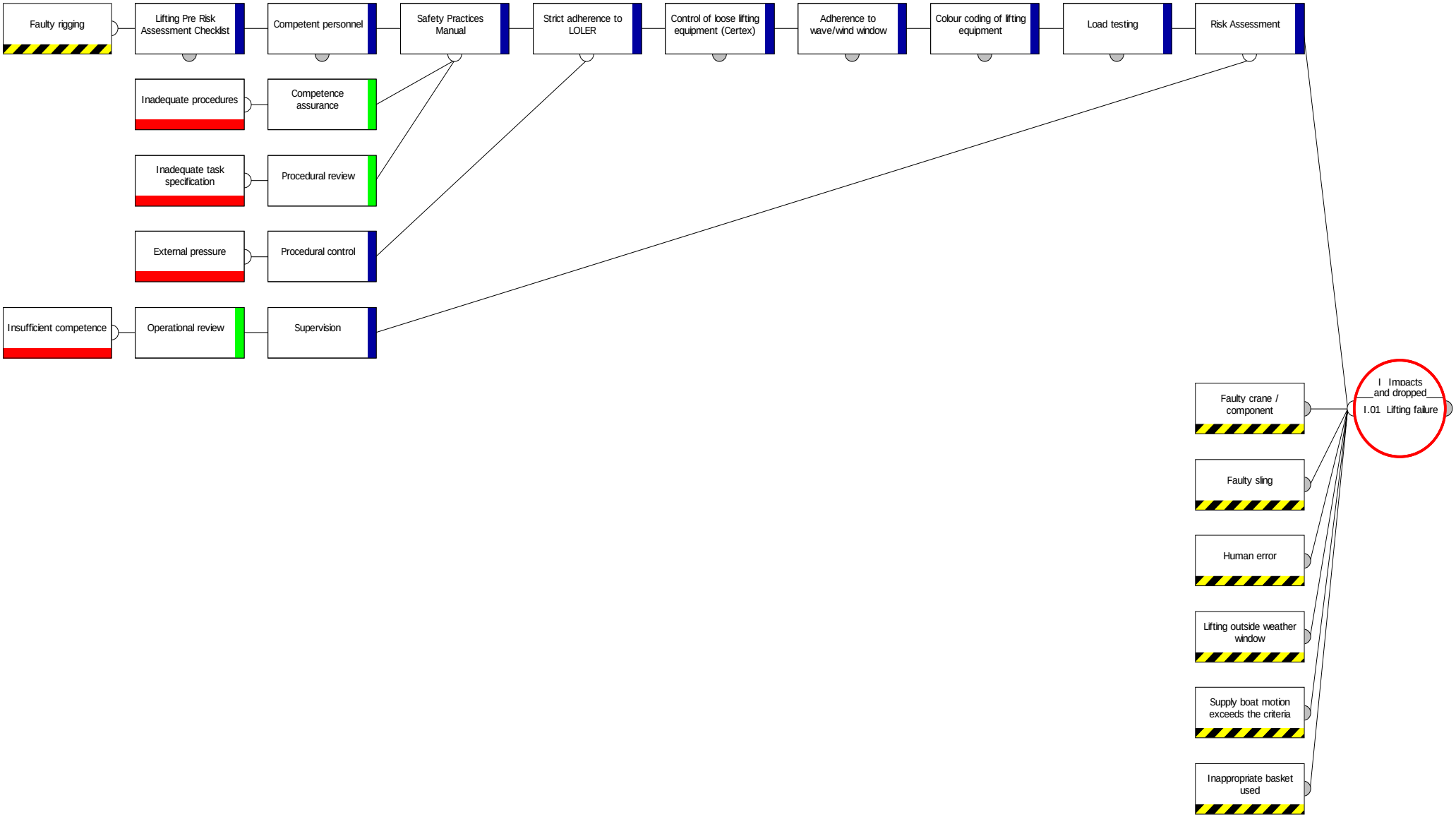

Overpressure
Riser designed for foreseeable operating cond.
Periodic inspection
Maintenance
Control Room monitors process
Daily walkrounds and anomaly reporting
Corrosion / erosion / deterioration
Riser designed for foreseeable operating cond.
Use of corrosion inhibitors
External routine corrosion inspection
Corrosion maintenance
Collision damage
Riser protected by restricted vessel activities near riser
No vessel within safety zone without OIM permission
All vessels comply with Marine Operations Manual
Standby vessel on watch out
Vibration / fatigue
Riser initial design
Weld defect
NDT performed on welds
Periodic inspections
Maintenance
Clamp failure
Periodic inspections
Maintenance
H
Hydrocarbon
H.02 Gas riser splash-zone release

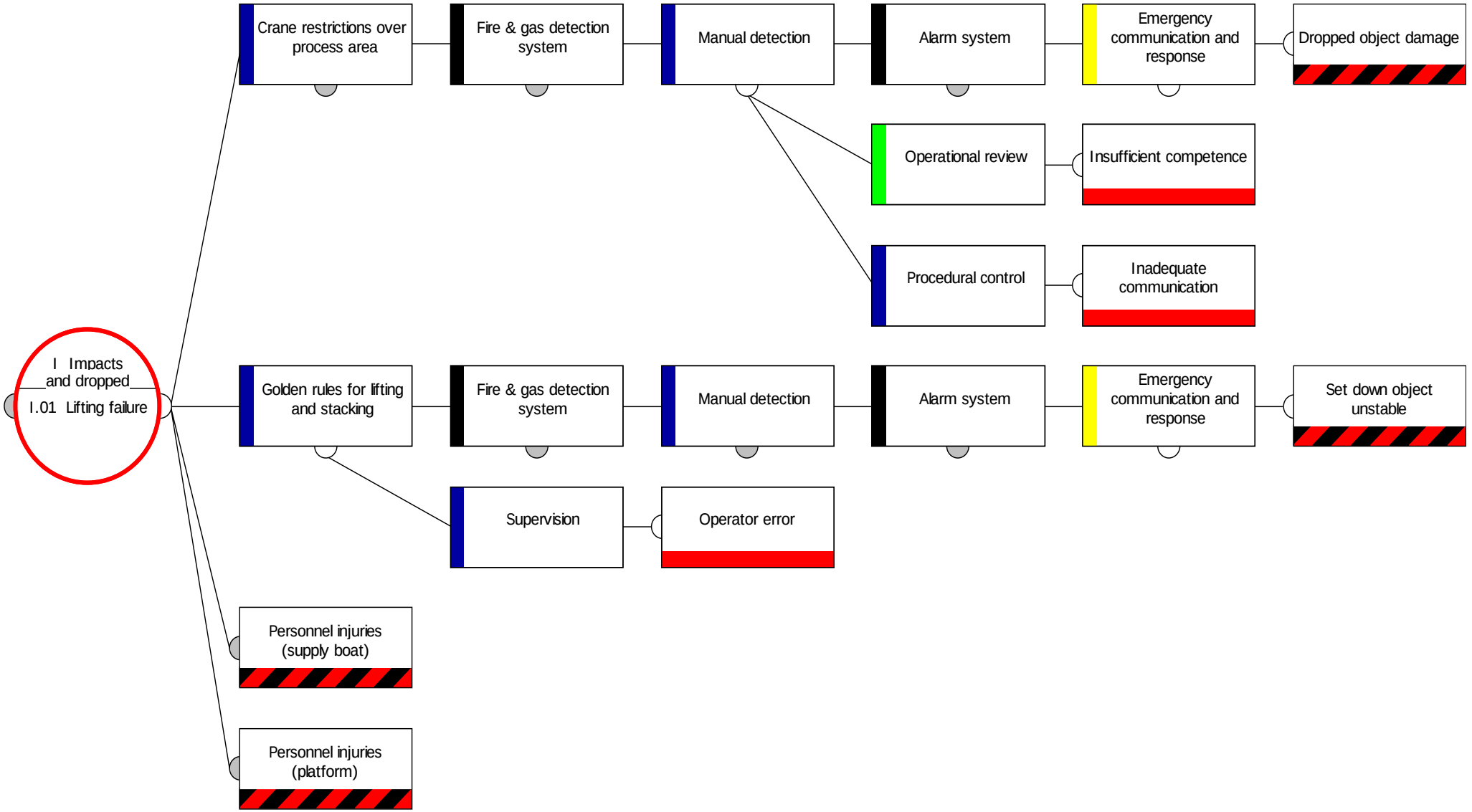

Overpressure
Riser designed for foreseeable operating cond.
Periodic inspection
Maintenance
Control Room monitors process
Daily walkrounds and anomaly reporting
Inadequate plan / criteria
Procedural review
Inadequate supervision
Competence assurance
Insufficient training / competence
Supervision
Demanning
Operational (best practice) review
Inadequate communication
Procedural control
H Hydrocarbon
H.02 Gas riser splash-zone release
Corrosion / erosion / deterioration
Riser designed for foreseeable operating cond.
Use of corrosion inhibitors
External routine corrosion inspection
Corrosion maintenance
Collision damage
Riser protected by restricted vessel activities near riser
No vessel within safety zone without OIM permission
All vessels comply with Marine Operations Manual
Standby vessel on watch out
Vibration / fatigue
Riser initial design
Weld defect
NDT performed on welds
Periodic inspections
Maintenance
Clamp failure
Periodic inspections
Maintenance

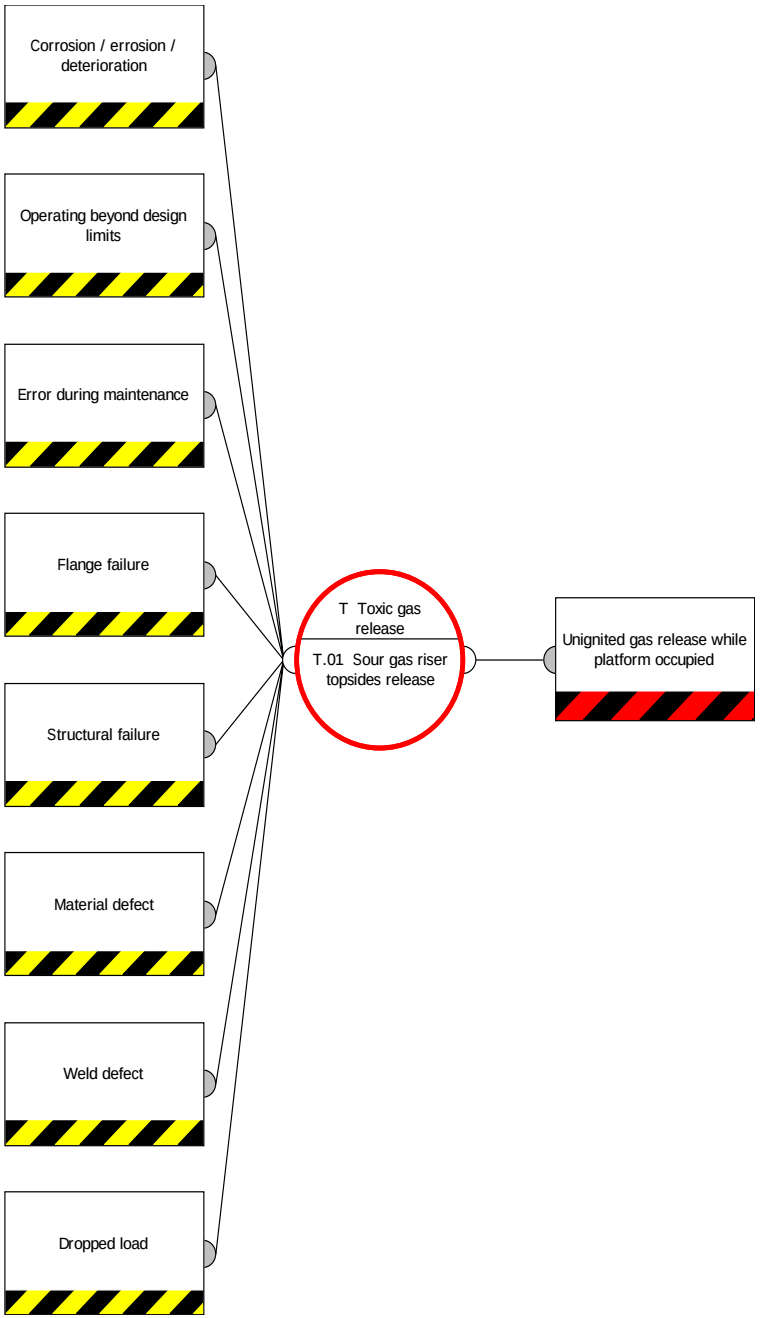

Electrical equipment specification
Fire & gas detection system
Alarm trips
Manual detection
ESD valve
SSIV
Manual blowdown
PA systems and alarms
Escape and evacuation from BP
Hazardous area classification
Fire
Operational (best practice) review
Insufficient competence
Procedural control
Inadequate communication
Commissioning review
Incorrect specification
Procedural review
Inadequate maintenance
H
Hydrocarbon
H.02 Gas riser splash-zone release
Personnel injuries due to fire or explosion
Fire explosion damage to assets
Unignited gas release to environment

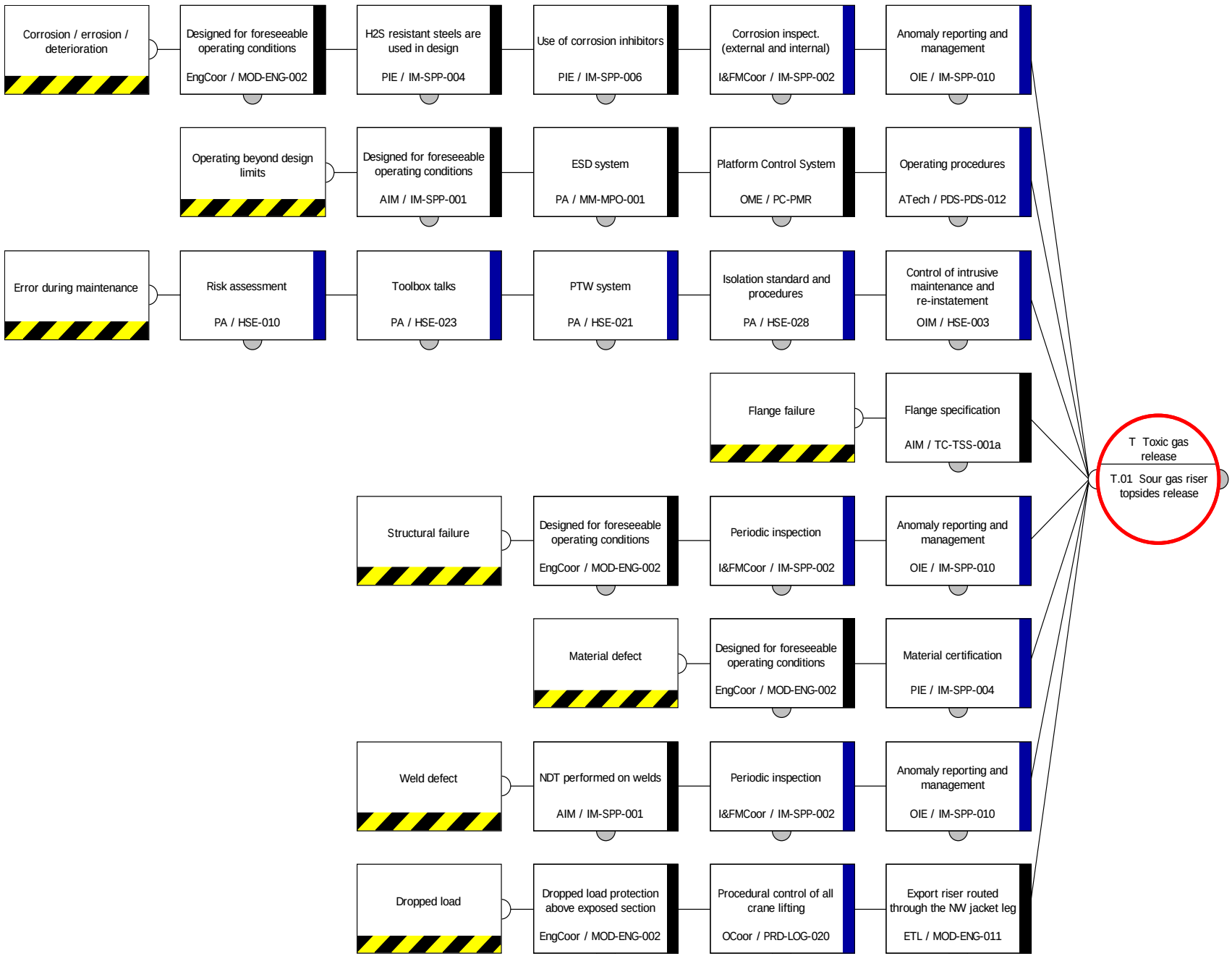

Faulty rigging
Faulty crane / component
Faulty sling
Human error
Lifting outside weather window
Supply boat motion exceeds the criteria
Inappropriate basket used
I Impacts and dropped
I.01 Lifting failure
Dropped object damage
Set down object unstable
Personnel injuries (supply boat)
Personnel injuries (platform)

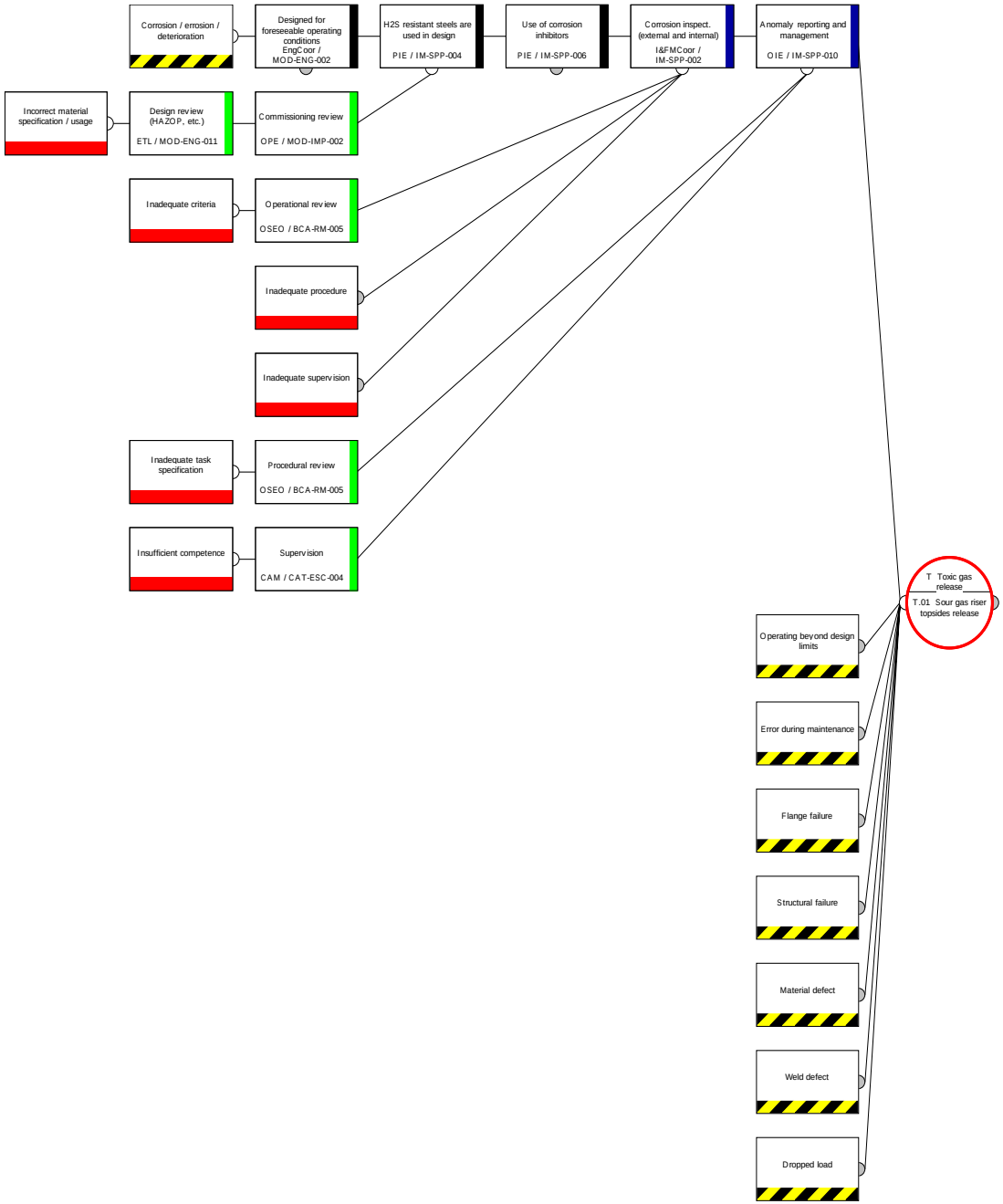

Faulty crane / component
Safety systems on crane (load ind., brakes)
Faulty rigging
Lifting Pre Risk Assessment Checklist
Competent personnel
Safety Practices Manual
Strict adherence to LOLER
Control of loose lifting equipment (Certex)
Adherence to wave/wind window
Colour coding of lifting equipment
Load testing
Risk Assessment
Lifting Pre Risk Assessment Checklist
Crane inspection and maintenance
Lifting plans
Strict adherence to LOLER
Control of fixed lifting equipment (Certex)
Adherence to wave/wind window
Colour coding of lifting equipment
Load testing
NDT testing where appropriate
Risk assessment
Faulty sling
Strict control of pre-slung goods onshore
Visual inspection as soon as the load is lifted off the deck
Competent Banksman
Human error
Competent personnel
Lifting Pre Risk Assessment Checklist
Lifting plans
Communication
Safety Practices Manual
Job Step Plans
Banksman actively monitors lifting operations
Adherence to wave/wind window
PTW system
Lifting outside weather window
Strict weather criteria for lifting
Lifting controlled by Banksman
OIM approves lifting
Supply boat motion exceeds the criteria
OIM refuses entry into 500m zone if weather not for lifting
Banksman enforces weather window constraints
Inappropriate basket used
Adherence to LOLER
Old type baskets colour red coded
I Impacts and dropped
I.01 Lifting failure

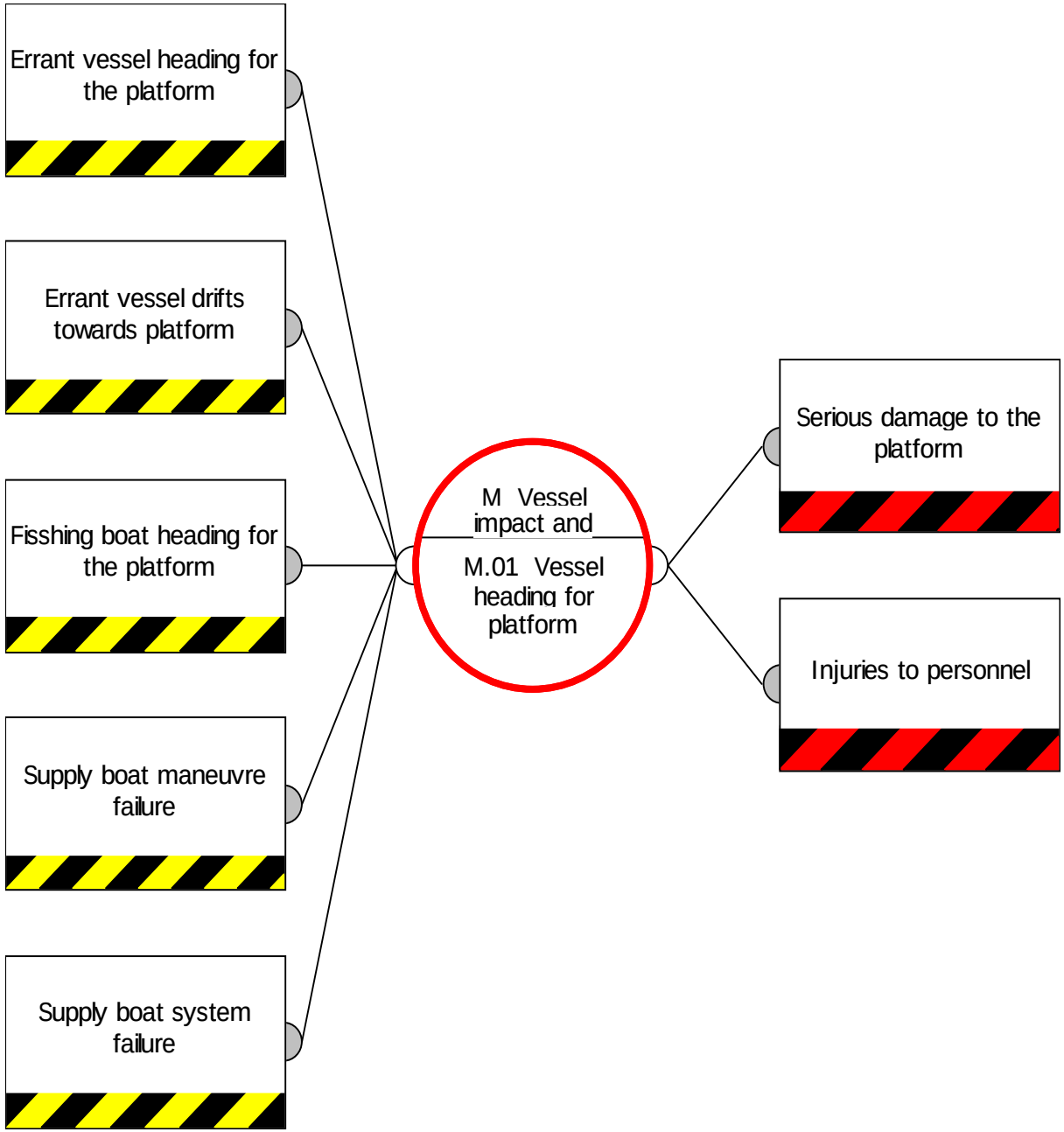

Faulty rigging
Lifting Pre Risk Assessment Checklist
Competent personnel
Safety Practices Manual
Strict adherence to LOLER
Control of loose lifting equipment (Certex)
Adherence to wave/wind window
Colour coding of lifting equipment
Load testing
Risk Assessment
Inadequate procedures
Competence assurance
Inadequate task specification
Procedural review
External pressure
Procedural control
Insufficient competence
Operational review
Supervision
Faulty crane / component
Faulty sling
Human error
Lifting outside weather window
Supply boat motion exceeds the criteria
Inappropriate basket used
I Impacts and dropped
I.01 Lifting failure

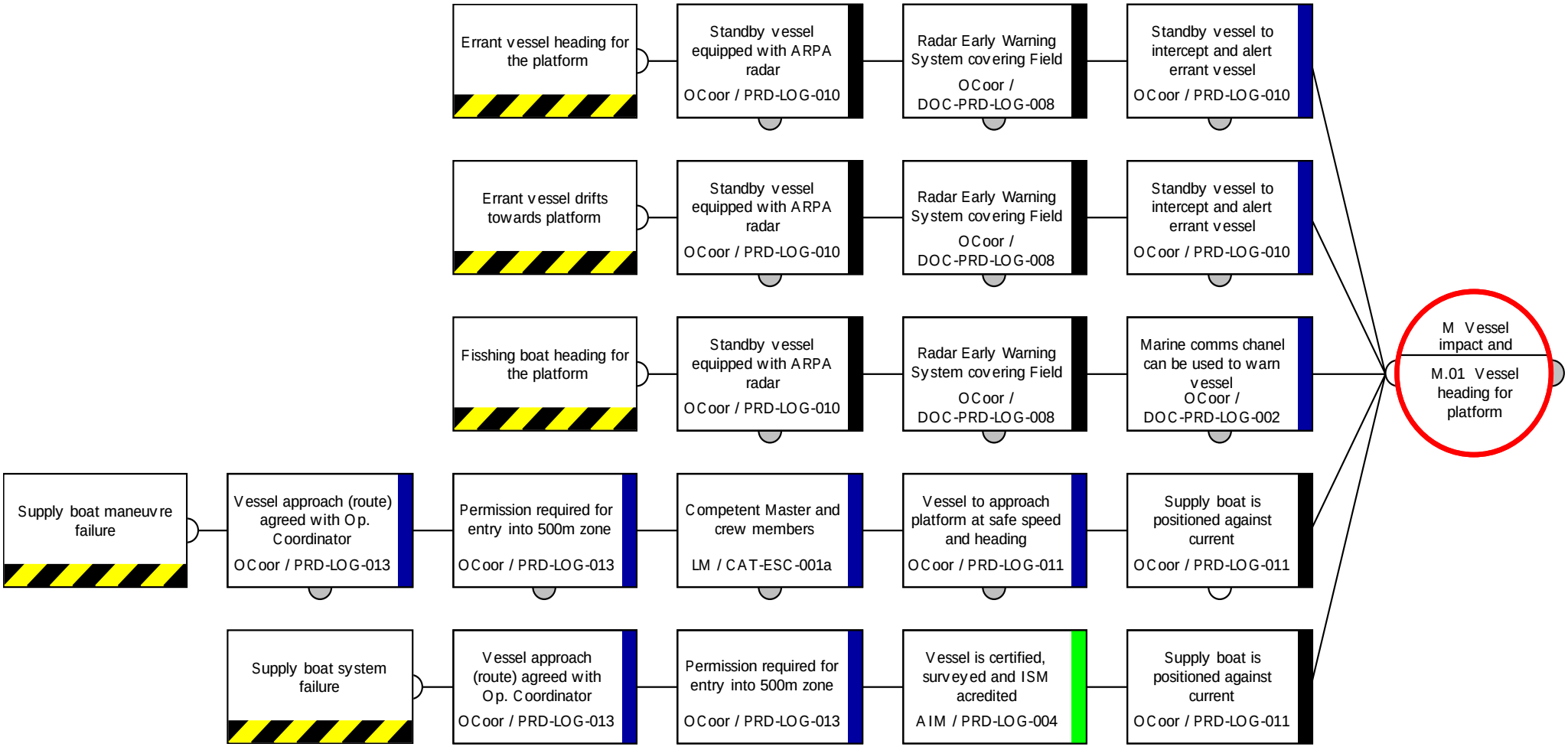

I Impacts and dropped
I.01 Lifting failure
Crane restrictions over process area
Fire & gas detection system
Manual detection
Alarm system
Emergency communication and response
Dropped object damage
Operational review
Insufficient competence
Procedural control
Inadequate communication
Golden rules for lifting and stacking
Fire & gas detection system
Manual detection
Alarm system
Emergency communication and response
Set down object unstable
Supervision
Operator error
Personnel injuries (supply boat)
Personnel injuries (platform)

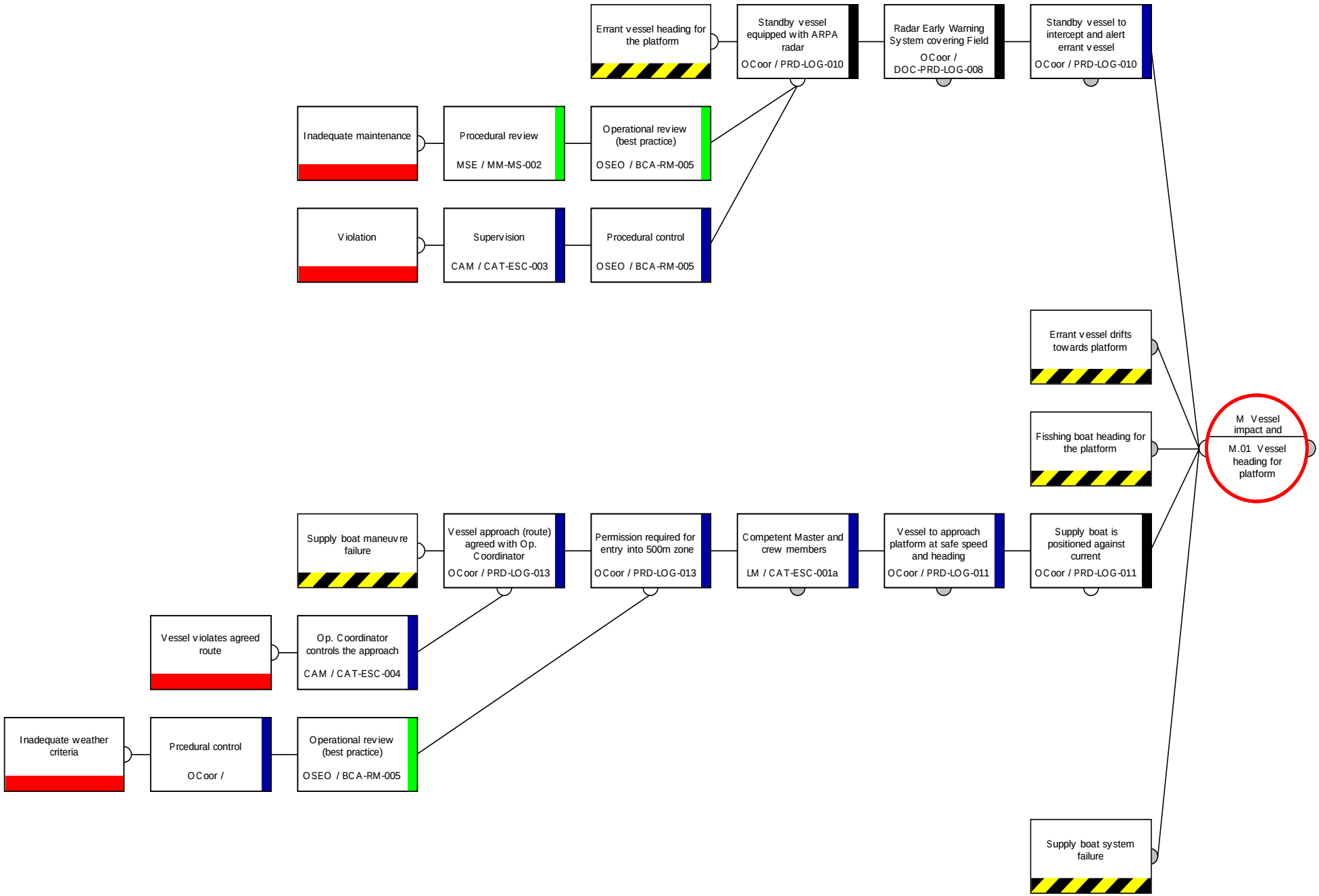

Corrosion / errosion / deterioration
Operating beyond design limits
Error during maintenance
Flange failure
Structural failure
Material defect
Weld defect
Dropped load
T Toxic gas release
T.01 Sour gas riser topsides release
Unignited gas release while platform occupied

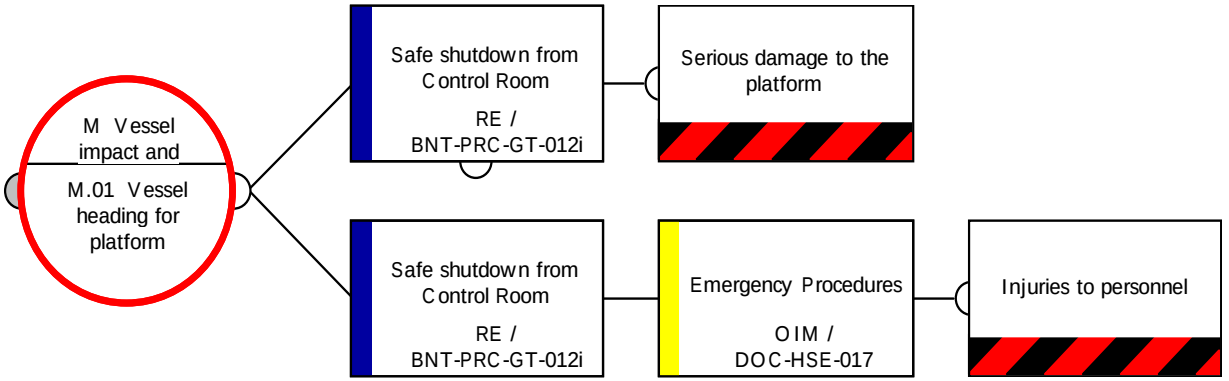

Corrosion / errosion / deterioration
Designed for foreseeable operating conditions
EngCoor / MOD-ENG-002
H2S resistant steels are used in design
PIE / IM-SPP-004
Use of corrosion inhibitors
PIE / IM-SPP-006
Corrosion inspect. (external and internal)
I&FMCoor / IM-SPP-002
Anomaly reporting and management
OIE / IM-SPP-010
Operating beyond design limits
Designed for foreseeable operating conditions
AIM / IM-SPP-001
ESD system
PA / MM-MPO-001
Platform Control System
OME / PC-PMR
Operating procedures
ATech / PDS-PDS-012
Error during maintenance
Risk assessment
PA / HSE-010
Toolbox talks
PA / HSE-023
PTW system
PA / HSE-021
Isolation standard and procedures
PA / HSE-028
Control of intrusive maintenance and re-instatement
OIM / HSE-003
Flange failure
Flange specification
AIM / TC-TSS-001a
Structural failure
Designed for foreseeable operating conditions
EngCoor / MOD-ENG-002
Periodic inspection
I&FMCoor / IM-SPP-002
Anomaly reporting and management
OIE / IM-SPP-010
Material defect
Designed for foreseeable operating conditions
EngCoor / MOD-ENG-002
Material certification
PIE / IM-SPP-004
Weld defect
NDT performed on welds
AIM / IM-SPP-001
Periodic inspection
I&FMCoor / IM-SPP-002
Anomaly reporting and management
OIE / IM-SPP-010
Dropped load
Dropped load protection above exposed section
EngCoor / MOD-ENG-002
Procedural control of all crane lifting
OCoor / PRD-LOG-020
Export riser routed through the NW jacket leg
ETL / MOD-ENG-011
T Toxic gas release
T.01 Sour gas riser topsides release


Corrosion / errosion / deterioration
Designed for foreseeable operating conditions
EngCoor / MOD-ENG-002
H2S resistant steels are used in design
PIE / IM-SPP-004
Use of corrosion inhibitors
PIE / IM-SPP-006
Corrosion inspect. (external and internal)
I&FMCoor / IM-SPP-002
Anomaly reporting and management
OIE / IM-SPP-010
Incorrect material specification / usage
Design review (HAZOP, etc.)
ETL / MOD-ENG-011
Commissioning review
OPE / MOD-IMP-002
Inadequate criteria
Operational review
OSEO / BCA-RM-005
Inadequate procedure
Inadequate supervision
Inadequate task specification
Procedural review
OSEO / BCA-RM-005
Insufficient competence
Supervision
CAM / CAT-ESC-004
T Toxic gas release
T.01 Sour gas riser topsides release
Operating bevond design limits
Error during maintenance
Flange failure
Structural failure
Material defect
Weld defect
Dropped load


Errant vessel heading for the platform
Errant vessel drifts towards platform
Fisshing boat heading for the platform
Supply boat maneuvre failure
Supply boat system failure
M Vessel impact and
M.01 Vessel heading for platform
Serious damage to the platform
Injuries to personnel


Errant vessel heading for the platform
Standby vessel equipped with ARPA radar
OCoor / PRD-LOG-010
Radar Early Warning System covering Field
OCoor / DOC-PRD-LOG-008
Standby vessel to intercept and alert errant vessel
OCoor / PRD-LOG-010
Errant vessel drifts towards platform
Standby vessel equipped with ARPA radar
OCoor / PRD-LOG-010
Radar Early Warning System covering Field
OCoor / DOC-PRD-LOG-008
Standby vessel to intercept and alert errant vessel
OCoor / PRD-LOG-010
Fisshing boat heading for the platform
Standby vessel equipped with ARPA radar
OCoor / PRD-LOG-010
Radar Early Warning System covering Field
OCoor / DOC-PRD-LOG-008
Marine comms chanel can be used to warn vessel
OCoor / DOC-PRD-LOG-002
M Vessel impact and
M.01 Vessel heading for platform
Supply boat maneuvre failure
Vessel approach (route) agreed with Op. Coordinator
OCoor / PRD-LOG-013
Permission required for entry into 500m zone
OCoor / PRD-LOG-013
Competent Master and crew members
LM / CAT-ESC-001a
Vessel to approach platform at safe speed and heading
OCoor / PRD-LOG-011
Supply boat is positioned against current
OCoor / PRD-LOG-011
Supply boat system failure
Vessel approach (route) agreed with Op. Coordinator
OCoor / PRD-LOG-013
Permission required for entry into 500m zone
OCoor / PRD-LOG-013
Vessel is certified, surveyed and ISM acredited
AIM / PRD-LOG-004
Supply boat is positioned against current
OCoor / PRD-LOG-011


Errant vessel heading for the platform
Standby vessel equipped with ARPA radar
OCoor / PRD-LOG-010
Radar Early Warning System covering Field
OCoor / DOC-PRD-LOG-008
Standby vessel to intercept and alert errant vessel
OCoor / PRD-LOG-010
Inadequate maintenance
Procedural review
MSE / MM-MS-002
Operational review (best practice)
OSEO / BCA-RM-005
Violation
Supervision
CAM / CAT-ESC-003
Procedural control
OSEO / BCA-RM-005
Errant vessel drifts towards platform
Fisshing boat heading for the platform
M Vessel impact and
M.01 Vessel heading for platform
Supply boat maneuvre failure
Vessel approach (route) agreed with Op. Coordinator
OCoor / PRD-LOG-013
Permission required for entry into 500m zone
OCoor / PRD-LOG-013
Competent Master and crew members
LM / CAT-ESC-001a
Vessel to approach platform at safe speed and heading
OCoor / PRD-LOG-011
Supply boat is positioned against current
OCoor / PRD-LOG-011
Vessel violates agreed route
Op. Coordinator controls the approach
CAM / CAT-ESC-004
Inadequate weather criteria
Prcedural control
OCoor /
Operational review (best practice)
OSEO / BCA-RM-005
Supply boat system failure


M Vessel impact and
M.01 Vessel heading for platform
Safe shutdown from Control Room
RE / BNT-PRC-GT-012i
Serious damage to the platform
Safe shutdown from Control Room
RE / BNT-PRC-GT-012i
Emergency Procedures
OIM / DOC-HSE-017
Injuries to personnel

APPENDIX C – CURRENT PRACTICE IN COMPETENCE ASSURANCE

INTRODUCTION

The majority of the operators have adopted the National Vocational Qualification (NVQ) system for their Competence Assurance. The NVQs typically comprise:

1. **National Occupational Standards** – Statements of performance that describe what people in a particular occupation are expected to be able to do. They cover current best practice, the ability to adapt to future requirements and the knowledge and understanding that underpins competent performance.
2. **Units of competence** – These describe a specific job function which can be performed by an individual in the workplace. A person consistently fulfilling the requirements of the unit can receive credit for this achievement. The unit defines the criteria for demonstrating competent performance and the knowledge which is essential for this function as well as the range of circumstances which apply. The unit is subdivided into elements of competence.
3. **Elements of competence** – Part of the Unit of Competence containing detailed description of the standard of performance expected (performance criteria).
4. **Performance criteria** - These are statements against which performance can be demonstrated and hence assessed. They are expressed in terms of outcome rather than the methods or procedures used and contain the minimum standard required, and which can be evaluated, for competent performance. The range of circumstances (e.g. equipment, procedures, processes, etc.) to which the criteria apply are also specified.
5. **Knowledge specification** – An outline of the knowledge, which is fundamental to support competent performance, is specified in the Units of Competence.
6. **Evidence requirement** – Descriptions of the evidence people must show to prove to an assessor that they are competent.

The NVQ has five levels of attainment, from foundation skills in occupation (level 1) to chartered, professional and senior management occupations (level 5). The levels of attainment in offshore practice vary from 3 to 4, for example,
Operator A is using three levels as follows:

1. Discipline staff – minimum **Level 3 NVQ** within the discipline
2. Supervisor – minimum **Level 4 NVQ**
3. Section leader (Assessor) – minimum **Level 3 or 4 NVQ**
4. Assessor – Level 4 or 5 NVQ

Operator B is using four levels as follows:

1. **Familiar** – basic knowledge of competence with limited practical experience and requiring guidance, advice and/or supervision
2. **Skilled** – adequate knowledge of competence and adequate practical experience in applying this knowledge and requiring some guidance, advice and/or supervision.
3. **Accomplished** – extensive knowledge of competence with significant practical experience in applying this knowledge and in a position to provide guidance in this field and regarded as accomplished in this field.
4. **Expert** – expert knowledge of competence with a comprehensive level of practical experience and achievements in the subject thereby having the ability to teach others in the subject.

TECHNICAL COMPETENCY PROFILE

Technical competence profile is developed for each installation and is based on the analysis of location specific production systems and component parts of those systems and the appropriate level of personnel training required to provide front line support. An operational training matrix is shown in Figure C.1.

Course Title	Supervisor	Mechanical	Electrician	Operator	Crane driver	Safety adviso
Wire Rope Change					M	
Scaffold Inspection						R
Permit to Work (Level 3)	M					M
Permit to Work (Level 1)		M	M	M		
Permit to Work (Level 2)					M	
Banksman/Slinger					M	
Banksman/Slinger Refresher					M	
High Voltage Switching			M			
Change Management	M					
COSHH Assessor						M
Crane Driving (Stage 1)					M	
Crane Driving (Stage 2)					M	
Crane Driving (Stage 2) Refresher					M	
Crane Driving (Stage 3 Assessment)					M	
Crane Driving (Stage 3 Assessment) Refresher					M	
Radiation Protection Supervisor						M
Flange Management - Hand Torquing		M		M		
Flange management - Tensioning & Hydraulic Torquing		M				
Flange Management - Assessor Accreditation		R				
Twin Ferrule Compression Fittings Refresher		M		M		
M = Mandatory R = Recommended						

Figure C.1 Specimen of operational training matrix (Incomplete)

It can be seen that the units of competence (and associated elements of competence) are job focused and not barrier focused. Therefore, the Mechanical Technician (Figure C.1) is aware of the Permit to Work (Level 1) and the Flange management – hand and tensioning and hydraulic torquing, but for example, may not be aware of the function of the equipment on the other side of the flange (see the accident description in Section 4.2). The purpose of the bow tie approach is to transfer such knowledge.

AREAS OF IMPROVEMENT

Some of the areas of improvement identified in the research on competence assessment for the hazardous industries (HSE, 2003) are listed here together with the comments related to the proposed bow tie approach which are given in bold italics:

1. The full scope of safety critical tasks, such as process upsets and shutdowns should be covered by competence assessment;
2. A wider application of risk assessment for the purpose of identifying and prioritising safety critical tasks for which competence needs to de assessed;
3. Ensuring that NVQ syllabus clearly denotes the major hazard consequences of tasks and the safety role of equipment and is tailored to the needs of the site;
4. Wider considerations of the potential for skills to decay or become outdated, and therefore the need to consider effective reassessment system for people carrying out safety related tasks, such as adopting "check and train" process for staff, perhaps linking this to existing schemes such as annual reviews.

REFERENCES

HSE (2003) *Competence assessment for the hazardous industries*, Prepared by Greenstreet Berman Ltd, Research Report 086.

HSE
Health and Safety Executive

Optimising hazard management by workforce engagement and supervision

Offshore oil and gas duty holders have recognised that a lack of skilled workforce, change to shorter working hours and increase in activity can lead to an erosion of health and safety unless balanced by significant increase in level of training and supervision. The way forward suggested in this report is based on:

a) improving comprehension of major hazards by the workforce; and

b) optimising the management processes such as balancing workforce competence and level of supervision.

By improving comprehension of major hazards the workforce itself can play a central role in safety case preparation by being involved in identifying real improvements in safety that are reasonable and based on the day-to-day grass-roots operational experience of various disciplines. Workforce involvement in optimising safety management processes not only increases the experience of the group of workers who can contribute to the process (contributory expertise), but also of other groups of workers who acquire interactional expertise. Safety optimisation can be applied to any process by challenging the existing situation along the lines ‘what more can we do’, or ‘how can we do it better’, etc. Evaluating complexity of protection systems is based on understanding the work that has to be done to maintain, control and operate protective systems, and the available competence.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

RR637

www.hse.gov.uk