

UNDERSTANDING MAJOR ACCIDENT HAZARDS – THE CUTTING EDGE OF COMMON SENSE

Graham Dalzell, BSc FI Mech E, Safety Consultant, Safety Analysis, BP Exploration & Production Ltd, Dyce and Stuart Ditchburn, CEng BSc M Inst MC, Principal Consultant, Det Norske Veritas Limited, Aberdeen.

INTRODUCTION

During the last decade, hazard identification, risk assessment and management has become a universally used tool in the offshore and petrochemical industries. Huge improvements have been made in the way that these industries now manage their business, leading thankfully to a greatly reduced likelihood of a Major Accident. But the process has now matured to the point where it is doubtful that it is capable of delivering much more in terms of added value.

Whilst it is certainly true that the introduction of a suite of goal setting regulations has help drive this vast improvement in hazard management, it is also the case that it has led to an unwelcome side effect. The detailed hazard evaluation and risk analysis now required by regulation, has necessitated the extensive use of risk analysts, invariably provided by consulting organisations. The level of detail demanded by the regulations has also led to an enormous amount of 'hazard information' being required supporting the Safety Cases and Safety Reports

Thus we have a situation where valuable hazard management information is often 'locked up' in the Safety Case, Safety Report and associated studies. Also, all the 'hazard understanding' is most likely in the hands and minds of the specialist risk analyst, who do not usually play an active part in the day to day operations where risk is most effectively managed

So the search is on to find new ideas or refinements of the process which can be used to 'ratchet up' the value gained in terms of tangible and worthwhile risk reduction. Unsurprisingly, cost is a significant factor in determining which new ideas and alternative approaches are viable; so cost effective methods are liable to be taken up more readily.

This Paper proposes one solution in the form of an integrated Major Accident Hazard Management System (MAHMS), which is currently being developed and implemented on bp Trinidad & Tobago's oil and gas operations in the Caribbean.

CONTENTS

A SOLUTION
Understanding Major Accident Hazard Management – a Common Sense Approach

- Wholistic Approach to Risk Management
- Managing all Levels of Risk as a Continuum
- Pragmatic and Qualitative Approach
- Critical Measures (People, Processes & Plant)
- Major Accident Hazard Understanding
- Major Accident Hazard Information

THE PROBLEM: HAZARD UNDERSTANDING – IN THE HANDS OF THE SPECIALISTS

Under the UK's present 'Goal Setting Regulations' there is a compelling need for duty holders to demonstrate in their installation Safety Case that they have:-

- Identified all the hazards involved in their undertaking which may pose risks to personnel
- Evaluated the risks arising from those hazards
- Identified and put in place the means to manage the hazards and reduce the risks
- Made a demonstration that those risks are as low as reasonably practicable

These tasks necessitate an analysis in some considerable detail, often of a quantitative nature. Most duty holders engage specialist consultants to perform the analysis, using Quantitative Risk Analysis (QRA) techniques. Often, the same risk analysts conduct the numerous supporting studies required to identify the hazards, determine the characteristics of the risks arising from the hazards and recommend measures required to reduce the risks to as low as reasonably practicable (ALARP). The risk analysis concentrates purely on risks to personnel as required by the regulations. Risk to the environment or production in terms of business interruption, are largely ignored. Some operators use specialist risk consultant to provide a service covering the ongoing management of the Safety Case and the associated risk analysis and risk management activities that are entailed.

Before going further we must emphasise that we are not advocating an end to the above approach. Specialist risk analysts have and continue to deliver exceptional service in this area, where not even the largest operators have much, if any, 'in-house' expertise. Indeed it would be difficult to perceive how duty holders would be successful at achieving the goals of the Safety Case Regulations without such specialist assistance. This is a process that will need to continue for the foreseeable future in the UK Sector at least.

However, the above situation has introduced an unwelcome side effect, which has four symptoms:-

(i) The Safety Case 'customer' tends to be viewed as the Regulatory Body (HSE), rather than the 'workforce' which we believe was the spirit if not the intent of Lord Cullen's Recommendations;

(ii) All the ‘hazard understanding’ is in the hands and minds of the specialist risk analyst, who do not usually play an active part in the day to day operations where risk is most effectively managed;
(iii) There is a major disconnect between the management of occupational health and safety risks and the management of major accident hazard risks, the latter often been relinquished to the specialists; and
(iv) Environmental risks and risks to business interruption, if considered at all are not being managed wholistically and with the same rigour as safety risks to personnel.

So what are the effects of the above symptoms and how are they detracting from the effectiveness of risk management on the facility?

SAFETY CASE CUSTOMER

A notion that the Safety Case was written for the HSE, is quite widespread throughout the workforce. This means that there is a great deal of apathy towards the Safety Case process, both in terms of its preparation, maintenance and the usefulness of the information it contains. This is most acute in those lower levels of the workforce, who paradoxically are perhaps those personnel at the greatest risk.

Those who do make a point of consulting the facility Safety Case, more often than not find that:-

- the information it contains is difficult to interpret and understand,
- the risk information is couched in terms and values which are almost impossible to appreciate; and
- the information is of little practical use in their daily activity.

If net result is to produce a Safety Case with the primary aim of satisfying the regulatory requirements, it may be of very little use in the day to day management of risk at any level.

ACCESS TO HAZARD INFORMATION

Those personnel in the duty holders organisation who are responsible for managing risk, invariably do not have the information or knowledge that they require to discharge their responsibilities effectively. This information, which we are calling ‘hazard understanding’, is more than likely available somewhere but is often ‘locked-up’ in the mass of documents and specialist studies which support the Safety Case.

Even when the relevant information is found, it is not usually presented in a form that is readily appreciated or re-usable directly. To achieve this often requires the safety specialist/risk analyst to interpret the information they have to hand to reproduce it in a useable form. This takes time and because the specialists are not part of the operations team, the information is not readily available when required. There is also a risk that if the risk analyst is not familiar with the day to day operations, that his/her interpretation of the data is inappropriate. Information is therefore often supplied either too late or in an inappropriate form to be of effective use.

RELINQUISHMENT OF MAJOR ACCIDENT HAZARD RISK MANAGEMENT RESPONSIBILITY

The management of occupational health and safety has latterly been much improved and continues to improve throughout the industry. However, there is a serious disconnect between the management of occupational safety, health and indeed environmental risk management and the management of major accident hazard risks. Most line management tend to assume that the responsibility for the latter is that of the risk management specialists and not part of their role.

It is also the case that causes of major accidents could originate as occupational safety related incidents, because the barriers designed to prevent incidents or limit escalation are ineffective. This is often due to them being inhibited as part of the work being carried out, without any consideration of what other temporary measures could be put in place to provide equivalent protection.

This situation is of great concern. Firstly, it raises a doubt that major accident hazard management is being performed with the same rigour as that for occupational safety. Secondly, the obvious benefits of addressing the management of occupational and major accident hazard risk as a continuum are not being realised.

INCOHERENT RISK MANAGEMENT

Major Accident Hazards (MAH), put personnel, production, capital investment and corporate reputations at risk. In most cases, they also pose a threat of environmental damage. Figure 1, below illustrates the way risks are related. It also shows the links that should exist between the management systems although they are often independent.

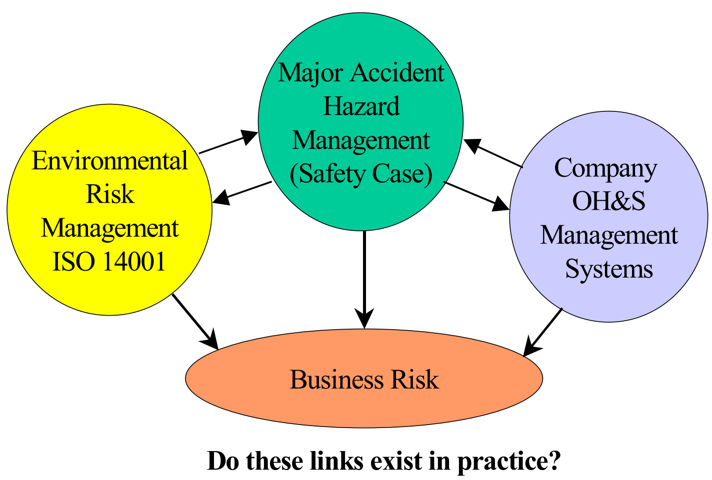

Figure 1. (In)Coherent risk management

It seems sensible and convenient therefore to consider all three types of risk together, yet this rarely happens. This appears to be due to the fact that the legislative drive is purely on safety risks to personnel. Most organisations however regard preventing environmental damage as having equal importance with safety. Also, although not stated, it is implicit that any operator will also rank production as having high importance, often equal with safety and protecting the environment. We should not be reticent to accept this fact as the basic function of an operators' business, nor feel we are in any way reducing the importance of safety by doing so. If the business is successful, then there is more likely to be more resources devoted to safety and environmental risk management.

In summary, whilst a Safety Case represents a sizeable investment, the situation discussed above prevents duty holders from maximising its value.

A SOLUTION: UNDERSTANDING MAJOR ACCIDENT HAZARD MANAGEMENT – A COMMON SENSE APPROACH

The following proposal describes how one Operator intends to overcome the difficulties discussed above by adopting a common sense approach called Major Accident Hazard Management System (MAHMS).

MAHMS is currently being developed and implemented for the Operators offshore and onshore oil and gas operating assets in Trinidad & Tobago. Although this is an operating environment where there is as yet very little regulation, we believe the principles employed are equally viable in a tightly regulated operating area like the North Sea. These principles of MAHMS are that it:-

- Adopts a wholistic approach to risk management, dealing with safety, environment and business interruption risk in one integrated system, considering the complete lifecycle of the operation.
- Manages all levels of risk, from occupational health & safety to major accident hazards, as a continuum, on a day-to-day basis and with the same rigour.
- Adopts a pragmatic and largely qualitative approach to risk assessment and management, only resorting to detailed quantitative analysis where it is not obvious that critical measures have reduced residual risks to ALARP.
- Recognises that measures in place to manage safety, environment or business risks, can be categorised as people, processes or plant; each of which have a performance standard to state functionality, performance and survivability expectations.
- Provides information on major accident hazards, sufficient to impart an understanding about the characteristics of the hazards or Major Accident Hazard Events to all levels of the workforce; thus enabling everyone to understand their role in MAHMS and carry it out effectively.
- Makes MAHM information continuously available in a form that can be readily understood and used in every day management of risks.

The above principles should be embedded into the key business management processes such that they become a fully integrated part of the management system. This is illustrated in the MAHMS Process Map, Figure 2.

What follows is a more detailed description of how each of these elements is intended to work in practice.

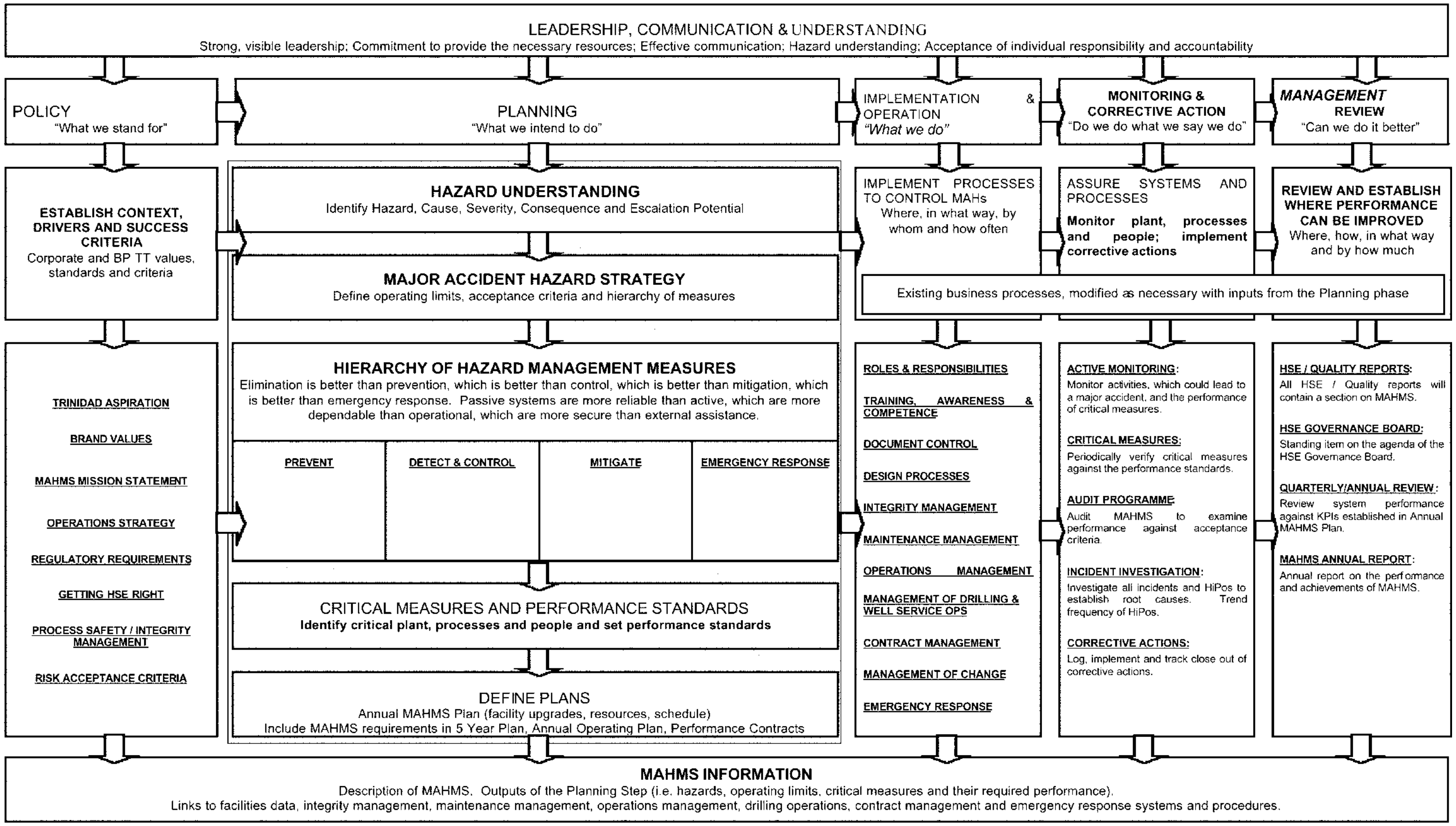

Figure 2. MAHMS process map

Revision 2: Dated 2nd November 2001

THE WHOLISTIC APPROACH TO RISK MANAGEMENT

Major Accident Hazard Management (MAHM) is a wholistic, structured approach to minimising the likelihood and reducing the consequences of a Major Accident Event, throughout the lifecycle of the operation. Here the lifecycle includes concept selection, detail design, construction, installation, hook-up, commissioning, operation, modification, de-commissioning and abandonment. This is shown in Figure 3, below:-

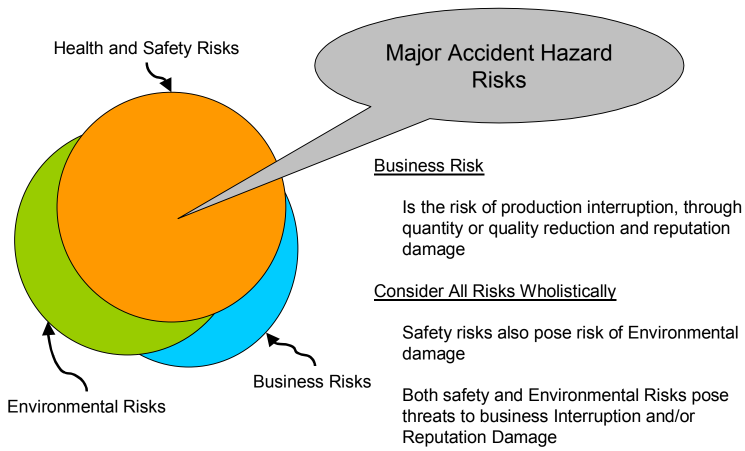

Figure 3. Wholistic risk management

Increasingly, there is a move towards voluntarily considering and managing risks of environmental damage through emissions or accidental spillage. This is largely as a result of societal pressure to do so, a realisation amongst employees that it is the right thing to do and Operators recognising that they should be adopting an environmentally responsible attitude when conducting their operations.

A business needs to be successful in order to thrive. A successful business generates revenue, some of which can be invested back into operations to support amongst other things, the wholistic management of risk. Where investment monies are limited, the activities that have the best financial justifications are more successful at securing funding. Although accepted as a high priority, spending on safety and environmental risk management alone has very often to vie with many other demands on a limited operating (OpEx) budget. Spending on safety and environmental protection measures does not normally show a tangible financial payback. Combining business risk management with safety and environmental risk makes good business sense and effective use of limited resources, providing a more robust business justification for allocation of monies.

MAHMS is unashamed and blatant at taking this approach to securing its funding.

MAHMS also considers risk management throughout the lifecycle of the operation. For a new facility this means eliminating hazards or reducing the likelihood of major accident hazard events by:-

- Ensuring concept selection evaluates options to reduce risks to personnel, the environment and business interruption; for example:-
  - Adopting Normally Unattended Installation designs wherever possible.
  - Maximising spatial separation of the process plant, control rooms and accommodation by adopting bridge-linked multiple jacket designs
  - Building-in robust integrity management features and arrangements
- Taking full advantage of the opportunity to achieve an inherently safe design by incorporating as many measures to avoid or prevent the hazards as possible
- Adopt a layout of the facility, plant and hazardous areas, which minimises the effects and escalation potential during a major accident hazard event.

For an existing facility this means reducing the consequences of a major accident hazard event by:-

- Selecting critical measures which control and mitigate the effects of the event effectively whilst minimising the cost and difficulty of installing the measures or modifying plant.
- Reduce safety risks by segregating people from the hazardous operations or areas
- Placing a greater emphasis on the effectiveness of emergency response measures to protect people and the environment from the worst effects of a major accident hazard event, and ensure that personnel can muster, evacuate or escape and be rescued and recovered safely.

MAHMS adopts a hierarchy of measures, placing emphasis on avoiding and preventing MAH events.

MANAGING ALL LEVELS OF RISK AS A CONTINUUM

MAHMS utilises the variety of sound workplace risk assessment tools employed and extends their use beyond occupational safety and health risk management, into the realm of major accident hazard prevention. The basic tools and techniques are the same regardless of the hazards being managed. Figure 4 shows how risks can be regarded as a continuum.

MAHMS achieves this by providing the information to impart a thorough understanding about the causes of major accident hazards, and then coaching users of workplace risk assessment tools to use the information to assess:-

- Whether the work being planned could initiate a major accident hazard event
- In what ways could the work being planned go wrong to cause or threaten to cause a major accident hazard event
- Whether the work will disable or interfere with any critical measures designed to prevent, control, mitigate or provide emergency response to major accident hazard events; and if so what additional temporary measures will be required to provide equivalent protection.

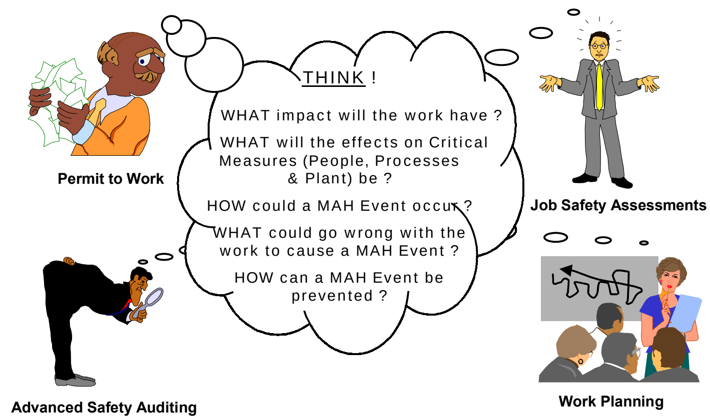

Figure 4. Risk management as a continuum

Some tools in common use where the above process can be applied are:-

Table 1. Common workplace risk analysis tools

Tools	Methodology
Job Safety Analysis	• Provide Hazard information to impart MAH Understanding • Provide guide-words and checklists of Facility MAH to ensure all potential MAH events are covered • Provide checklists to ensure all critical measures for each MAH are considered
Combined Operations or SIMOPS HAZOP	• Ensure a MAHMS specialist attends HAZOP Meeting • Ensure all potential work conflicts are considered • Develop a Combined Ops/SIMOPS Matrix to provide guidance on allowable simultaneous operations
Advanced Safety Auditing	• Provide Hazard information to impart MAH Understanding • Engage in on-the-job conversations about job planning and risk assessment • Extend the conversations to cover MAH avoidance and prevention considerations

PRAGMATIC & QUALITATIVE APPROACH

One thing must be borne in mind in the pursuit of perfection in terms of risk assessment and management, that is the resources (operators' personnel, professional assistance and funding for critical measures) is and always will be finite.

This means we must be ***realistic*** in what can be achieved, whilst at the same time having a goal in mind which will achieve levels of acceptable risk. The MAHMS approach is to ***evaluate risk, primarily in a qualitative*** way where it is obvious that risk are being adequately managed and only resort to ***detailed quantitative risk analysis*** to show how the levels of risk compare with the Operators' Risk Acceptance Criteria.

Risk assessment is the evaluation of the likelihood and consequence and the judgement of its acceptability. It should be applied to evaluate the risks to individuals, the environment and business interruption arising from each hazard, and to the cumulative risk on each asset/facility both individually and its contribution to the business unit as a whole. Work is also necessary to demonstrate compliance with the Operators' Risk Acceptability Criteria.

Where the initial assessment determines that further risk reduction is required, it should follow the standard hierarchy of risk reduction measures shown in Figure 5, below.

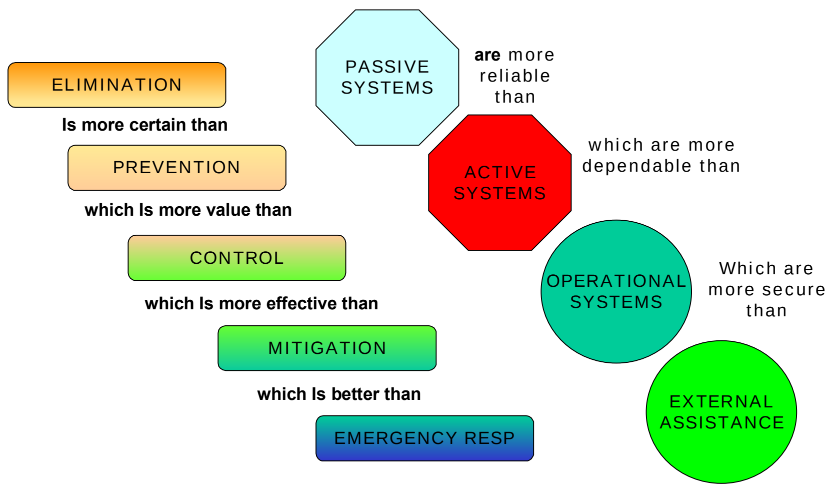

Figure 5. Hierarchy of risk reduction measures

Qualitative Risk Assessment

This is the use of informed judgement of an experienced group of people to assess the tolerability of risks and the adequacy of measures to prevent or control them. It is essential that this team has an adequate understanding of the cause and consequence, rather than applying guesswork and perception. The group should include people who have operating experience and the eventual responsibility for managing these risks.

Hazard/Risk matrices are the preferred qualitative documentation tool shown in Figure 10. These should be appropriate for major accident hazards and calibrated to align with corporate risk criteria when used for an overall assessment.

Quantitative Risk Assessment

This is the numerical quantification of the totality of risks to life on a facility. It may calculate both individual and societal risk and be used to determine if further investment to reduce risks is warranted. It should integrate all of the information about the hazards and their potential for escalation to a major accident to deliver both the overall risk figures and a picture of the spread of those risks.

The input data to quantitative analysis should be based on realistic likelihood of initiating events taking into account both historical data, actual site conditions, and an assessment of the long term effectiveness of proposed prevention measures. The likelihood and severity of the consequences should take full account of the realistic performance and reliability of the critical measures to eliminate, prevent, control, mitigate and provide emergency response.

Risk Assessment Methodology

For the above approach to work, we need some means of making a qualitative assessment of the risks (safety, environmental and business risk), which can also link qualitative levels of risk to quantitative risk figures if required.

The following methodology describes one possible approach. This methodology is for rapidly ranking the major accident hazard (MAH) on onshore and offshore facilities, and has been adapted for use on the Major Accident Hazard Management System (MAHMS) for Trinidad.

The methodology is used where a multi-discipline team of operations, technical and specialists in hazard assessment carry out Major Accident Hazard Identification (MAHID) for each asset/facility, identifying the principal major accident hazards. In some cases, it may be better if these are grouped so that all hazards in one area could be considered together, e.g. a cellar deck.

Using the experience of the group and specific knowledge of the arrangements, manning and condition of the facilities, the likelihood and safety, environment and business consequence can be assessed and qualitatively ranked according to tables 2 to 5, given below. The risk ranking is the event likelihood and the highest of the safety, environmental or business consequence categories.

These rankings can be assigned a quantitative 'score' according to values given in the risk-ranking matrix. These scores for all the MAHs, can then be added to give an overall risk picture for the facility, denoting the contribution from each MAH. Note that the scoring system is exponential; i.e. the method recognises that one increment of frequency represents a factor of 10 and similarly, one increment of consequence is also a factor of 10. As a result, a risk ranked as "C III" has 100 times the relative risk level of a "B II"

It should be noted that this methodology only provides relative risk-rankings. To achieve numerical risk values, these scores must be 'calibrated' against a detailed quantitative risk analysis. Until this is done, they must not be cross-related to any specific assessment of risk, such as individual risk, probability of any given event, or other established numerical criteria.

Using this approach allows the summation of all of the results from each of the hazards on one facility to give an overall figure that may be compared with the others hazards of facilities.

Example

On a three jacket installation, the following hazards were identified, ranked and scored:

- Gas riser release with escalation to adjacent high-pressure risers which could then affect the accommodation; Ranking B III; Score 10^{-7}.
- Fuel gas leakage at the generators under the accommodation exploding within the engine enclosure but not affecting other areas; Ranking C II; Score 10^{-7}.
- Gas leakage from compressors ingested into and exploding within a local control room with four occupants; Ranking D III; Score 10^{-5}.
- Manifold oil fire in a cellar deck with smoke affecting the top deck and bridge escape route to other jackets; Ranking C II; Score 10^{-7}.
- Separator fire engulfing the accommodation in smoke; Ranking C III; Score 10^{-6}.
- Gas leak and explosion in the cellar deck damaging the riser ESD valves and allowing simultaneous release through the manifolds; Ranking B IV; Score 10^{-6}.

Overall Score; $10^{-7} + 10^{-7} + 10^{-5} + 10^{-7} + 10^{-6} + 10^{-6} = \underline{1.23 \times 10^{-5}}$

Table 2. Likelihood category

Category	Description
E	Incident happens several times per year in BP Indonesia/Likely to continue to occur
D	Incident occurs several times per year in BP/Incident may occur in BP Indonesia at some time
C	Incident has occurred in BP/Incident unlikely to occur in BP Indonesia
B	Incident has occurred in major accident hazard industries (e.g. oil and gas, petrochemical, chemical)/Incident very unlikely to occur in BP Indonesia
A	Never heard of in the world

Table 3. Consequence category (Safety)

Signifies a Major Accident Hazard

Category	Description
V	Potential for more than 30 fatalities (e.g. potential loss of entire drilling rig or large installation with immediate fatalities and survivors having to escape to sea in an uncontrolled manner)
IV	Potential for between 10 and 30 fatalities (e.g. an event on a drilling rig or large installation with immediate fatalities and which may require controlled evacuation or a helicopter ditching with loss of all onboard)
III	Potential for between 2 and 10 fatalities (e.g. an event that does not escalate with the potential for immediate fatalities only or loss of an entire satellite crew)
II	Potential for a single fatality or serious injury
I	Potential for first aid or medical treatment only, possible lost time injury

Table 4. Consequence category (Environment)

Category	Environmental description	Socio-economic description
V	Potential to change ecosystem or activity leading to long term (+10 years) damage and poor potential for recovery to a normal state (e.g. significant damage to a fragile ecosystem)	Potential for long term loss or change to users or public finance (e.g. long term impact on fishing or tourist industry)
IV	Potential to change ecosystem or activity leading to medium term (+2 years) damage but with likelihood of recovery within 10 years	Potential to cause financial loss to other users or the public (e.g. cause a temporary suspension of fishing in the area)
III	Potential to change ecosystem or activity in a localised area for a short time, with good recovery potential. Similar scale of effect to existing variability	Potential to cause a nuisance to other users or the public
II	Change which is within scope of existing variability but can be monitored and/or noticed	Potential to affect behaviour but not a nuisance to other users or the public
I	Negligible effect (unlikely to be noticed or measurable against background activities)	Negligible effect

Table 5. Consequence category (Business)

Category	Description
V	Potential for major cost or revenue impact across the whole of the Indonesia and/or loss of reputation impacting on future viability of BP's Indonesia operations. (e.g. major contract violation, impact on Indonesia gas supplies for thirty or more days) **Total Company Losses >$US 1billion**
IV	Potential for major cost or revenue impact to BP Indonesia (e.g. contract violation, impact on Indonesia gas supplies for more than 3days or significant loss of oil production for prolonged period) **Total Company Losses $US 100M – $US 1billion**
III	Potential for major cost or revenue impact on Performance Unit (e.g. contract violation, impact on Indonesia gas supplies for less than 3 days or significant loss of oil production for a period of days/weeks) **Total Company Losses $US 10M – $US 100M**
II	Potential for minor cost or revenue impact
I	Negligible cost or revenue impact

Consequence						
	V	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}
	IV	10^{-7}	10^{-6}	10^{-5}	10^{-4}	10^{-3}
	III	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}
	II	10^{-9}	10^{-8}	10^{-7}	10^{-6}	10^{-5}
	I	10^{-10}	10^{-9}	10^{-8}	10^{-7}	10^{-6}
		A	B	C	D	E
		Likelihood				

Figure 6. Hazard risk-ranking matrix

Note that when assessing consequences, likelihood and corresponding risk level, credit should be taken for passive safeguards, e.g. the layout of the facility, drains and bunds, passive fire protection, escape routes, etc.

The three colours in the matrices are the classic gradings; red; unacceptable and must be improved; yellow; significant risk and risk reduction measures must be evaluated and implemented if reasonably practicable; and green, risks are low but existing management systems must be maintained. The scoring is simply a means of describing the relative risk according to the position in the matrix. The authors acknowledge the contribution of Chris Rawlings for the concept of an exponential scoring system.

Major Accident Hazard Definition (for bpTT)
An accidental event that has the potential to lead to:

- the death of 2 or more people
- long term or widespread damage to the environment (>2 years)
- major costs or loss of revenue (>$US 10 M)

Having determined the likelihood and safety, environmental and business interruption consequences of each hazard in the Hazard/Risk Matrices, the hazard management strategy can be formulated.

CRITICAL MEASURES (PEOPLE, PROCESSES & PLANT)
The Design and Construction Regulations, DCR, within the UK Goal Setting Regulations require that items of plant that are Safety Critical are identified with a view to their performance being subject to regular maintenance, testing and assurance, which we know as 'verification'.

The above requirement detracts from the possibility that safety critical measures could also be people; in that the roles they play in an emergency for example, are crucial to the effectiveness of muster, evacuation or escape rescue and recovery. It also neglects the possibility that certain processes could be safety critical; for example corrosion monitoring and control is a management process which is often crucial to maintaining integrity of the pressure envelope.

Since MAHMS also takes a wholistic view on risk, the notion that measures are only safety critical no longer applies. MAHMS therefore refers to ***critical measures*** as being the ***people, processes or plant*** which eliminate, prevent, control, mitigate or provide the arrangements for muster, evacuation or escape and the facilities for rescue & recovery. These critical measures may also provide a role in either reducing the likelihood and/or the safety, environmental or business consequences of a major accident hazard event.

Within reason the bigger the range and depth of measures the better, since this provides strength in depth in terms of preventative or control barriers. Prevention or control of a major accident hazard event, should not normally rely on only one barrier and should never rely solely on either a people or process critical measure, since both these measures are highly vulnerable to human factors effects.

In order to determine priorities, for repair, maintenance, testing and other assurance processes; it may sometimes be necessary to identify the relative importance of a range of critical measures. The following provides some guidance on how this may be achieved.

Not all critical measures have the same criticality (importance). One common system should be used to determine the relative importance of widely different systems relying on competencies (people), providing hydrocarbon containment assurance (processes) or physical safety systems (plant).

There are numerous factors that dictate the importance of critical measures. These are:-

- **Their relative positions in the hierarchy of measures (eliminate, prevent, control, mitigate or provide emergency response).**
- **Whether the measure is passive or active; automatic or manual**
- **Whether there are human factors dimensions and potential for human error**
- **The required levels of availability and reliability (performance specification)**
- **Whether there is duplication or redundancy**
- **Whether the measure is an emergency response measure crucial to effect successful muster, evacuation, escape, rescue or recovery.**
- **Whether failure of the critical measure would initiate a major accident hazard event**
- **The extent to which the measure is reliant on or interacts with other measures**
- **The critical measures vulnerability to the effects of a MAH event.**
- **Whether the critical measure is providing the only barrier, which prevents a MAH event. (This situation should normally be avoided by design).**

The criticality of any given measure therefore depends upon the above factors. The diagram of Figure 7 below, illustrates this:-

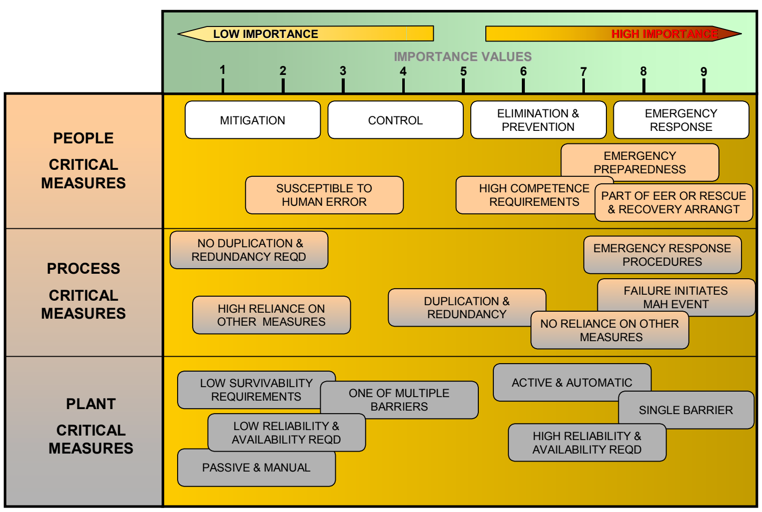

Figure 7. Importance of critical measures

The importance of any given critical measure can be determined by a summation of points values of all the factors which apply to that measure. Doing this for all critical measures, will provide a relative importance ranking and hence form the basis for prioritising effort and resources to install, maintain, repair, test and examine them.

CRITICAL MEASURE PERFORMANCE STANDARDS

A Performance Standard is a clear unambiguous statement of what a critical measure is required to do, in terms of its performance parameters. The critical measure performance parameters are defined for people, process and plant measures as shown in Figure 8, below:-

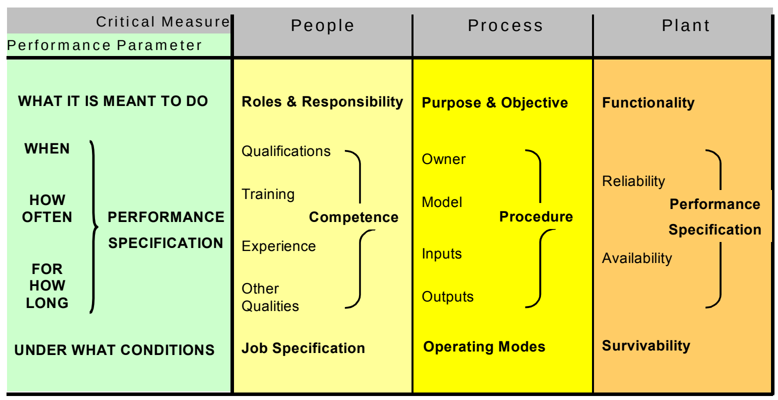

Figure 8. Critical measure performance parameters

What the measure is required to do, and not what it actually does, is defined by the ***functionality*** of the measure. This should be a very simple statement giving a clear unambiguous definition of what the measure is for. This will be the role in the case of a people critical measure, the purpose in the case of a process or the function in the case of a plant critical measure. The functionality statement should not go into details about how the role, purpose or function of the critical measure is achieved.

How the critical measure is required to perform, how long and how often it will be required to do it, is described in the ***performance specification*** part of the performance standard.

It may be for example that a crucial role in emergency response will be performed in isolation (eg Lifeboat Coxswain) or as part of a team (eg. a member of a fire-fighting team). How long the role is to be performed could be determined in terms of the expected duration of events, or the physical limits of an individual to remain on duty. These latter factors will help determine how many personnel should be trained and in place to take on such crucial roles. Finally, the performance specification will stipulate when (how often) those able to conduct the roles should be available to do it. For most emergency response roles this will be continuous (ie. 24 hours per day, 7 days per week). Where this is the case, then this dictates that a crew manning a facility will need to have as a minimum the crucial roles covered at all times.

Similarly for plant critical measures, where a measure is required to be continuously available (eg a life boat), and this cannot be achieved because of the need to maintain and service that measure, then there is a need for duplication and redundancy. This could also apply to a process critical measure (eg crane driver competence assurance), which is only continuously available so long as only competent crane drivers are allowed to operate the cranes.

Lastly, the performance standard defines under what conditions the critical measure is required to continue performing, and for how long; in other words its ***survivability***. This is particularly relevant to plant critical measures. For example, an emergency shut-down valve and actuator will be required to survive the effects of explosions and fires for long enough for the valve to close; and once closed remain able to effect a seal in a fire.

Once a Performance Standard has been written to unambiguously define all the factors discussed above, it provides the unequivocal benchmark against which the performance assurance activities can be judged. If at any time a critical measure is found to be failing to meet its performance standard, then action needs to be taken to rectify the problem and put such temporary arrangements or limitations in place until the measure is satisfactory.

It may be that in the light of more information or operating experience, that the performance standard requirements are found to be either more onerous than required or not good enough. In this case, the performance standard can be revised, approved and re-issued under rigid document control processes. <u>It is not acceptable however, to revise a performance standard just because the critical measure concerned cannot meet it</u>.

MAJOR ACCIDENT HAZARD UNDERSTANDING

One of the primary objectives of MAHMS is to identify the hazards and assess the risks posed by the operation. From this information an "understanding" of the major accident hazards can be imparted to members of the organisation working at each operating level. The level of detail of the understanding and thus hazard information requirements will be different as dictated by their operating level, roles and responsibilities and job function.

Table 6, over the page illustrates this:-

The following describes the hazard information needs and the hazard understanding to be provided at each operational level.

Hazard/Risk Picture – Senior Management

The Senior Management in an organisation need to understand the Major Accident Hazards arising from their operation, in order to make sure that the risks introduced by the hazards are managed adequately. The Senior Manager has ultimate ***accountability*** for the risk assessment and management activity and provide ***leadership*** to the business in this task.

Understanding will be provided at this level by means of hazard/risk pictures. These will be presented in the form of simple pie charts showing a qualitative risk analysis of Business Unit risks by "Hazard" and by "type of operation".

Table 6. MAHMS hazard understanding & information

	Hazard understanding & information	Risk assessment & management
Level 1 Accountable	Have the ultimately ***Accountability*** for assessment and management of risk and	***Evaluating risk***, to show that they are being adequately managed and show how the levels of risk

SENIOR MANAGEMENT	provide the ***Leadership*** to ensure MAHMS is successful:- • By understanding the hazards of the operation and their contribution to the overall risk picture. • By providing visible and unwavering leadership and commitment to MAHMS • By being responsible for creating the conditions under which the right HSE Culture is in place and engenders the right attitude amongst the workforce for MAHMS to succeed.	compare with the BP Corporate Risk Acceptance Criteria:- • Through risk pictures which show the relative levels of risk across the BU • By the qualitative assessment of risk to show the risk distribution by activity and Performance Unit/Asset and Facility • Through appropriate quantitative risk analysis to show how the significant risks compare with the bp Corporate Risk Acceptance Criteria
Level 2 Responsible OPERATIONAL MANAGEMENT	To be able to decide the ***priorities*** and supply the ***resources*** to manage the business as efficiently as possible whilst reducing and maintaining MAH risks to as low a level as possible:- • By having a sufficiently detailed understanding of the principal risk drivers and how they influence the likelihood and consequences of a MAH event in their operation. • Through knowing how changes to the operation, organisation and resources could have a detrimental effect on risk management arrangements.	Determine for each MAH a ***risk management strategy*** to reduce the safety, environmental and business interruption risk within each Performance Unit:- • Through conducting a qualitative Risk Ranking exercise for all MAHs which shows the event likelihood, and Safety, Environmental and Business Interruption consequences • By identifying the Key Risk Drivers which influence likelihood and/or Safety, Environmental or Business Interruption consequences • By deciding the most appropriate strategy to avoid or reduce the likelihood and reduce the consequences to tolerable levels.
Level 3 Facilitators	Instinctively know what is important about day to day operation, so that they can	Determine a range of ***critical measures*** to be deployed which enable the Asset/Facility

FACILITY MANAGEMENT (OIMs OSMs & SUPERVISORS)	make ***informed judgements*** about the criticality of work and assign the priorities and resources accordingly:- • By understanding the role of critical measures (people, processes and plant) in MAHMS. • By playing a key role in the day to day management of critical measures to ensure their sufficiency and effectiveness through assurance processes like active monitoring and verification.	Management to effectively manage their MAH risks:- • Through Risk Registers detailing the Anatomy of all Reasonably Foreseeable MAH Events • By putting in place the Critical Measures (People, Processes & Plant) required to manage risk to a Reasonably Practicable level
Level 4 Implementers INDIVIDUALS (The Wider WORKFORCE)	Be fully aware of how his/her ***acts or omissions*** could lead to a MAH event, either by triggering the event directly or by rendering ineffective one or more of the critical measures. • Through workforce involvement in MAHMS Hazard Identification and Risk Analysis to gain the appropriate levels of Hazard Understanding • By having Training in terms of MAHMS awareness integrated into a structured Induction process for new starts and refreshers for all personnel • By having access to MAHMS information through an on-line MAHMS Web site Database, readily accessible for all who need to identify and use information.	Determine the ***Performance Standards*** required for critical measures to facilitate the management of their maintenance, availability and provide Performance Assurance on a day to day basis:- • By preparing a Performance Standard for each Critical Measure (People, Processes & Plant), which describes what it is meant to do; when, how often and for how long it is meant to do it and under what conditions it should remain effective • The Performance Standard will provide the benchmark against which Performance Assurance activities will be carried out.

Figure 9 below shows a typical Hazard/Risk Picture (NB: risk values shown are for demonstration only).

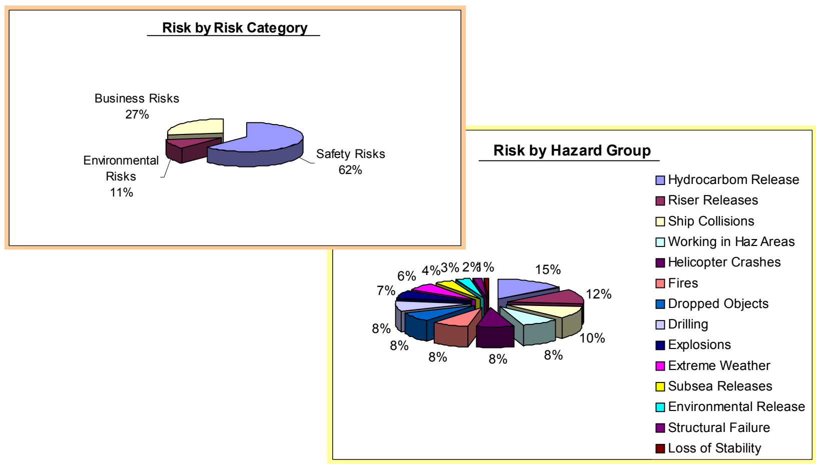

Figure 9. Hazard/risk ranking by risk category and hazard group

Hazard/Risk Ranking Matrices – Asset Managers

Asset Managers require sufficient MAH understanding to be able to appreciate the priorities and resource requirements are for MAHMS to be effective. Thus their primary role is to determine ***priorities*** and provide ***resources*** for MAHMS activities in their part of the organisation.

The relevant level of understanding will be provided to the Performance Units by means of both the risk pictures described above; and Hazard/Risk Ranking Matrices. The Matrices will be the output from qualitative risk analysis and will list the Hazards in descending order of risk contribution. They will also identify the principal drivers influencing likelihood and consequence for each different MAH. This information will be presented in the form of:

- Simple pie charts showing risk profile between different facilities/assets
- Hazard/Risk ranking matrix for each facility/asset showing the principal risk drivers

Figure 10 illustrates a typical Hazard/Risk Ranking Matrix (NB: risk values shown are for demonstration only).

Hazard Registers – Facility Management

The Facility Management Team (Delivery Managers, OIMs, Onshore Shift Managers and Supervisors), need to instinctively know what is important about day to day risk management on the operation, so that they can make ***informed judgements*** about the criticality of work and assign the priorities and resources accordingly.

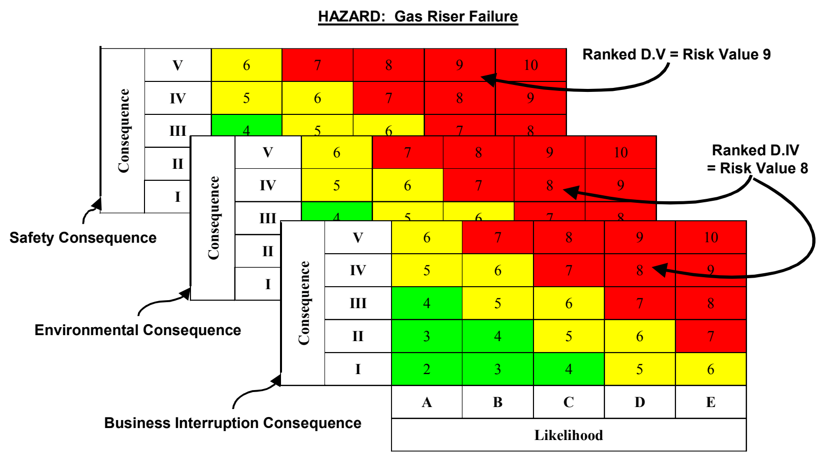

Figure 10. Hazard/risk ranking of a MAH

MAHM understanding will be provided to facility operations and maintenance personnel through the Hazard/Risk Pictures and Rankings described above, and the hazard register. Hazard registers are where the detailed information on each hazard will be documented. The information will be gleaned through Major Hazard Identification (MAHID) exercises to be held for each facility.

The layout and content of a hazard register is illustrated in Figure 11.

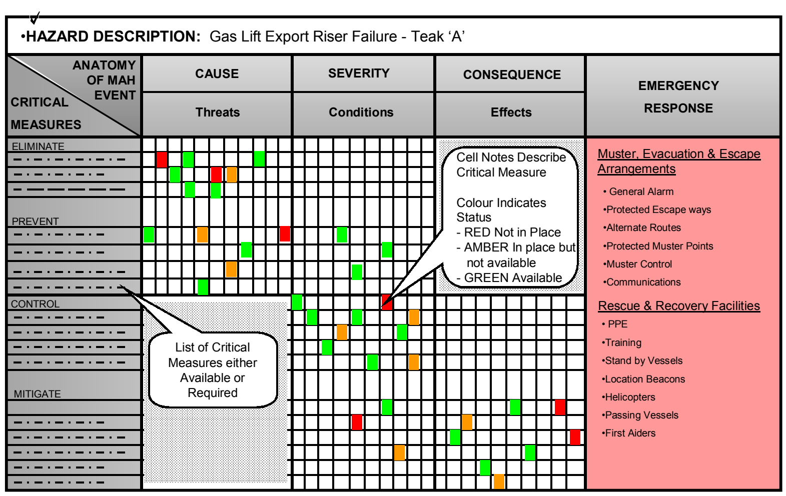

Figure 11. Layout and content of a hazard register

In particular, the information presented in the Hazard Register will provide the means for supervisors to apply "active monitoring" to manage their MAHMS Performance Assurance responsibilities on a day to day basis.

Anatomy of a Major Accident Hazard – Operations Workforce

Apart from their other MAHMS Roles and Responsibilities, individuals have a need to understand Major Accident Hazards sufficiently well to be fully aware of how his/her ***acts or omissions*** could lead to a MAH event. This could either be by triggering the event directly or by rendering ineffective one or more of the critical measures.

As well as all the sources of information described above, a detailed understanding of the relevant Hazards, will be supplied through various communication tools all describing the Anatomy of each Major Accident Hazard. The Anatomy of a Hazard is illustrated in Figure 12 below:-

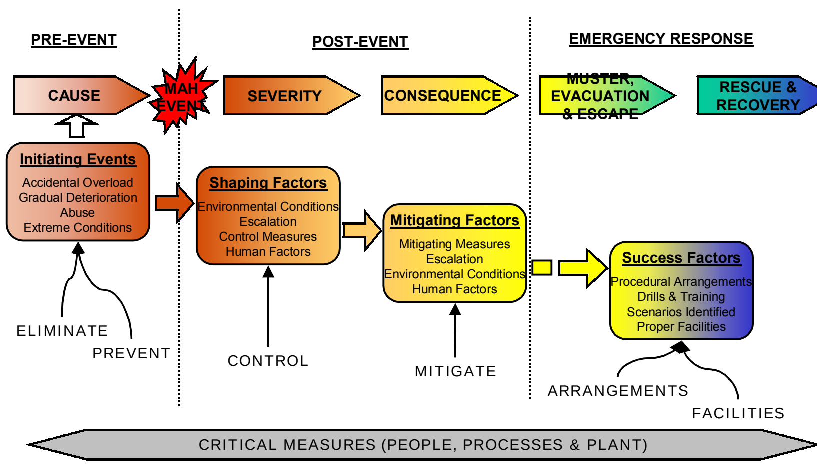

Figure 12. Anatomy of a major accident hazard event

MAJOR ACCIDENT HAZARD INFORMATION

The Major Accident Hazard Information required for each of the operating levels described above, will be continuously available to all individuals in the organisation through the MAHMS on-line web based database. It will be presented in a form suitable for them to understand MAH sufficient to fulfil their individual requirements.

Figure 13 shows an overview of the information obtained from the above analyses, and illustrates how it will be presented in order to be usable to the various personnel involved in day to day risk management operations.

The type of MAH information available is typically as follows:-

Causes and Likelihood

There should be a detailed understanding of the types of causes, whether due to human factors, procedural malfunction or failure of plant or the structure, and the likelihood for those causes to occur on the facility. For example the possibility of corrosion, the number of corrosion sites and the corrosivity of the process fluids, are all factors which determine the likelihood of corrosion led failures of the pressure envelope.

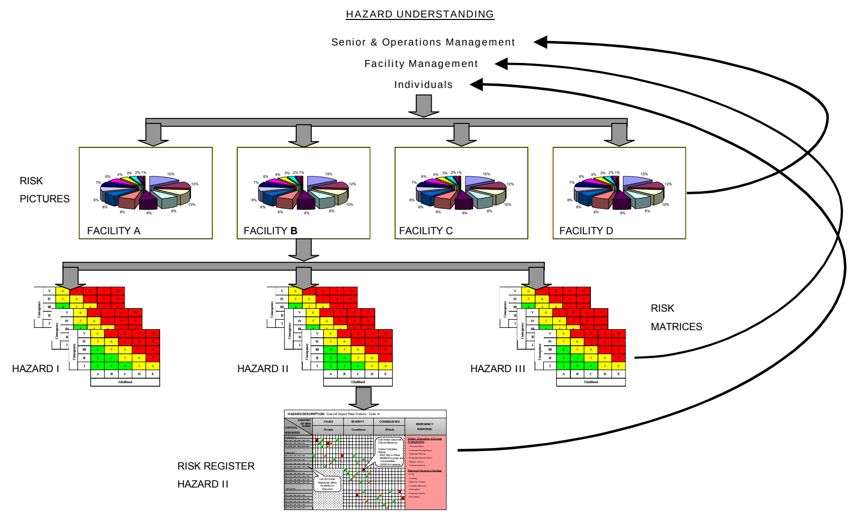

Figure 13. Overview of MAHMS database

There should be a formal process, such as a MAHID, to confirm that all causes have been identified. It must be applied to all major hazards arising from any aspect of the operation, failure of plant or structures, not just process plant. For example, all of the means whereby a floating marine structure could be overloaded or damaged should be rigorously examined. The level of further analysis of the identified causes should be determined, so that they may be effectively managed.

Severity

Where hazards have the potential to cause a major accident, the severity should be quantified in relevant terms such as the type of hazardous event, the energy released, the size and the area affected, intensity of noise, heat and smoke, location and duration. The quality of analysis needed will depend upon the potential impact of the event, the risks and the type of information needed to make informed decisions.

Immediate Effects and Escalation Potential

Where hazards have the potential to escalate into a major accident, the effects of the initial event on people, processes and the plant, structure or safety systems that may fail leading to further escalation, should be determined. The quality of that analysis required will depend on the type of event, the underlying potential for significant escalation, and the type of information needed to make informed decisions. Tools will be required to map these escalations and methods to assess the effectiveness or vulnerability of safety systems and emergency response facilities.

Consequence

Where hazards have the potential to result in a major accident, all of the routes that lead to that consequence should be identified and mapped. The sequence, timing and characteristics of the event progression should be determined. The quality of the analysis required will depend on the likelihood of that escalation, the overall potential loss of life and facility damage, and the type of information needed to make informed decisions.

Risk

A picture of the relative risks to the overall facility from individual hazards should progressively develop as the assessment progresses. This is essential information for the decisions in the hazard management process. The quality of risk analysis required for individual hazards will depend upon their contribution to the overall risk. Major accident hazards may each be subjected to a qualitative risk analysis that covers both the initial event and its potential for escalation. Where specific hazards make a dominant contribution to the overall risk, or the overall risks cannot easily be reduced to tolerable levels, a more formal process of Quantitative Risk Assessment (QRA) may be applied.