Risk Assessment and Management: Challenges of the Macondo Well Blowout Disaster

Robert. G. Bea

1 Looking Back

In this Deepwater Horizon Study Group Working Paper, 'looking back' at the Macondo well blowout failures is developed by first describing how failures in Risk Assessment and Management (RAM) processes have been responsible for previous failures of engineered systems. Special attention is given to high consequence 'system' failures. Experience has shown these failures have signatures that are very different than those which are much less severe. These system failures develop over long periods of time, involve many people and organizations, and result from a sequence of multiple malfunctions that combine to result in high consequence failures.

The purpose of looking back at the Macondo well blowout failures is not to place blame on people or organizations having responsibilities for this disaster. There still is much missing information on how the failures developed. Consequently, what happened and why these things happened is not understood with certainty at this time. If previous system failures are any guide, it will take many more years before these things are known. The purpose of looking back is to understand how the failures might have developed; these are plausible scenarios for the RAM failures. This is done so these plausible scenarios are accounted for in recommendations for future improvements. We look back to enable us to better look forward.

2 Lessons from Failures of Offshore Oil and Gas Systems

During the period 1988 – 2010, studies have been performed by the Marine Technology and Management Group, the Center for Risk Mitigation, and the Center for Catastrophic Risk Management at the University of California Berkeley on more than 600 well-documented system failures involving a wide variety of types of engineered systems. Sufficient reliable documentation was available about these failures to understand the roles of the various components that comprised the systems during the life-cycle phases that led to the failure. In many cases, personnel who had participated in the developments were interviewed to gain additional insights about how and why the failures had developed. Care was exercised to neutralize biases in developing these insights (e.g., corroboration with multiple reliable sources). This work included study of the failures of the Ocean Ranger drilling unit (Canadian East Coast, 1982) Piper Alpha production platform (North Sea, 1988), the Ranger I mobile drilling platform (Gulf of Mexico, 1979), the Alexandar Kielland (1980), the South Pass Block 70 production platforms (Gulf of Mexico, 1969), the Exxon Valdez tank ship (Prince William Sound, Alaska, 1990), and the P36 production platform (Brazil, 2001). This work included studies of other complex engineered systems operating in high hazard environments such as the failure of the NASA Columbia space shuttle (2003) and the failure of the flood protection system for the Greater New Orleans Area during Hurricane Katrina (2005).

A key element in the processes used to study these failures was the goal of the studies. There are many different ways to study failures and there are many different goals in such studies. In this case,

a specific goal of the studies was to better understand how to organize and implement future RAM processes during the life-cycles of complex engineered systems.

3 Defining Failures

In this work, failure has been defined as realizing undesirable and unanticipated compromises in the 'quality' of an engineered system. Quality is characterized as resulting from the integrated effects of four desirable system performance attributes:

- Serviceability (fitness for intended purposes),
- Safety (freedom from undue exposure to harm or injury of people, property, and the environment),
- Durability (freedom from unanticipated degradation in the Quality attributes), and
- Compatibility (meets business, government, social – public, and environmental requirements).

Each of these four system performance attributes includes considerations of resilience (abilities to re-establish services in acceptable time periods after significant disruptions) and sustainability (abilities to provide acceptable services over desirable periods of time).

Failures are defined in this way for several reasons. Failures occur in a variety of different ways at different times during the life of engineered systems. Failures involve many more performance attributes than what has been traditionally defined as 'safety'. To prevent failures, as systems are configured, designed, constructed, operated, maintained, and ultimately – decommissioned, it is important to preserve balance between the critical performance characteristics. This struggle for balance in developing performance characteristics frequently shows up as unresolved tensions between business goals - providing desirable goods and services with resulting desirable profitability (production) and the other quality characteristics (protection). When this tension is not resolved, then production increases without commensurate increases in protection; failures are an inevitable outcome (Reason 1997).

4 Defining Systems

The studies of failures engineered systems have shown that the term 'systems' needs to be clearly defined. In this work, seven primary interactive, inter-related, and interconnected components have defined as comprising engineered systems:

- Structure (provides support for facilities and operations),
- Hardware (facilities, control systems, life support),
- Procedures (formal, informal, written, computer software),
- Environments (external, internal, social),
- Operators (those who interface directly with the system),
- Organizations (organizational and institutional frameworks in which operations are conducted), and
- Interfaces among the foregoing.

Engineered systems are not static mechanical systems. Because of the human and environmental components, they are dynamic, highly interactive, and adaptive. Past failures of offshore exploration and production systems have repeatedly demonstrated the performance and reliability of these systems depend primarily on 'humanware' – operating teams and organizations. A combination of reliable hardware and humanware are needed to realize high quality reliable systems.

Studies of failures of engineered systems have identified the importance of system 'interfaces' in the development of failures. Breakdowns in communications frequently have developed at the interface between the operators (groups of people with daily responsibilities for the conduct of system operations) and the organizations that control resources, means, and methods used by the operators. Communication malfunctions at organization-to-organization interfaces (e.g., operator – regulator, operator – subcontractrors) are even more prevalent.

These characteristics of systems makes them particularly challenging for RAM approaches and processes. A variety of dynamic RAM approaches and strategies must be employed to address real systems. These approaches will be further developed in the looking forward part of this section.

5 Understanding the Life-Cycle

To understand failures, it is essential to identify how the system was developed throughout its life-cycle to the point of failure. System failures are deeply rooted in their history. Understanding the history of a particular system should include development of an in-depth understanding of how the system was conceived, designed, constructed, operated, maintained, and for some systems, decommissioned. This understanding must be developed in the context of the locale and industrial – governmental enterprises in which the system was developed. Contrasting development of the life-cycle of the failed system with 'best practice' systems that have performed satisfactorily can provide important insights into how and why a particular system fails and another comparable system succeeds (pattern matching).

6 Uncertainties

Uncertainties that have been major contributors to failures of engineered systems have been organized into four major categories:

- Type I - natural or inherent variability (aleatory),
- Type II - analytical (qualitative, quantitative) modeling uncertainties (epistemic),
- Type III - human and organizational task performance uncertainties, and
- Type IV - knowledge related uncertainties.

This is only one way to organize and characterize uncertainties. This organization has been based on the failure studies cited earlier and on specific RAM approaches and strategies ('barriers') that can be used to address these categories of uncertainties.

Uncertainty is something that is indefinite, problematical, not certain to occur, dubious, not clearly identified or defined. Very few things are really certain. Much engineering is taught in a deterministic framework where outcomes are certain - right or wrong - yes or no. Many

investigations of failures are performed in similar deterministic ways. Real engineered systems rarely operate in deterministic frameworks.

The first category of uncertainty has been identified as natural or inherent randomness. This category of uncertainty is essentially 'information insensitive' - gathering additional data and information has no important effect on characterizations of the uncertainties. Variability in the properties of manufactured and natural materials is an example of Type I uncertainty.

The second category of uncertainty is identified as analytical modeling or professional uncertainty. This type of uncertainty applies to deterministic, but unknown values of parameters (parameter uncertainty); to modeling uncertainty (imperfect understanding of problems, simplified analytical models used in practice); and to the actual state of the system (imprecise knowledge of properties and characteristics). This category of uncertainty is 'information sensitive' - gathering additional data and information can have important effects on characterizations of the uncertainties.

The third category of uncertainty has been identified as related to human and organizational task performance. People and organization task performance have important effects on all engineered systems from the time of development of a concept to the time the system is decommissioned. The actions and inactions of people cannot always be anticipated and are not always desirable or have desirable outcomes. A primary reason for identifying this category of uncertainty in development of understanding of failures is because different approaches and strategies must be used to address and manage this source of uncertainties.

Human and organizational task performance malfunctions frequently have been termed 'human errors' and accident causations attributed to this source of uncertainty. As pointed out by several investigators, 'errors are results not causes' (Woods 1994). This means additional efforts are needed to understand what causes these errors or malfunctions so that effective approaches and strategies can be used to minimize their occurrence and effects. A wide variety of Performance Shaping Factors (e.g., fatigue) have important influences on development of human malfunctions. It is clear there are reasonable limits to what can be done to minimize this category of uncertainties – 'to err is human'. This recognition encourages attention to development of systems that will minimize the effects of human and organizational task performance malfunctions – these are defect and damage tolerant 'robust' systems.

The fourth category of uncertainty is related to development of knowledge and understanding. This category has been divided into two sub-categories: unknown knowables and unknown unknowables. In the first case, the knowledge does exist, but it has not been accessed or not accessed and utilized properly. This category of knowledge uncertainty has been termed 'Black Swans' (Taleb 2007). In the second case, the knowledge does not or did not exist; it is not reasonable to conclude what happened could have been predicted in any reasonable way. This category of knowledge uncertainty has been termed "Flying Cows" (Bea 2002).

One could contend that uncertainty is uncertainty and these differentiations are not necessary. In this work, differentiations have been used in developing understanding of failures because different approaches and strategies are useful in assessing and managing the different categories of uncertainties.

7 Risks and Uncertainties

Risks result from uncertainties. Risks can be expressed as resulting from the combination of two elements: the likelihoods of something going wrong (failing), and the consequences associated with something going wrong. Risk sometimes is expressed as the product of the likelihood of failure and the consequences associated with that failure – the 'expected' risk. That expression has been avoided in this work because it does not encourage appropriate recognition and management of the two categories of things that determine risk: likelihoods and consequences of failures.

A primary goal of RAM is to assess and manage the risks associated with engineered systems during their life-cycle so performance of the system is desirable and acceptable. Determination of what constitutes desirable and acceptable risks associated with engineered systems ideally is a deliberative, interactive, ongoing social process involving the public, industry and commerce, government, and advocates for the environment (Wenk 2010). Failures of engineered systems frequently have been developed when specific 'risk targets' have not been defined and agreed upon (failure of social processes) before the systems are designed. One group, for example the industry, thinks the risks are acceptable, while the other groups (public, government agencies, environmental advocates) have not understood and acknowledged that the risks are acceptable.

Failures frequently develop because uncertainties, likelihoods, and consequences of failures are not properly understood (failure of assessment) and/or not properly managed (failures of management). Failures develop when the definitions and characterizations of what constitutes desirable and acceptable risks are flawed; the assessment and management processes are not directed to achieve the proper goal (acceptable performance). The likelihoods of undesirable performance are expressed as the probabilities of failure. Reliability is defined as the likelihood (probability of future occurrence) that desirable and acceptable quality is developed during the life-cycle of an engineered system.

Because of inevitable uncertainties, the likelihoods of failure are finite; perfect reliability is not possible. It takes expenditure of resources – including monetary and human capital – to achieve desirable and acceptable risks. Adequate industrial – commercial profitability is essential to be able to have the resources required to develop acceptable risks. This is another key point at which past failures of engineered systems have been founded. This can be because the risks are not properly assessed – they are undervalued. Consequently, insufficient resources are allocated to defend against these risks. There are a wide variety of important reasons for the under-valuations of risks – including 'wishful thinking'.

Risk management utilizes multiple approaches and strategies – barriers - to address both likelihoods and consequences of failure. Three general categories of risk management approaches have been employed: proactive (before activities are carried out), reactive (after activities are carried out), and interactive (during performance of activities). Three general categories of risk management strategies have been employed as parts of these three approaches: minimize the likelihoods of malfunctions, minimize the effects of malfunctions, and increase the proper detection – analysis – and remediation of malfunctions. Prevention, remediation – emergency response, and control – crisis management are employed in continuous coordinated interactive processes intended to achieve acceptable risks throughout the life-cycle of a system. Effective RAM is a continuous improvement processes that is conducted throughout the life-cycle of a system (Figure 7.1).

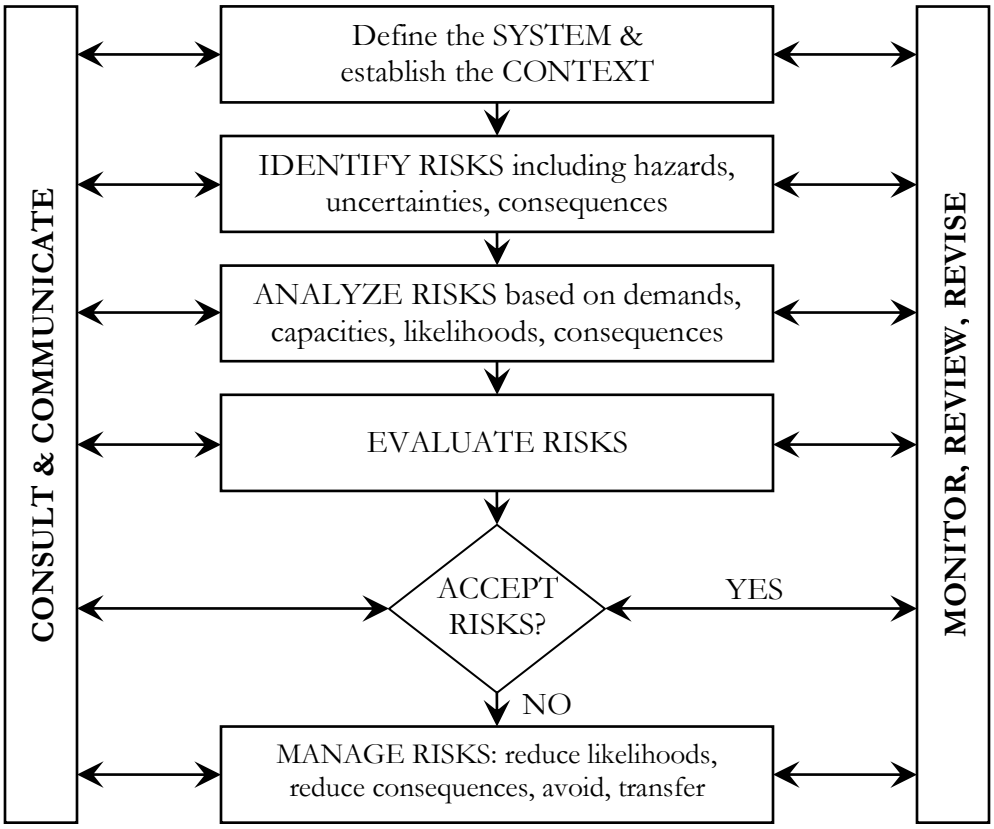

Figure 7.1 – RAM process.

This work has shown that the single most important and essential element in effective RAM is creating, developing, and maintaining collaborative enterprises of High Reliability Organizations (Roberts 1989) and High Reliability Governance (Carnes 2010) that develop and maintain High Reliability Systems. Healthy and productive industry requires equally healthy and productive government. If these three components are not present, then one can expect significant problems in realizing acceptable quality and reliability from an engineered system. It has been adequately demonstrated that organizations have critical influences in contributing and compounding malfunctions that can lead to system failures. High reliability organizations with high reliability governance are important because of their determination and controls over the resources, means and methods that can be mobilized to improve system quality and reliability. Development of high reliability systems must effectively integrate the industrial and governmental components (high reliability governance) and the owner – operator and sub-contractor components (high reliability organizations) to develop an effective collaborative enterprise enabling realization of high reliability systems.

Properly assessing the consequences of failures – before the failures develop – is very important. Experience shows the single dominant tendency is to underestimate the true consequences of failures. The system operators and organizations think they are prepared to handle failures, but when the failures happen, the responses clearly show the thinking and preparations were seriously

deficient. The underestimates in the consequences of failures result from a wide variety of deficiencies in the assessment processes (e.g., not recognizing long-term and off-site effects). Frequently, important things are simply left out and there are major flaws embedded in the assumptions concerning controllability of the consequences. In the face of evidence to the contrary, we hope that things will work as they should and the consequences will be low. Failures frequently develop because of the tendency to underestimate the consequences of failure coupled with the consequent tendency to improperly manage the consequences associated with an engineered system; the system is not properly prepared to deal with the potential consequences of the potential failures it faces.

8 The Hows of Failures

Studies of past failures of engineered systems clearly show that the uncertainties involved in causation of failures most often (80% or more) involve human, organizational and knowledge uncertainties (Bea 2000a, 2002). These two categories of uncertainties have been identified as *Extrinsic Uncertainties*. The remainder of the uncertainties (20% or less) involve natural and modeling related uncertainties. These two categories of uncertainties have been identified as *Intrinsic Uncertainties*.

Of the extrinsic uncertainties, about 80% of these developed and became evident during operations and maintenance activities; frequently, maintenance activities interacted with operations activities in undesirable ways. Of the failures that occurred during operations and maintenance, more than 60% of these failures could be traced to seriously flawed concept development and design; the physical system may have been designed according to accepted standards and yet was seriously flawed due to limitations and imperfections that were embedded in the standards and/or how they were used. As a result of incentives to reduce initial costs, systems were configured that were very 'brittle' – as long as everything planned was done according to guidelines and there were no undesirable surprises (unforeseen hazards) – the systems performed satisfactorily. When things were not done according to guidelines and the unanticipated hazards became reality, the system did not have sufficient 'robustness' (tolerance to damage and defects) to perform acceptably.

In addition, engineered systems were designed that could not be built, operated, and maintained as originally intended. Changes (work-arounds, field modifications) were made during the construction process to allow the construction to proceed and flaws were introduced by these changes. In some cases, flaws and defects were introduced by the construction process itself. After the system was placed in operation, modifications were made in an attempt to make the system workable or to facilitate the operations, and in the process additional flaws were introduced. Thus, during operations and maintenance phases, operations personnel were faced with an accumulation of flaws and defects reflected in a seriously deficient or defective system that could not be operated and maintained as intended.

Of the 20% of failures that did not occur during operations and maintenance of the systems, the percentages of failures developing during the design and construction phases were about equal. There are a large number of failures that develop during these phases that represent project failures that end up in legal proceedings.

The following classifications of how components in engineered systems fail are heuristic; they are based on studies of past failures of engineered systems. The classifications are intended to identify the key modes (how's) in which malfunctions or failures develop. Generally, the why's are not identified because these are extremely difficult, if not impossible, to determine accurately. There is a very wide diversity of types of 'biases' that involve many people, at different locations, performing over long periods of time that influence looking back investigations and studies to determine the why's of failures. This is particularly true when people involved in the development of a failure are subjected to formal investigations and legal proceedings (e.g., defensive avoidance).

8.1 Operator malfunctions

There are many different ways to define, classify and describe operator (those who have direct interfaces with the system) malfunctions. Operator malfunctions can be defined as actions taken by individuals that can lead an activity to realize a lower quality and reliability than intended. These are malfunctions of commission. Operator malfunctions also include actions not taken that can lead an activity to realize a lower quality than intended. These are malfunctions of omission. Operator malfunctions also have been described as mis-administrations and unsafe actions. Operator errors result from operator malfunctions.

Operator malfunctions can be described by types of malfunction mechanisms. These include slips or lapses, mistakes, and circumventions. Slips and lapses lead to low quality performance where the outcome of the action was not what was intended. Frequently, the significance of this type of malfunction is small because these actions are easily recognized by the person involved and in most cases easily corrected.

Mistakes can develop where the action was intended, but the intention was wrong. Circumventions (violations, intentional short-cuts) are developed where a person or an operating team decide to break some rule for what seems to be a good (or benign) reason to simplify or avoid a task. Mistakes are perhaps the most significant because the perpetrators have limited or misleading clues that there is a problem. Often, it takes a domain experienced outsider to the situation to identify mistakes.

Based on studies of available failure databases on engineered systems, and studies of case histories in which the acceptable quality of these systems has been compromised, a taxonomy of operating team malfunctions is summarized as follows:

- Communications – ineffective transmission of information
- Culture – inappropriate goals, incentives, values, and trust; imbalances between production and protection
- Slips – accidental lapses
- Violations – intentional infringements or transgressions
- Ignorance – unaware, unlearned
- Planning & Preparation – lack of sufficient program, procedures, readiness, and robustness
- Selection & Training – not suited, educated, or practiced for the activities
- Limitations & Impairment – excessively fatigued, stressed, and having diminished senses

- Mistakes – cognitive malfunctions of perception, interpretation, decision, discrimination, diagnosis, and action

The sources of mistakes or cognitive malfunctions (operators, organizations) are:

- Perception – unaware, not knowing
- Interpretation – improper evaluation and assessment of meaning
- Decision – incorrect choice between alternatives
- Discrimination – not perceiving the distinguishing features
- Diagnosis-incorrect attribution of causes and or effects
- Action- improper or incorrect carrying out activities

Studies of past system failures clearly indicates that the single leading factor in operator malfunctions is communication breakdowns. Communications can be very easily flawed by 'transmission' problems and 'reception' problems. Feedback,so important to validate communications, frequently is not present nor encouraged. Language, culture, societal, physical problems, organizational and environmental influences can make this a very malfunction prone process. In team settings, management 'authority gradients' (lethal arrogance, hubris) are frequently responsible for breakdowns in communications ("do not bother me with the facts, I already have my mind made up").

8.2 Organization malfunctions

Analysis of failures of engineered systems provides many examples in which organizational malfunctions have been primarily responsible for the failures. Organization malfunction is defined as a departure from acceptable or desirable practice on the part of a group of individuals or of a group of organizations that results in unacceptable or undesirable results. Based on the study of case histories of failures of engineered systems and studies of High Reliability Organizations, a classification of organization malfunctions was developed as follows:

- Culture – inappropriate goals, incentives, values, and trust; imbalances between production and protection
- Communications – ineffective transmission of information
- Violations – intentional infringements or transgressions
- Ignorance – unaware, unlearned
- Planning & Preparation – lack of sufficient program, procedures, readiness
- Structure & Organization – ineffective connectedness, interdependence, lateral and vertical integration, lack of sufficient robustness
- Monitoring & Controlling – inappropriate awareness of critical developments and utilization of ineffective corrective measures
- Mistakes – cognitive malfunctions of perception, interpretation, decision, discrimination, diagnosis, and action

Frequently, the organization develops high rewards for maintaining and increasing 'production'. Meanwhile the organization hopes for quality and reliability – 'protection'. This has been expressed as "rewarding 'A' (production) while hoping for 'B' (protection)." The formal and informal rewards

and incentives provided by an organization have a major influence on the performance of operators and on the quality and reliability of engineered systems. In a very major way, the performance of people is influenced by the incentives, rewards, resources, and disincentives provided by the organization. Many of these aspects are embodied in the 'culture' (shared beliefs, artifacts, and operating practices) of an organization. This culture largely results from the history (development and evolution) of the organization. Cultures that are developed over long periods of time are extremely resistant to change.

Several examples of organizational malfunctions recently have developed as a result of efforts to down-size and out-source as a part of 're-engineering' organizations. Loss of corporate memories (leading to repetition of errors), inadequate 'core competencies' in the organization, creation of more difficult and intricate communications and organization interfaces, degradation in morale, unwarranted reliance on the expertise of outside contractors, cut-backs in quality assurance and control, and provision of conflicting incentives (e.g., cut costs, yet maintain quality) are examples of activities that have lead to substantial compromises in the intended quality of systems. Much of the down-sizing ('right-sizing'), outsourcing ('hopeful thinking'), and repeated cost-cutting ('remove the fat until there is no muscle or bone') seems to have its source in modern 'business consulting'. While some of this thinking can help promote 'increased efficiency' and maybe even lower CapEx (Capital Expenditures), the robustness (damage and defect tolerance) of the organization and the systems its creates can be greatly reduced. Higher OpEX (Operating Expenditures), more failures, and unexpected compromises in desired quality and reliability can be expected; especially over the long-run.

Experience indicates that one of the major influences in organizational malfunctions is the culture of the organization. Organizational culture is reflected in how action, change, and innovation are viewed; the degree of external focus as contrasted with internal focus; incentives provided for risk taking; the degree of lateral and vertical integration of the organization; the effectiveness and honesty of communications; autonomy, responsibility, authority and decision making; rewards and incentives; and the orientation toward the quality and reliability of performance (protection) contrasted with the quantity of production. The culture of an organization is embedded in its history. Frequently, the culture of an organization is heavily influenced by its geographic location – and in the history and culture associated with that location.

The culture of an organization often is severely challenged as a result of 'mergers' – corporate or governmental. Corporate culture 'clashes' develop when one culture attempts to 'take over' another culture that exists within the same organization. Drives to achieve uniformity in 'how things are done' can be very counterproductive – particularly when there is more than one way to 'do the right things right'. One of the major culture elements is how managers in the organization react to suggestions for change in management and the organization. Given the extreme importance of the organization and its managers on quality and reliability, it is essential managers see suggestions for change in a positive manner. This is extremely difficult for some managers because they do not want to relinquish or change the strategies and processes that helped make them managers.

Organizations do not exist in isolation; they influence other organizations and are influenced by other organizations. Many high consequence failures of engineered systems involve malfunctions that develop in multiple organizations having different responsibilities for different parts of a given system. In this work, the interactions amoung different organizations has been cast in the framework

of a Technology Delivery System (TDS) (Wenk 2010). A TDS consists of four fundamental components: the public, the governmental organizations (local, state, national, and international), commercial and industrial organizations, and the environment (generally represented by environmental advocate organizations). The function of a TDS is to apply scientific and engineering knowledge to develop and deliver goods, services, and resources needed by a society. A TDS models reality with inputs of knowledge, fiscal, natural, and human resources synchronized by a network of communications. Outputs are both intended and unintended. The system is driven and steered by three operating instructions—market place economics, public policies, and social norms.

In the case of system failures, malfunctions in the TDS have often developed at the interfaces and interactions between the commercial – industrial component and the governmental component. The government component empowers the industrial component to develop goods, services, and resources by and for the public. The government is charged with oversight of the industrial activities: with defining the goals and objectives of the industrial activities and with assuring that these goals and objectives are realized to serve the public interests and protect the environment. The industrial component is also responsible to the public in the form of shareholders who help provide financial capital to maintain and develop the commercial – industrial enterprise. Major failures of engineered systems frequently have developed because of severe, long-term breakdowns in collaborations between the industrial and governmental components (Reason 1997, Bea 2000a, 2002). These breakdowns are exacerbated when the governmental component merges its goals with those of the industrial component. High Reliability Governance is not developed (Carnes 2010). Severe conflicts are developed between the public governmental responsibilities and the commercial industrial responsibilities and which result in failures of the engineered systems. Similar breakdowns develop when the capabilities and behaviors of either of the components are not able to constructively collaborate to assure that the goals and objectives of the four TDS components are well served. There must be comparable 'strengths' and 'capabilities' in the industrial and governmental components and these must work in responsible and collaborative ways for the goals of quality, reliability, and acceptable risks to be realized.

8.3 Structure, hardware, and equipment malfunctions

Human malfunctions can be initiated by or exacerbated by poorly designed and engineered systems that invite malfunctions. Such systems are difficult to construct, operate, and maintain. A classification system for hardware-related malfunctions (equipment, structure) is as follows:

- Serviceability – inability to satisfy purposes for intended conditions
- Safety – excessive threat of harm to life and the environment, demands exceed capacities
- Durability – occurrence of unexpected maintenance and degradations in the performance characteristics of the system, less than expected useful life
- Compatibility – unacceptable and undesirable economic, schedule, environmental, and aesthetic characteristics

The important characteristics of resilience and sustainability are a part of these four characteristics of 'quality'. Resilience is defined as the time required to re-establish performance of a system after it has been disrupted. Sustainability is defined as the ability of a system to provide its intended goods and services with desirable quality and reliability.

New technologies compound the problems of latent system flaws (system pathogens) (Reason 1997). Excessively complex design, close coupling (failure of one component leads to failure of other components) and severe performance demands on systems increase the difficulty in controlling the impact of human malfunctions even in well operated systems. The field of ergonomics (people-hardware interfacing) has much to offer in helping create 'people friendly' engineered systems. Such systems are designed for what people will and can do, not what they should do. Such systems facilitate construction (constructability), operations (operability), and maintenance (maintainability, repairability).

The issues of system robustness (defect or damage tolerance), design for constructability, and design for IMR (Inspection, Maintenance, Repair) are critical aspects of engineering systems that will be able to deliver acceptable quality and reliability. Design of the system to assure robustness is intended to combine the beneficial aspects of configuration, ductility, excess capacity, and appropriate correlation (it takes all four). The result is a defect and damage tolerant system that is able to maintain its quality characteristics in the face of human malfunctions. This has important ramifications with regard to engineering system design criteria, guidelines, and practices which have been directed toward development of 'cost-optimized' systems – minimum CapEx systems. Effective 'back-ups', frequently referred to as 'redundancy', are removed to reduce first costs. In the process, damage and defect intolerant systems are developed. When these systems are challenged with unexpected uncertainties, defects, and damage, they are not able to perform acceptably and failures are developed.

It is becoming painfully clear that the majority of engineering design codes and guidelines do not provide sufficient direction for creation of robust – damage – defect tolerance systems. Thinking about sufficient damage tolerance and inherent stability needs rethinking. Thinking about designing for the 'maximum incredible' events needs more development. While two engineered systems can both be designed to 'resist the design conditions', the two systems can have very different robustness or damage stability (intrinsic reliability). 'Minimum' CapEx systems can and do not have an appropriate configuration, sufficient excess capacity and ductility, or appropriate relationships (correlations) to allow them to successfully sustain the inevitable defects and damage that can be expected to develop during its life. Sufficient damage and defect tolerance almost invariably results in increases in CapEx (capital expenditures); the expectation and the frequent reality is that OpEx (operating expenditures) will be significantly lowered. But, one must have a 'long-term' view for this to be realized.

Studies of failures of engineered systems has clearly shown that the foregoing statements about structure and hardware robustness apply equally well to organizations and operating teams. Proper configuration, excess capacity, ductility, and appropriate correlations play out in organizations and teams in the same way they do in structure and hardware components. It is when the organization or operating team defected and damaged – and is under serious stress, that the benefits of robustness become evident. A robust organization or operating team is not a repeatedly downsized (lean and mean), excessively out-sourced (unable to manage correctly), and financially strangled, excessive cost-cutting organization. Robust organizations are Higher Reliability Organizations.

8.4 Procedure and software malfunctions

Based on the study of procedure and software related issues that have resulted in failures of engineered systems, A classification system for procedure or software malfunctions is as follows:

- Incorrect - faulty
- Inaccurate - untrue
- Incomplete - lacking the necessary parts
- Excessive Complexity - unnecessary intricacy
- Poor Organization - dysfunctional structure
- Poor Documentation - ineffective information transmission

These malfunctions can be embedded in engineering design guidelines and computer programs, construction specifications, and operations manuals. They can be embedded in contracts (formal and informal) and subcontracts. They can be embedded in how people are taught to do things. With the advent of computers and their integration into many aspects of the design, construction, and operation of oil and gas structures, software errors are of particular concern because the "computer is the ultimate fool." Several failures and near-failures of offshore oil and gas systems have developed as the result of undetected or uncorrected computer program defects – computer 'bugs'.

Software errors in which incorrect and inaccurate algorithms were coded into computer programs have been at the root cause of several recent failures of engineered systems. Guidelines have been developed to address the quality of computer software for the performance of finite element analyses. Extensive software testing is required to assure that the software performs as it should and that the documentation is sufficient. Of particular importance is the provision of qualified people who put information into computers and interpret output from the computer. Independent checking procedures that can be used to validate the results from analyses are needed to help eliminate 'computational malfunctions'. High quality procedures need to be verifiable based on first principles, results from testing, and field experience.

Given the rapid pace at which significant industrial and technical developments have been taking place, there has been a tendency to make design guidelines, construction specifications, and operating manuals more and more complex. Such a tendency can be seen in many current guidelines used for design of engineered systems. In many cases, poor organization and documentation of software and procedures has exacerbated the tendencies for humans to malfunction. Simplicity, clarity, completeness, accuracy, and good organization are desirable attributes in procedures developed for the design, construction, maintenance, and operation of engineered systems.

Procedure and software (computer) related malfunctions frequently have been found to be a primary player in failure causation. The procedures were found to be incorrect (faulty), inaccurate (untrue), incomplete (lacking important parts), excessively complex (unnecessary intricacy), obsolete (did not incorporate the best available technology), poorly organized (dysfunctional structure), and poorly documented (ineffective information transmission). These malfunctions often were embedded in engineering design guidelines and computer programs, construction specifications, and operations manuals. They were also embedded in contracts (formal and informal) and subcontracts. They were embedded in how people were taught to do things; "this is how we do things here."

With the advent of computers and their integration into many aspects of the design, construction, and operation of engineered systems, software errors are of particular concern because it is easy to become "trapped in the net" (Rochlin 1997). Software errors in which incorrect and

inaccurate algorithms were coded into computer programs have been at the root cause of several recent failures of engineered system (computer aided failures). Guidelines have been developed to address the quality of computer software for the performance of engineering analyses and qualification of software users. Extensive software testing is required to assure that the software performs as it should and that the documentation is sufficient. Of particular importance is the provision of independent checking procedures that can be used to validate the results from analyses. High quality procedures need to be verifiably based on first principles, results from testing, and field experience.

Given the rapid pace at which significant industrial and technical developments have been taking place, there has been a tendency to make design guidelines, construction specifications, and operating manuals more and more complex. Such a tendency can be seen in many current guidelines used for design of engineered systems. In many cases, poor organization and documentation of software and procedures has exacerbated the tendencies for humans to make errors. Simplicity, clarity, completeness, accuracy, and good organization are desirable attributes in procedures developed for the design, construction, maintenance, and operation of engineered systems.

8.5 Environmental influences promoting malfunctions

Environmental influences can have important effects on the quality and reliability of engineered systems. Environmental influences that can promote malfunctions include: 1) external (e.g., wind, temperature, rain, fog, darkness), 2) internal (e.g., lighting, ventilation, noise, motions), and 3) sociological and cultural factors (e.g., values, beliefs, morays). Sociological factors have proved to be of critical importance in many of the failures that were studied during this work. These environmental influences can have extremely important effects on human, operating team, and organizational malfunctions, the performance of structures and hardware.

9 Understanding Failures

Many different ways have been developed to facilitate understanding how the failures developed. Some of these processes are highly structured, extremely detailed and complex. All of these processes can be useful when used for their intended purposes. As a result of the failure studies summarized here, the failure development process was organized into three categories of events or stages: 1) *initiating*, 2) *contributing*, and 3) *propagating*. This failure analysis process does not attempt to detail or structure the ways the failure unfolded. Rather, it uses the system structure and malfunction classifications that have been developed earlier in this section.

For the failures studied, the dominant initiating events (about 80%) were developed by operators (e.g., design engineers, construction, operations, maintenance personnel) performing erroneous acts of *commission;* what was carried out had unanticipated and undesirable outcomes. The other initiating events were acts or developments involving *omissions* (something important left out, often intentional short-cuts and violations). Communications breakdowns (withheld, incomplete, untrue, not timely) were a dominant category of the initiating events. Various categories of violations (intentional, unintentional) were also very prevalent and were highly correlated with organizational and social cultures.

The dominant contributing events were organizational malfunctions (about 80%); these contributors acted directly to encourage or trigger the initiating events. Communication

malfunctions, interface failures (organization to operations), culture malfunctions (excessive cost cutting, down-sizing, outsourcing, excessive production pressures, ineffective protection measures), unrealistic planning and preparations, and violations (intentional departures from acceptable practices) were dominant categories of these organizational malfunctions.

The dominant propagating events also were found to be organizational malfunctions (about 80%); these propagators were responsible for allowing the initiating events to unfold into a failure or multiple failures (frequently called a disaster or catastrophe). With some important additions, the dominant types of malfunctions were found to be the same as for the contributing events. The important additions concerned inappropriate selection and training of operating personnel, failures in quality assurance and quality control (QA/QC), brittle structures and hardware (damage and defect intolerant), and ineffective planning and preparations to manage the consequences of one or more failures.

10 Impossible Failures

Most failures studied during this work involved never to be exactly repeated sequences of events and multiple breakdowns or malfunctions in the components that comprised a particular system. Failures resulted from breaching multiple defenses that were put in place to prevent the failures. These events are frequently dubbed 'incredible' or 'impossible'. After many of these failures, it was observed that if only one of the failure 'barriers' had not been breached, then the accident or failure would not have occurred. The failures developed when the proactive (conducted before activities), interactive (conducted during activities), and reactive (conducted after activities) RAM barriers were all breached simultaneously.

Experience shows it is extremely difficult, if not impossible, to recreate accurately the time sequence of the events that took place during the period leading to the failure. Unknowable complexities generally pervade this process because detailed information on the failure development is not available, is withheld, or is distorted by memory. Hindsight and confirmation biases are common as are distorted recollections. Stories told from a variety of viewpoints involved in the development of a failure have proved to be the best way to capture the richness of the factors, elements, and processes that unfold in the development of failures.

One of the very sobering observations concerning many 'impossible' failures is their occurrence is directly related to knowledge (information) access, development, and utilization. The unknown knowables have been identified as 'predictable surprises'. The second category - *unknown unknowables* - represents limitations in knowability or knowledge. Things combine in unpredictable ways to create 'crises' (unpleasant surprises) that if not properly assessed and managed turn into failures. There is ample history of accidents and failures due to both of these categories of challenges to knowledge. They appear to be most important during the early phases of constructing and operating engineered systems - 'burn-in' failures. They also appear to be most important during the late life-cycle phases; 'wear-out' failures. In this case, the quality characteristics of the system have degraded due to the inevitable effects of time and operations (frequently exacerbated by improper or ignored maintenance) and the hazards posed by unknown knowables and unknown unknowables interact in undesirable ways. This recognition poses a particularly important limitation on proactive reliability and risk analyses that are conducted before systems are constructed and put in service; in a predictive sense, one can only analyze what one understands or knows.

Frequently, organizations involved in development of a system failure will construct barriers to prevent the failure causation to be traced up the blunt end of the 'spear' of accident causation. The pointed end of the spear involves the system operators – frequently identified as the 'proximate causes'. The blunt end of the spear involves the system organizations including corporate and governmental management and administration that control means, methods, and resources used to organize and operate a given system. Until recently, legal and failure investigation processes focused on the proximate causes in failures – the pointed end of the spear. There have been some recent major exceptions to this focus. The major roles of organizational malfunctions in failure causation have been recognized in court and in failure investigations such as those conducted by the Columbia Accident Investigation Board and the Chemical Safety Board in the investigation of the failure of the British Petroleum Texas City refinery. Organizations exert extremely important influences in development of system failures (Reason 1997; Bea 2000a, 2002; Hopkins 1999, 2000, 2010).

11 Failures in the Macondo Well Risk Assessment and Management

There is sufficient evidence to conclude the Macondo well failure - the blowout - developed because of a cascade of poor decisions involving poor tradeoffs made by the organizations with responsibilities for the quality of the Macondo well project (BP 2010; National Commission 2010; National Academy of Engineering and National Research Council 2010; U.S. Coast Guard – Bureau of Energy Management, Regulation, and Enforcement 2010; Committee on Energy and Commerce 2010; Parsons 2010; Marsh 2010; Table 11.1). Critical things were compromised for the wrong reasons in the wrong ways at the wrong times.

From the outset of the Macondo well project, the hazards, uncertainties, and risks were not properly assessed or managed (Houck 2010). Requirements to address the potentials for a blowout were waived. The consequences of a blowout were evaluated to be "insignificant" (BP 2009a, 2009b, 2009c). The likelihoods and consequences of the individual and multiple failures were dramatically and systematically underestimated. As a result, preventative measures, emergency response, containment, and clean-up processes were inadequate.

The Macondo well failures involve a specific group of people and organizations. However, these failures transcend this specific group of people and organizations. The Macondo well failures involve a national and international industrial – governmental – public enterprise that in the last several decades has embarked on a series of extremely challenging undertakings whose risks and rewards are substantially greater than those previously undertaken. The environments of ultra-deep water combined with those of high pressure – high temperature (HPHT) hydrocarbon reservoirs are extremely challenging and unforgiving – particularly in the northern Gulf of Mexico where the reservoir formations have relatively weak strengths (Anderson, Boulanger 2009; Buller, Bjorkum, Nadeau, and Walderhaug 2005; Neadeau 2010). Compounding these hazards are the complexities of the sub-sea and surface 'hardware' systems that are like those of space exploration systems. There are similar complexities in the 'humanware' systems involving interactions between industry, government, the public, and advocates for the environment. There are similar complexities within each of these human components. When these complex hardware and humanware systems are developed and deployed into unforgiving environments without appropriate safeguards, one should

expect a disaster sooner or later. Available evidence indicates this is what happened during the Macondo well project.

Table 11.1 – Decisions made during the Macondo well drilling and completion that increased risks.

to leave well drilling liner overlaps uncemented
to delay installation of the lock-down for the production casing hanger seal assembly until after the riser mud was circulated out
to use single long string casing instead of liner and tieback
to use minimum positive pressure test on cemented production casing
to not use recommended casing centralizers
to not confirm proper conversion of float equipment
to perform only partial bottoms-up circulation to remove well debris before cementing
to run underbalance test with most of the drill pipe out of the well instead of running a full string to total depth
to not perform cement bond log on basis of cement lift pressures and absence of fluid losses during cementing
to not cement the annulus between production casing and drilling liner
to place sole reliance on float equipment and shoetrack cement to isolate bottom of production casing
to displace drilling mud from riser before setting plug in production casing
to set temporary abandonment plug at 3,300 feet below the seafloor
to use nitrogen in cement mix to lighten the slurry density rather than non-gaseous additives
to not perform proof tests of cement slurry mix to be used in cementing the production casing
to not use MMS approved plan for negative testing
to perform negative testing before cement could have fully cured (based on laboratory test data)
to not verify location of spacer before negative pressure test
to not verify functionality of negative pressure test system before and during negative tests
to perform multiple important simultaneous operations preventing accurate determination of mud volumes
to not properly monitor mud pit volumes and flow out meter during displacement of drill mud with seawater during temporary abandonment
to not perform required maintenance of the blowout preventer
to not resolve conflicting information developed during the negative pressure testing
to use lost circulation material as spacer during drill mud – sea water displacement negative testing temporary abandonment operations
to place emergency alarms and response systems on 'inhibit' – manual mode of operation
to divert well to the mud gas separator rather than overboard

Analyses of currently available evidence indicates the single critical element precipitating this blowout was the undetected entry of high pressure – high temperature 'highly charged' hydrocarbons into the Macondo well. This important change in the 'environment' was then allowed to exploit multiple inherent weaknesses in the system's barriers and defenses to develop a blowout. Once the blowout occurred, additional weaknesses in the system's barriers and defenses were exposed and exploited to develop the Macondo well disaster. Investigations have disclosed an almost identical sequence of developments resulted in the Montara well blowout that occurred 8 months earlier offshore Australia (Montara Commission of Inquiry 2010).

The Mississippi Canyon Block 252 lease and well permitting documentation and lease regulations indicate the primary responsibilities for the Macondo well developments reside with BP

(Hagerty and Ramseur, 2010). As leaseholder, BP is responsible for the quality and reliability of the operations. BP is responsible for the stewardship of the public hydrocarbon resources vis-à-vis the public trust as well as the protection of the environment. As the Federal regulator and trustee of the public resources, the MMS bears primary responsibility for proper oversight of the operations of BP. The experiences since 20 April 2010 clearly show BP and the MMS failed to adequately assess and manage the risks associated with the Macondo well project.

BP as operator and general contractor for the Macondo well project employed a large number of contractors who supplied goods and services used in the Macondo well project. Based on currently available information, it is possible to identify the types of goods and services the contractors were supposed to supply. It is not possible to identify many important specifics associated with the operator - contractor 'interactions' that developed before and during the Macondo well project. However, there is sufficient evidence and testimony to indicate that there were significant problems with the good and services that were actually provided during the Macondo well project and in the interactions between BP and the contractors as the project was developed. As the project was developed, there is evidence that there was significant confusion about responsibilities and authorities. Many critical communication and 'sensemaking' malfunctions were evident. The available evidence indicates the lack of a cohesive and capable well project 'team' (operator, regulator, contractors) had much to do with development of this disaster.

Following the 'roadmap' of previous system failures, the vast majority of RAM malfunctions involved in the Macondo well disaster are attributable to Extrinsic Uncertainties (operating team and organization malfunctions, knowledge development and utilization malfunctions). However, unlike the majority of past system failures, these malfunctions did not become evident during operations and maintenance of the system. They became evident during construction – during the processes of completing the Macondo well for production. However, as for the majority of the past major failures of offshore exploration and production systems, the seeds for the construction phase failure were planted during the concept development and design phases.

Evidence indicates that during the last days of the Macondo well activities, there were significant pressures to save time, decrease costs, and develop early production from this very difficult well – the "well from hell" (USCG – BOEMRE 2010, Committee on Energy & Commerce 2010). The project had taken much longer and cost much more than originally estimated. The final days decisions to complete the exploratory well in preparation for early production and to utilize cost and time savings 'minimum' barrier well structure (long string design) played important roles in development of the blowout. Other subsequent decisions and actions progressively increased the hazards and decreased the defenses against these hazards (Table 11.1). At the end, due to the progressive removal and erosion of protective defenses, when one important barrier was breached the other defenses were not effective in preventing hydrocarbons from entering the well and moving to the surface with disastrous effects.

Subsequent emergency provisions and defenses proved ineffective. For 87 days after the blowout, actions to control the well and protect the environment were not effective. The relief well that was able to intersect the Macondo well and stop the flow of hydrocarbons proved to be the only effective means to control the well. The assessments developed during the well permitting that the likelihoods and consequences of a blowout were not significant led to lack of sufficient preparations for the sequence of failures that developed the Macondo disaster.

The dominant initiating actions that led to the blowout represent operating team (BP and the contractors involved in drilling and completion of the well) commission malfunctions (Marsh 2010, BP 2010, NRC-NAE 2010). The actions were planned and carried out, but had unexpected and undesirable outcomes.

The decisions and actions associated with the last phase placement of the single long string production casing, cementing operations, decisions to run the positive and negative tests on the well soon after the cement had been placed, the decisions to proceed with the work after the pressure tests had not produced unambiguous positive results, the decision to replace the upper portion of the column of drilling mud with sea water with ineffective monitoring of the well fluids before the protective surface plug was set, the decision to offload the drilling mud during the completion operations, the decision to not shut in the well at the first signs of significant well inflow, the decision not to activate the automatic shut down system, and the final fatal decision to not divert the blowing out well overboard; represent a sequence of choices that when they were combined had disastrous consequences.

There were also critical initiating omission malfunctions that were particularly evident during the time period between completion of the displacement of the upper portion of the drill column mud with seawater (about 9:00 PM on April 20th) and the blowout (about 9:50 PM). Failures to properly monitor the well discharges into the mud pit and changes in the well pressures during this time period prevented the drill crew from taking early action to shut-in the well.

As for previous system failures, the dominant contributing factors were organizational. The lack of effective and timely Quality Assurance and Quality Control and Management of Change processes during concept development, design, and well completion operations are evident. The operator's responsibilities for the conduct of safe operations were not satisfied. The Best Available and Safest Technologies were not used. The regulator's responsibilities for effective oversight to assure conduct of safe operations were not satisfied. Pressures to complete the well as soon as possible and minimize costs as much as possible are evident in the cascade of decisions and choices that led to the blowout. Diversion of attention of key personnel on the rig during the time of the completion operations (loss of situational awareness) and the conduct of multiple simultaneous operations were contributing factors that facilitated development of the initiating malfunctions.

Again, as for previous system failures, the dominant compounding factors were organizational. Once the blowout developed, the ineffectiveness of the control procedures, processes, and hardware allowed the triggering actions to propagate into a cascade of failures that developed the Macondo well disaster. The multiple failures of the blowout control equipment, the emergency shutdown systems, the emergency disconnect system, and the emergency alarm systems all had sources founded in organizational and operating team elements that permeated the design, construction, operation, and maintenance of these critical pieces of hardware. These compounding organizational malfunctions contributed significantly to the difficulties associated with subsequent operations to control and contain the escaping hydrocarbons and protect the environment.

The failures of the Macondo well involved failures in all parts of the system including the operating teams, the organizations, the hardware, the procedures, the environments, and the interfaces among the foregoing. Operating teams clearly developed communications malfunctions,

slips, violations (departures from acceptable and accepted practice), knowledge, selection and training, structure and organization, monitoring and controlling malfunctions, and a significant series of mistakes. Similarly, there were multiple organizational malfunctions including breakdowns in communications, culture (gross imbalances between production and protection incentives), planning and preparations (to prevent, arrest, and recover from failures), structure and organization (teamwork among the responsible groups), monitoring and controlling (Quality Assurance and Quality Control, Management of Change, maintenance of important pieces of equipment and hardware), and mistakes (cognitive information processing malfunctions). There were failures in many important hardware components – most of which could be traced to operating team and organizational malfunctions. There were failures in all four of the system performance characteristics including the serviceability, safety, compatibility, and durability—degradations in the performance characteristics developed and were not properly detected, analyzed, and corrected. There were multiple malfunctions in the procedures including their correctness, accuracy, and completeness.

There were multiple RAM breakdowns in proactive, interactive, and reactive system safety 'barriers'. The plans, processes, and resources provided to prevent the multiple failures were not sufficient. From the outset of the planning and permitting processes, the likelihoods and consequences associated with an uncontrolled blowout of the Macondo well were dramatically underestimated. As a result, all of the barriers to prevent, arrest, and control failures were deeply flawed and ineffective.

The proactive plans, processes, and resources provided to interactively arrest developing failures were not sufficient. The interactive Quality Assurance and Quality Control and Management of Change processes – both industrial and governmental – were ineffective. Quality Assurance and Quality Control processes were not effective in the concept development (permit and environmental impact assessment), design (plans for blowout prevention and mitigations of environmental impacts), and construction (signal analysis, monitoring, oversight Management of Change) phases. During completion of the Macondo well, the interactive RAM processes, procedures, and resources to properly detect, analyze, and correct; to arrest the failure were not effective. After the blowout, the reactive barriers were similarly deeply flawed and defective. Reactive RAM control (emergency shutdown, blowout preventer, emergency disconnect), containment (capping, sealing), and mitigation (life and environment protection and clean-up) proved to be ineffective.

The tragic loss of the worker lives and lasting damage to the lives of their family members were one of the severe consequences of these failures. Similarly, there have been important negative short-term and potential longer-term severe negative impacts to the environment and societies directly affected by the failures. There were multiple breakdowns in the emergency shut-down and life-saving processes.

There was one important success in this sequence of failures – saving the lives of the people who were on the Deepwater Horizon after the blowout developed. Heroic actions by those onboard, early responders, and the U.S. Coast Guard saved lives that otherwise would have been part of the consequences of this system disaster.

The Macondo well disaster is firmly rooted in a history that goes back at least three decades. The Macondo well disaster followed a well established roadmap of previous system disasters. Those at the pointed end of this 'spear of disaster' played their sad roles in the causation of the Macondo well

blowout – a cascade of bad decisions (choices, tradeoffs), actions, and inactions. Those along the shaft of the spear of disaster had important influences on what happened at the pointed end of the spear. They supplied the power and resources for this disaster. The MMS and BP led organizations, policies, and practices provided the incentives, means, and measures that facilitated what happened at the pointed end of the spear onboard the Deepwater Horizon. The multiple failures that followed the blowout (control, containment, cleanup) have similar sources. The natural hazards associated with this environment (open ocean; high pressure – high temperature, low-strength reservoirs; toxic and explosive fluids and gases) combined with human and organizational malfunctions to form the 'perfect storm' of the Macondo well disaster.

12 Looking Forward

The Macondo well disaster has provided an important opportunity to develop and implement major improvements in U.S. drilling and production facilities and operations. In this section, a primary focus is on those facilities and operations that present very high risks – the combination of hazards and system complexities pose high likelihoods and consequences of major system failures that if not properly acknowledged, assessed, and managed have potentially major negative impacts on people, property, productivity, resources, and the environment.

These very high risks are associated with four categories of factors: 1) complexities of hardware, software, emergent technologies, and human systems used in these operations, 2) natural hazards posted by the ultra-deepwater marine environment including geologic, oceanographic, and meteorological conditions, 3) hazards posted by the physical properties of hydrocarbon reservoirs, such as high productivities, pressures, temperatures, gas-to-oil ratios, and low strength formations, and 4) the sensitivities of the marine environment to introductions of large quantities of hydrocarbons. There are other comparable very high risk facilities and operations located or to be located in other areas such as the Arctic.

13 Characterizing and Defining Acceptable Risks

A cornerstone for going forward with this important enterprise is development of an effective Technology Delivery System (TDS, Wenk 2010). The TDS has four major components: 1) the public, 2) the governments that represent the public, 3) the industry – commerce that provides goods and services for the public, and 4) the environment – represented by environmental advocates. To be effectively employed, the TDS must develop constructive collaborations between representatives of these four components. The beliefs, values, feelings, and resource allocations provided by these four components need to be focused on effective and sustainable delivery of the proposed technology so that its benefits can be developed with desirable quality and reliability. A key aspect of a successful TDS is the definition and the characterization of what constitutes 'acceptable risks'. These acceptable risks represent a consensus response of the TDS to the question: "how safe is safe enough?"

Ideally, definition and characterization of acceptable risk associated with an engineered system is a social process requiring effective collaboration of the public, their governments, industry and commerce, and representatives of the environment. This collaborative social process has been characterized as a TDS. The goal of this process is to define means and methods to reduce the risks associated with a proposed system from 'unacceptable' to 'acceptable'. As illustrated in Figure 13.1,

the concept of acceptable or risk is part of the principle of ALARP (As Low as Reasonably Practical) (Hartford 2008, International Standards Organization 2009, Malloy and McDonald 2008).

The ALARP principle recognizes there are three broad categories of risk. The first category is Significant Risk – the risk level is so high that society is not prepared to tolerate it – the losses far outweigh any possible benefits from the proposed system. The second category is Tolerable Risk – society deems that the risk is acceptable in view of the benefits obtained by accepting the risk. The third category is Broadly Acceptable Risk – this risk is deemed acceptable by society as a part of normal living (background risk).

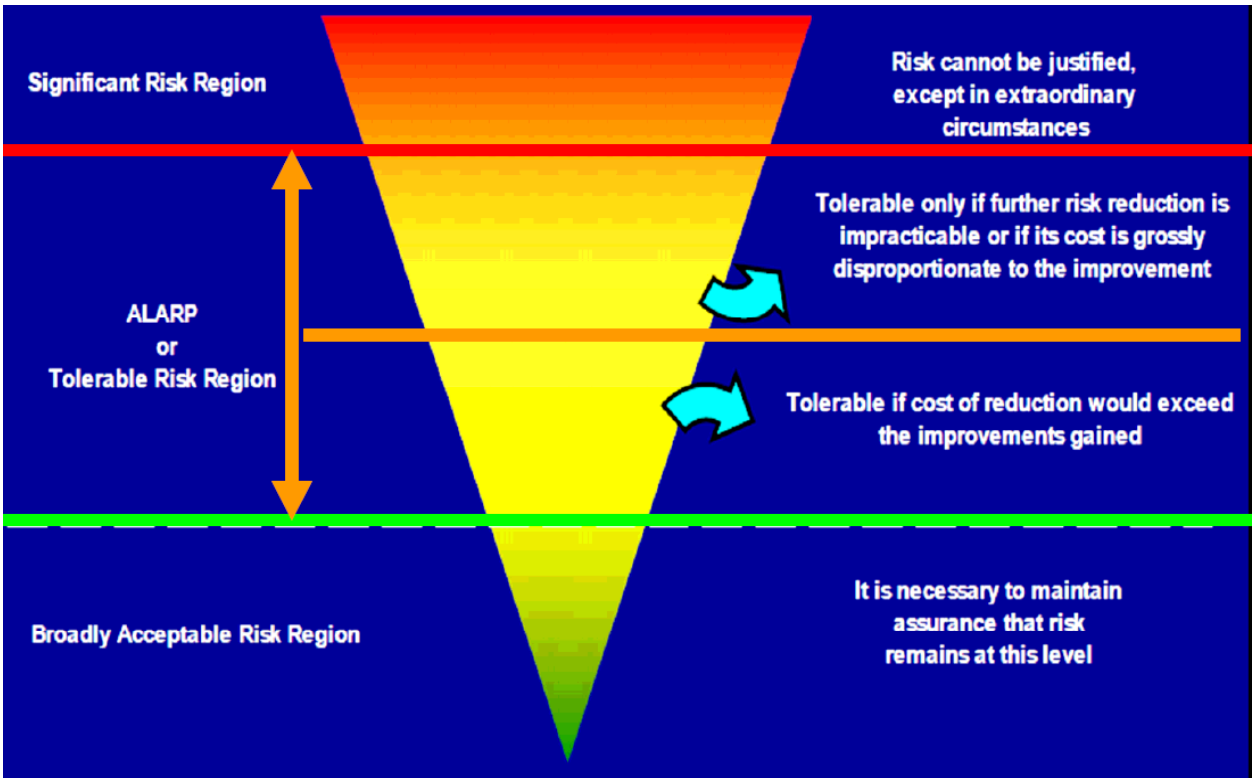

Figure 13.1 – As Low As Reasonably Practical risk regions (after Malloy and McDonald 2008).

The challenge is to define a level of risk that is ALARP in the context of a proposed system. Characterization of the proposed system must include the means and measures that will be provided to assure that the proposed is able to and will achieve performance throughout the life of the system that provides the level of risk that has been defined as tolerable or acceptable. The ALARP risk 'region' is divided into two broad categories: 1) tolerable only if further risk reduction is impracticable or its cost is grossly disproportionate to the improvement, and 2) tolerable if the cost of risk reduction would exceed the improvements gained.

In the context of ALARP, 'cost' is defined as the losses incurred during the processes of developing benefits from a system. Costs can be expressed with a variety of qualitative and quantitative metrics that address monetary, human, environment, and property damage; and production, reputation, and regulatory impacts. Figure13.2 illustrates results from an analysis of monetary evaluations of expected present valued initial costs (CI) and future failure costs (CF)

associated with a particular system. The likelihood of failure (annual) is shown as a function of the consequences of failure. The costs of failure have been 'normalized' by dividing the failure costs by the costs required to reduce the likelihood of failure by a factor of 10 (ΔCI). The consequences of failure have been present valued with an annualized continuous net discount function (PVF, units of years) (Bea 1991).

Three diagonal lines divide the graph (Figure 13.2) into two sections: 1) Fit For Purpose, and 2) Not Fit For Purpose. The line labeled 'Optimum' results from the analysis that defines the minimum present valued expected initial and future costs. The range between the lines labeled 'Marginal' and 'Acceptable' define the upper and lower bounds of the ALARP region (Figure 13.1).

The circle labeled 'LC' is that associated with a Lower Consequence system that has an annual likelihood of failure of 1/1,000 per year. This likelihood of failure is approximately that associated with drilling and production activities in the Gulf of Mexico (Bea 1991, Spouge 1999). The consequences associated with the failure are of the order of $500 million (ΔCI = PVF) (Pritchard and Lacy 2010). Given a CF of the order of $50 billion (Higher Consequence system, HC), an annual likelihood of failure of 1/100,000 per year is indicated – two orders of magnitude lower than associated with the LC system.

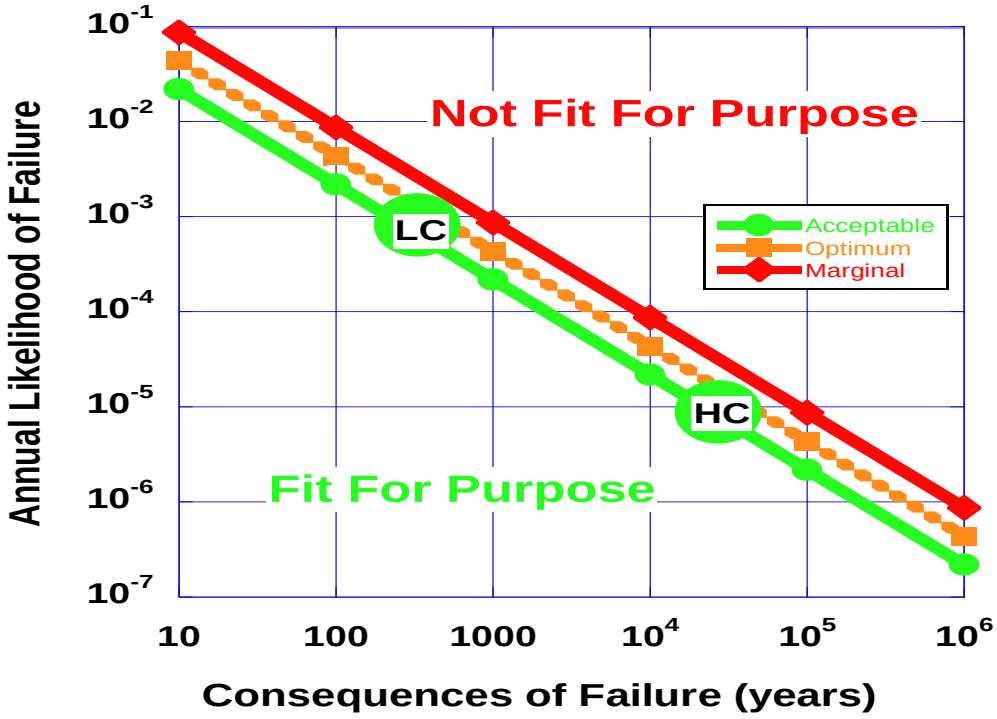

Figure 13.2 – Developing systems to achieve acceptable risks.

The TDS responsibility of the system operator is to demonstrate the system can and will be developed and maintained to enable its performance in the Fit For Purpose region – the operator is responsible for acceptable performance of the system. The TDS responsibility of the system regulator(s) is provision of effective oversight – governance - of the system and its operations to

assure that its performance is acceptable throughout the life of the system. Throughout the life of the system, the operator must demonstrate to the regulator that the system is Fit for Purpose.

Definition of acceptable risks for engineered systems has many precedents. This definition is an important characteristic of 'performance based' or 'goal setting' guidelines for the life-cycle performance characteristics of engineered systems (Hartford 2008, Det Norske Veritas 2010). This is a very important step for engineers because this definition provides quantitative measures of what must be achieved – 'you can't manage what you can't measure'. Such guidelines specify the required performance characteristics associated with a particular system – the goals of its performance. The guidelines do not specify how the goals are to be satisfied. Prescriptive guidelines and regulations specify how performance goals should be met. Prescriptive guidelines can be very useful when appropriate practice has been proven through sufficient experience and uncertainties about the practice and conditions in which the practice will be applied are low. Combinations of goal setting and prescriptive guidelines can provide meaningful goals and methods to help assure that systems develop acceptable performance during the life of the system (Det Norske Veritas 2010, International Standards Organization 2009).

Given these insights, the issue addressed by the Deepwater Horizon Study Group was: "how could operators demonstrate that proposed systems would be able to achieve the acceptable risks that are two orders of magnitude lower than previously achieved?"

The first group proposed proper application of current 'best practices' in hardware and human elements of the systems would enable such targets to be met. There were substantial concerns about what constitutes 'best practices' in both hardware and human elements and how they could be developed and validated before the HC systems were approved for implementation. Of particular concern were the human elements – these would take significant resources to develop.

The second group proposed significant changes – beyond current best practices – would be required to achieve acceptable risk requirements. A combination of quantitative analytical methods and information from prototype demonstration projects would be needed to provide the necessary information and qualifications. These processes were likened to those the commercial power industry confronted as it added nuclear fueled power plants to its inventory of fossil fueled power plants. Similar analogies were made with the U.S. Navy's addition of nuclear powered submarines to the diesel powered submarine fleet (Wenk 2010).

The third group in the DHSG proposed it is currently beyond the industry's abilities to demonstrate such operations can be undertaken with acceptable risks – primarily because of the industry's inabilities to control and mitigate the potential consequences of major system failures. This group posited there were major improvements in hardware and human systems that needed to be developed and proven by industry before such operations should be approved. In addition, this group advanced this 'final frontier' in the ultra-deep waters of the northern Gulf of Mexico and other similar areas provides access to an important public resource that has significant implications for the future generations and security of the United States. These social, economic, and national security interests, as well as safety and environmental considerations, dictate a more measured pace of development consistent with sustainable supplies and best attainable industry practices. This group also posited the requirements for improvements were a function of location – local environmental and social conditions. There would not be a 'one size fits all' set of either acceptable

risk targets or means and methods to demonstrate such targets could be satisfied before and after the operations were approved.

14 Developing Acceptable Risks

Experience with high consequence engineered systems shows that the defined acceptable risks can be developed and maintained when there are sustained efforts to develop hardware and human components that are able to achieve and maintain quality and reliability in the systems during their life-cycles (Figure 7.1) (International Standards Organization 2009). High quality and reliability human components are a prerequisite to realization of high quality and reliability hardware components.

There are three fundamental, complimentary, and interactive approaches to achieving adequate and acceptable quality and reliability in engineered systems:

- Proactive (activities implemented before malfunctions occur),
- Reactive (activities implemented after malfunctions occur), and
- Interactive or real-time. (activities implemented during development of malfunctions)

In the context of these three approaches there are three primary strategies to be employed:

- Reduce incidence of malfunctions,
- Increase detection and correction of malfunctions, and
- Reduce effects of malfunctions.

15 Proactive Approaches and Strategies

The proactive approach attempts to understand a system before it fails (unacceptable quality) in an attempt to identify how it could fail in the future. Measures can then be put in place to prevent the failure or failures that have been anticipated. Proactive approaches include well developed qualitative methods such as HazOp (Hazard Operability) and FMEA (Failure Mode and Effects Analyses) and quantitative methods such as SRA (Structural Reliability Analyses), PRA (Probabilistic Risk Analyses), and QRA (Quantified Risk Analyses)—(Center for Chemical Process Safety, 1989; Spouge, 1999; Moan, 1997). Each of these methods have benefits and limitations (Groeneweg, 1994; Molak, 1997; Apostolakis, et al, 1990; Aven, Porn, 1998; Bier, 1999).

Proactive approaches also include organizational – management improvements and strategies intended to develop Higher Reliability Organizations (HRO). Such organizations are able to operate over long periods of time conducting relatively free error operations and to consistently make good decisions regarding quality and reliability. Creation of HROs is perhaps the most important proactive approach.

Another important proactive approach is the creation of 'robust' engineered systems and similarly robust organizations. Robustness is defined as damage or defect tolerance. Robustness in a system or an organization means it can continue to operate satisfactorily without compromising

fundamental quality and reliability performance characteristics until repairs and/or modifications can be made. These are 'human friendly' systems in the sense that they can tolerate high probability defects and damage that have sources in human and organizational malfunctions. Studies of robustness in engineered systems (Bea, 2000a, 2002) have shown that it takes the combination of four attributes to create a robust engineered system:

- Configuration,
- Ductility,
- Excess capacity, and
- Appropriate correlation (relationships) of components.

Configuration relates to the topology of the system; how elements, components and materials are arranged. Frequently, this has been called 'redundancy'. Configuration goes beyond redundancy so that as elements or members are damaged or defective, that the system is still able to perform acceptably until repairs and modifications can be made. Ductility relates to the ability of the system to shift the paths of demands imposed on the damaged and undamaged elements and components in a system. Ductility relates to the ability of the system materials and elements to 'stretch' without undue loss in capacity. Excess capacity relates to the ability of the system to carry normal demands and excess demands even though some its elements may be damaged or defective. This means that some elements must be intentionally 'over-designed' relative to the normal demands so these elements can carry the demands that are transferred to them when other components or elements are damaged, defective, or fail. Appropriate correlation refers to how the various components in the system relate to and with each other. In a 'series element' system, high degrees of correlation are desirable to prevent 'rogue' elements that do not have desirable robustness characteristics. In a 'parallel element' system, low degrees of correlation are desirable to assure 'independence' (requisite variety) in the elements. Robust systems are not created by overzealous Value Improvement Programs, excessive down-sizing and outsourcing, and excessive initial cost cutting.

The true value of proactive approaches does not lie in their predictive abilities. The true value lies in the disciplined process such approaches can provide to examine the strengths and weaknesses in systems; *the objective is detection and not prediction*. The magnitudes of the quantitative results, if these results have been generated using reasonable models and input information, can provide insights into where and how one might implement effective processes to encourage development of acceptable quality and reliability.

Perhaps the most severe limitation to proactive approaches regards 'knowability'. One can only analyze what one can or does know. Predictability and knowability are the foundation blocks of quantitative analytical models (Apostolakis, et al, 1990; Rasmussen, 1996; Center for Chemical Process Safety, 1989; Spouge, 1999). But, what about the unknowable and the unpredictable? Can we really convince ourselves that we can project into the future of engineered systems and perform analyses that can provide sufficient insights to enable us to implement the measures required to fully assure their quality and reliability? Or are some other processes and measures needed? This fundamental property of unknowability has some extremely important ramifications with regard to application of the ALARP principle (Melchers, 1993; Hessami, 1999)

Studies of HRO (Higher Reliability Organizations) have shed some light on the factors that contribute to errors made by organizations and risk mitigation in HRO. HRO are those

organizations that have operated nearly error free over long periods of time. A wide variety of HRO have been studied over long periods of time. The HRO research has been directed to define what these organizations do to reduce the probabilities of serious errors. The work has shown that the reduction in error occurrence is accomplished by the following (Roberts, 1989; 1993; Weick, 1995; Weick, et al, 1999): 1) Command by exception or negation, 2) Redundancy (robustness – defect and damage tolerance), 3) Procedures and rules, 4) Selection and training, 5) Appropriate rewards and punishment, and 6) Ability of management to 'see the big picture'.

Command by exception (management by exception) refers to management activity in which authority is pushed to the lower levels of the organization by managers who constantly monitor the behavior of their subordinates. Decision making responsibility is allowed to migrate to the persons with the most expertise to make the decision when unfamiliar situations arise (employee empowerment).

Redundancy involves people, procedures, and hardware. It involves numerous individuals who serve as redundant decision makers. There are multiple hardware components that will permit the system to function when one of the components fails. The term redundancy is directed toward identification of the need for organizational 'robustness' – damage and defect tolerance that can be developed given proper configuration (deployment), ductility – ability and willingness to shift demands, and excess capacity (ability to carry temporary overloads).

Procedures that are correct, accurate, complete, well organized, well documented, and are not excessively complex are an important part of HRO. Adherence to the rules is emphasized as a way to prevent errors, unless the rules themselves contribute to error.

HRO develop constant and high quality programs of personnel selection and training. Personnel selection is intended to select people that have natural talents for performing the tasks that have to be performed. Training in the conduct of normal and abnormal activities is mandatory to avoid errors. Training in how to handle unpredictable and unimaginable unraveling of systems is also needed. Establishment of appropriate rewards and punishment that are consistent with the organizational goals is critical; incentives are a key to performance.

HRO organizational structure is defined as one that allows key decision makers to understand the big picture. These decision makers with the big picture perceive the important developing situations, properly integrate them, and then develop high reliability responses.

In recent organizational research performed by Libuser (1994), five prominent failures were addressed including the Chernobyl nuclear power plant, the grounding of the Exxon Valdez, the Bhopal chemical plant gas leak, the mis-grinding of the Hubble Telescope mirror, and the explosion of the space shuttle Challenger. These failures were evaluated in the context of five hypotheses that defined risk mitigating and non-risk mitigating organizations. The failures provided support for the following five hypotheses:

- Risk mitigating organizations will have extensive process auditing procedures. Process auditing is an established system for ongoing checks designed to spot expected as well as unexpected safety problems. Safety drills would be included

in this category as would be equipment testing. Follow ups on problems revealed in prior audits are a critical part of this function.

- Risk mitigating organizations will have reward systems that encourage risk mitigating behavior on the part of the organization, its members, and constituents. The reward system is the payoff that an individual or organization gets for behaving one way or another. It is concerned with reducing risky behavior.
- Risk mitigating organizations will have quality standards that exceed the referent standard of quality in the industry.
- Risk mitigating organizations will correctly assess the risk associated with the given problem or situation. Two elements of risk perception are involved. One is whether or not there was any knowledge that risk existed at all. The second is if there was knowledge that risk existed, the extent to which it was understood sufficiently.
- Risk mitigating organizations will have a strong command and control system consisting of five elements: a) migrating decision making, b) redundancy, c) rules and procedures, d) training, and e) senior management has the big picture.

These concepts have been extended to characterize *how* organizations can organize to achieve high quality and reliability. Effective HRO's are characterized by (Weick, Sutcliffe, Obstfeld, 1999; Weick, Quinn, 1999; Weick, Sutcliffe, 2001):

- Preoccupation with failure – any and all failures are regarded as insights on the health of a system, thorough analyses of near-failures, generalize (not localize) failures, encourage self-reporting of errors, and understand the liabilities of successes.
- Reluctance to simplify interpretations – regard simplifications as potentially dangerous because they limit both the precautions people take and the number of undesired consequences they envision, respect what they do not know, match external complexities with internal complexities (requisite variety), diverse checks and balances, encourage a divergence in analytical perspectives among members of an organization (it is the divergence, not the commonalties, that hold the key to detecting anomalies).
- Sensitivity to operations – construct and maintain a cognitive map that allows them to integrate diverse inputs into a single picture of the overall situation and status (situational awareness, 'having the bubble'); people act thoughtfully and with heed, redundancy involving cross checks, doubts that precautions are sufficient, and wariness about claimed levels of competence; and exhibit extraordinary sensitivity to the incipient overloading of any one of it members - sensemaking.
- Commitment to resilience – capacity to cope with unanticipated dangers after they have become manifest, continuous management of fluctuations, prepare for inevitable surprises by expanding the general knowledge, technical facility, and command over resources, formal support for improvisation (capability to recombine actions in repertoire into novel successful combinations), and simultaneously believe and doubt their past experience.

- Under-specification of structures – avoid the adoption of orderly procedures to reduce error that often spreads them around; avoid higher level errors that tend to pick up and combine with lower level errors that make them harder to comprehend and more interactively complex, gain flexibility by enacting moments of organized anarchy, loosen specification of who is the important decision maker in order to allow decision making to migrate along with problems (migrating decision making); and move in the direction of a garbage can structure in which problems, solutions, decision makers, and choice opportunities are independent streams flowing through a system that become linked by their arrival and departure times and by any structural constraints that affect which problems, solutions and decision makers have access to which opportunities.

On the other side of this coin are LRO (Lower Reliability Organizations). The studies show that these non-HRO's are characterized by a focus on success rather than failure, and efficiency rather than reliability (Weick, Sutcliffe, Obstfeld, 1999; Weick, Sutcliffe, 2001). In a non-HRO the cognitive infrastructure is underdeveloped, failures are localized rather than generalized, and highly specified structures and processes are put in place that develop inertial blind spots that allow failures to cumulate and produce catastrophic outcomes. LRO have little or no robustness. LRO have little or no diversity; they have focused conformity.

Efficient organizations practice stable activity patterns and unpredictable cognitive processes that often result in errors; they do the same things in the face of changing events, these changes go undetected because people are rushed, distracted, careless, or ignorant (Weick, Quinn, 1999). In a non-HRO expensive and inefficient learning and diversity in problem solving are not welcomed. Information, particularly 'bad' or 'useless' information is not actively sought, failures are not taken as learning lessons, and new ideas are rejected. Communications are regarded as wasteful and hence the sharing of information and interpretations between individuals is stymied. Divergent views are discouraged, so that there is a narrow set of assumptions that sensitize it to a narrow variety of inputs.

In a non-HRO success breeds confidence and fantasy, managers attribute success to themselves, rather than to luck, and they trust procedures to keep them appraised of developing problems. Under the assumption that success demonstrates competence, a non-HRO drifts into complacency, inattention, and habituated routines which they often justify with the argument that they are eliminating unnecessary effort and redundancy. Often down-sizing and out-sourcing are used to further the drives of efficiency and insensitivity is developed to overloading and its effects on judgment and performance. Redundancy (robustness or defect tolerance) is eliminated or reduced in the same drive resulting in elimination of cross checks, assumption that precautions and existing levels of training and experience are sufficient, and dependence on claimed levels of competence. With outsourcing, it is now the supplier, not the buyer, who must become preoccupied with failure. But, the supplier is preoccupied with success, not failure, and because of low-bid contracting, often is concerned with the lowest possible cost success. The buyer now becomes more mindless and if novel forms of failure are possible, the loss of a preoccupation with failure makes the buyer more vulnerable to failure. Non-HRO's tend to lean toward anticipation of 'expected surprises', risk aversion, and planned defenses against foreseeable accidents and risks; unforeseeable accidents and risks are not recognized or believed.

Reason (1997) in expanding his work from the individual (Reason, 1990) to the organization, develops another series of important insights and findings. Reason observes that all technological organizations are governed by two primary processes: production and protection. Production produces the resources that make protection possible. Thus, the needs of production will generally have priority throughout most of an organization's life, and consequently, most of those that manage the organization will have skills in production, not protection. It is only after an accident or a near-miss that protection becomes for a short period time paramount in the minds of those that manage an organization. Reason observes that production and protection are dependent on the same underlying organizational processes. If priority is given to production by management and the skills of the organization are directed to maximizing production, then unless other measures are implemented, one can expect an inevitable loss in protection until significant accidents cause an awakening of the need to implement protective measures. The organization chooses to focus on problems that it always has (production) and not on problems it almost never has (major failures and disasters). The organization becomes 'habituated' to the risks it faces and people forget to be afraid: "chronic worry is the price of quality and reliability" (Reason, 1997).

16 Reactive Approaches and Strategies

The reactive approach is based on analysis of the failure or near failures (incidents, near-misses) of a system. An attempt is to made to understand the reasons for the failure or near-failures, and then to put measures in place to prevent future failures of the system. The field of worker safety has largely developed from application of this approach.

This attention to accidents, near-misses, and incidents is clearly warranted. Studies have indicated that generally there are about 100+ incidents, and 10 to 100 near-misses, to every accident (Hale, Wilpert, Freitag, 1997; Rassmussen, Leplat, 1987). The incidents and near-misses can give early warnings of potential degradation in the safety of the system. The incidents and near-misses, if well understood and communicated provide important clues as to how the system operators are able to rescue their systems, returning them to a safe state, and to potential degradation in the inherent safety characteristics of the system. We have come to understand that responses to accidents and incidents can reveal much more about maintaining adequate quality and reliability than responses associated with successes.

Well-developed guidelines have been established for investigating incidents and performing audits or assessments associated with near-misses and accidents (Center for Chemical Process Safety, 1992; Hale, Wilpert, Freitag, 1997). These guidelines indicate that the attitudes and beliefs of the involved organizations are critical in developing successful reactive processes and systems, particularly doing away with 'blame and shame' cultures and practices. It is further observed that many if not most systems focus on 'technical causes' including equipment and hardware. Human – system failures are treated in a cursory manner and often from a safety engineering perspective that has a focus on outcomes of errors (e.g., inattention, lack of motivation) and statistical data (e.g., lost-time accidents) (Reason, 1997; Fischoff, 1975).

Most important, most reactive processes completely ignore the organizational malfunctions that are critically important in contributing to and compounding the initiating events that lead to accidents (Reason, 1997). Finding 'well documented' failures is more the exception than the rule. Most accident investigation procedures and processes have been seriously flawed. The qualifications,

experience, and motivations of the accident assessors are critical; as are the processes that are used to investigate, assess, and document the factors and events that developed during the accident. A wide variety of biases 'infect' the investigation processes and investigators (e.g., confirmation bias, organization bias, reductive bias) (Reason, 1997; Fischoff, 1975).

A primary objective of incident reporting systems is to identify recurring trends from the large numbers of incidents with relatively minor outcomes. The primary objective of near-miss systems is to learn lessons (good and bad) from operational experiences. Near-misses have the potential for providing more information about the causes of serious accidents than accident information systems. Near-misses potentially include information on how the human operators have successfully returned their systems to safe-states. These lessons and insights should be reinforced to better equip operators to maintain the quality of their systems in the face of unpredictable and unimaginable unraveling of their systems.

Root cause analysis is generally interpreted to apply to systems that are concerned with detailed investigations of accidents with major consequences. The author has a fundamental objection to root cause analysis because of the implication that there is a single cause at the root of the accident (reductive bias) (Center for Chemical Process Safety, 1994). This is rarely the case. This is an attempt to simplify what is generally a very complex set of interactions and factors, and in this attempt, the lessons that could be learned from the accident are frequently lost. Important elements in a root cause analysis include an investigation procedure based on a model of accident causation. A systematic framework is needed so that the right issues are addressed during the investigation (Hale, Wilpert, Freitag, 1997; Bea, Holdsworth, Smith, 1996). There are high priority requirements for comprehensiveness and consistency. The comprehensiveness needs to be based on a systems approach that includes error tendencies, error inducing environments, multiple causations, latent factors and causes, and organizational influences. The focus should be on a model of the system factors so that error reduction measures and strategies can be identified. The requirement for consistency is particularly important if the results from multiple accident analyses are to be useful for evaluating trends in underlying causes over time.

There is no shortage of methods to provide a basis for detailed analysis and reporting of incidents, near-misses, and accidents. The primary challenge is to determine how such methods can be introduced into the life-cycle Risk Assessment and Management (RAM) of engineered systems and how their long-term support can be developed (business incentives).

Inspections during construction, operation, and maintenance are a key element in reactive RAM approaches. Thus, development of IMR (Inspection, Maintenance, Repair) programs is a key element in development of reactive management of the quality and reliability of engineered systems (Bea, 1992). Deductive methods involving mechanics based SRA/PRA/QRA techniques have been highly developed (Spouge, 1999; Soares, 1998). These techniques focus on 'predictable' damage that is focused primarily on durability; fatigue, and corrosion degradations. Inductive methods involving discovery of defects and damage are focused primarily on 'unpredictable' elements that are due primarily to unanticipated human and organizational errors such as weld flaws, fit-up or alignment defects, dropped objects, ineffective corrosion protection, and collisions. Reliability Center Maintenance (RCM) approaches have been developed and are continuing be developed to help address both predictable and unpredictable damage and defects (Jones, 1995). Some very significant forward strides have been made in development and implementation of life-cycle IMR database

analysis and communications systems. But, due to expense and cost concerns, and unwillingness or inability of the organization to integrate such systems into their business systems, much of this progress has been short lived.

The reactive approach has some important limitations. It is not often that one can truly understand the causes of accidents. If one does not understand the true causes, how can one expect to put the right measures in place to prevent future accidents? Further, if the causes of accidents represent an almost never to be repeated collusion of complex actions and events, then how can one expect to use this approach to prevent future accidents? Further, the usual reaction to accidents has been to attempt to put in place hardware and equipment that will help prevent the next accident. Attempts to use equipment and hardware to fix what are basic HOF (Human and Organizational Factors) problems generally have not proven to be effective (Reason, 1997). It has been observed that progressive application of the reactive approach can lead to decreasing the accepted 'safe' operating space for operating personnel through increased formal procedures to the point where the operators have to violate the formal procedures to operate the system.

17 Interactive Approaches and Strategies

The third approach is interactive (real-time) engineering and management in which danger or hazards builds up in a system and it is necessary to actively intervene with the system to return it to an acceptable quality and reliability state. *This approach is based on the contention that many aspects that influence or determine the failure of engineered systems in the future are fundamentally unpredictable and unknowable*. These are the incredible, unbelievable, complex sequences of events and developments that unravel a system until it fails. We want to be able to assess and manage these evolving disintegrations. This approach is based on providing systems (including the human operators) that have enhanced abilities to rescue themselves. This approach is based on the observation that people more frequently return systems to safe states than they do to unsafe states that result in accidents.

Engineers can have important influences on the abilities of people to rescue systems and on the abilities of the systems to be rescued by providing adequate measures to support and protect the operating personnel and the system components that are essential to their operations. Quality assurance and quality control (QA/QC) is an example of the real-time approach (Matousek, 1990). QA is done before the activity, but QC is conducted during the activity. The objective of the QC is to be sure that what was intended is actually being carried out.

Two fundamental approaches to improving interactive performance are: 1) providing people support, and 2) providing system support. People support strategies include such things as selecting personnel well suited to address challenges to acceptable performance, and then training them so they possess the required skills and knowledge. Re-training is important to maintain skills and achieve vigilance. The cognitive skills developed for interactive RAM degrade rapidly if they are not maintained and used (Weick, 1995; Klein, 1999; Knoll, 1986; Weick, Sutcilffe, 2001).

Interactive teams should be developed that have the requisite variety to recognize and manage the challenges to quality and reliability and have developed teamwork processes so the necessary awareness, skills and knowledge are mobilized when they are needed. Auditing, training, and re-training are needed to help maintain and hone skills, improve knowledge, and maintain readiness (Center for Chemical Process Safety, 1993). Interactive RAM teams need to be trained in problem

'divide and conquer' strategies that preserve situational awareness through organization of strategic and tactical commands and utilization of 'expert task performance' (specialists) teams (Klein, 1999). Interactive teams need to be provided with practical and adaptable strategies and plans that can serve as useful 'templates' in helping manage each unique crisis. These templates help reduce the amount and intensity of cognitive processing that is required to manage the challenges to quality and reliability.

Improved system support includes factors such as improved maintenance of the necessary critical equipment and procedures so they are workable and available as the system developments unfold. Data systems and communications systems are needed to provide and maintain accurate, relevant, and timely information in 'chunks' that can be recognized, evaluated, and managed. Adequate 'safe haven' measures need to be provided to allow interactive RAM teams to recognize and manage the challenges without major concerns for their well being. Hardware and structure systems need to be provided to slow the escalation of the hazards, and re-stabilize the system.

One would think that improved interactive system support would be highly developed by engineers. This does not seem to be the case (Kletz, 1991). A few practitioners recognize its importance, but generally it has not been incorporated into general engineering practice or guidelines. Systems that are intentionally designed to be stabilizing (when pushed to their limits, they tend to become more stable) and robust (sufficient damage and defect tolerance) are not usual. Some provisions have been made to develop systems that slow the progression of some system degradations.

Effective early warning systems and 'status' information and communication systems have not received the attention they deserve in providing system support for interactive RAM. Systems need to be designed to clearly and calmly indicate when they are nearing the edges of safe performance. Once these edges are passed, multiple barriers need to be in place to slow further degradation and there should be warnings of the breaching of these barriers. More work in this area is definitely needed.

Reason (1997) suggested that latent problems with insufficient quality (failures, accidents) in technical systems are similar to diseases in the human body:

> *"Latent failures in technical systems are analogous to resident pathogens in the human body which combine with local triggering factors (i.e., life stresses, toxic chemicals and the like) to overcome the immune system and produce disease. Like cancers and cardiovascular disorders, accidents in defended systems do not arise from single causes. They occur because of the adverse conjunction of several factors, each one necessary but not sufficient to breach the defenses. As in the case of the human body, all technical systems will have some pathogens lying dormant within them."*

Reason developed eight assertions regarding error tolerance in complex systems:

- The likelihood of an accident is a function of the number of pathogens within the system.
- The more complex and opaque the system, the more pathogens it will contain.
- Simpler, less well-defended systems need fewer pathogens to bring about an accident.

- The higher a person's position within the decision-making structure of the organization, the greater is his or her potential for spawning pathogens.
- Local pathogens or accident triggers are hard to anticipate.
- Resident pathogens can be identified proactively, given adequate access and system knowledge.
- Efforts directed at identifying and neutralizing pathogens are likely to have more safety benefits than those directed at minimizing active failures.
- Establish diagnostic tests and signs, analogous to white cell counts and blood pressure, that give indications of the health or morbidity of a high hazard technical system.

The single dominant cause of system design related failures has been errors committed, contributed, and/or compounded by the organizations that were involved in and with the systems. At the core of many of these organization based errors was a culture that did not promote quality and reliability in the design process. The culture and the organizations did not provide the incentives, values, standards, goals, resources, and controls that were required to achieve adequate quality.

Loss of corporate memory also has been involved in many cases of system failures. The painful lessons of the past were lost and the lessons were repeated with generally even more painful results. Such loss of corporate memory are particularly probable in times of down-sizing, out-sourcing, and mergers.

The second leading cause of system failures is associated with the individuals that comprise the design team. Errors of omission and commission, violations (circumventions), mistakes, rejection of information, and incorrect transmission of information (communications) have been dominant causes of failures. Lack of adequate training, time, and teamwork or back-up (insufficient redundancy) has been responsible for not catching and correcting many of these errors (Bea, 2000b).

The third leading cause of system failures has been errors embedded in procedures. Traditional and established ways of doing things when applied to engineered systems that 'push the envelope' have resulted in a multitude of system failures. There are many cases where such errors have been embedded in design guidelines and codes and in computer software used in design. Newly developed, advanced, and frequently very complex design technology applied in development of design procedures and design of engineered systems has not been sufficiently debugged and failures (compromises in quality) have resulted.

This insight indicates the priorities of where one should devote attention and resources if one is interested in improving and assuring sufficient quality in the design of engineered systems (Bea, 2000b):

- Organizations (administrative and functional structures),
- Operating teams (the design teams),
- Procedures (the design processes and guidelines),
- Robust systems, and

- Life-cycle engineering of 'human friendly' systems that facilitate construction, operation, maintenance, and decommissioning.

Formalized methods of QA/QC take into account the need to develop the full range of quality attributes in engineered systems including serviceability, safety, durability, and compatibility. QA is the proactive element in which the planning is developed to help preserve desirable quality. QC is the interactive element in which the planning is implemented and carried out. QA/QC measures are focused both on error prevention and error detection and correction (Harris, Chaney, 1969). There can be a real danger in excessively formalized QA/QC processes. If not properly managed, they can lead to self-defeating generation of paperwork, waste of scarce resources that can be devoted to QA/QC, and a minimum compliance mentality.

In design, adequate QC (detection, correction) can play a vital role in assuring the desired quality is achieved in an engineered system. Independent, third-party verification, if properly directed and motivated, can be extremely valuable in disclosing embedded errors committed during the design process. In many problems involving insufficient quality in engineered systems, these embedded errors have been centered in fundamental assumptions regarding the design conditions and constraints and in the determination of loadings or demands that will be placed on the system. These embedded errors can be institutionalized in the form of design codes, guidelines, and specifications. It takes an experienced outside viewpoint to detect and then urge the correction of such embedded errors (Klein, 1999). The design organization must be such that identification of potential major problems is encouraged; the incentives and rewards for such detection need to be provided.

It is important to understand that adequate correction does not always follow detection of an important or significant error in design of a system. Again, QA/QC processes need to adequately provide for correction after detection. Potential significant problems that can degrade the quality of a system need to be recognized at the outset of the design process and measures provided to solve these problems if they occur.

The elements of organizational sensemaking are critical parts of an effective QA/QC process, and in particular, the needs for requisite variety and experience. This is a need for background and experience in those performing the QA/QC process that matches the complexity of the design being checked. Provision of adequate resources and motivations are also necessary, particularly the willingness of management and engineering to provide integrity to the process and to be prepared to deal adequately with 'bad news'.

18 Implementation

Those responsible for the development and creation of engineered systems, the associated regulatory agencies, their engineers, managers, and operating staffs have much to be proud of. There is a vast international infrastructure of engineered systems that supply much needed goods and services to the societies they serve. This paper addresses the issues associated with helping achieve desirable quality and reliability of engineered systems during their life cycles. The primary challenge that is addressed is not associated with the traditional engineering technologies that have been employed in the creation of these systems. History has shown that this is not the challenge. Rather,

the primary challenge that is addressed is associated with the human and organizational aspects of these systems.

It should also be apparent to all concerned with the quality and reliability of engineered systems that organizations (industrial and regulatory) have pervasive influences on the assessment and management of threats to the quality and reliability of engineered systems. Industrial and governmental management's drives for greater productivity and efficiency need to be tempered with the need to provide sufficient protections to assure adequate quality and reliability.

The threats to adequate quality and reliability in systems emerge slowly. It is this slow emergence that generally masks the development of the threats to quality and reliability. Often, the participants do not recognize the emerging problems and hazards. They become risk habituated and loose their wariness. Often, emerging threats are not clearly recognized because the goals of quality and reliability are subjugated to the goals of production and profitability. This is a problem, because there must be profitability to have the necessary resources to achieve quality and reliability. Perhaps, with present high costs of lack of quality and reliability, these two goals are not in conflict. Quality and reliability can help lead to production and profitability. One must adopt a long term view to achieve the goals of quality and reliability, and one must wait on production and profitability to follow. However, often we are tempted for today, not tomorrow.

19 References and Recommended Reading

Anderson, R.N. and Boulanger, A., 2009. *Prospectivity of the Ultra-Deepwater Gulf of Mexico*, Lamont-0Dougherty Earth Observatory, Columbia University.

Apostolakis, GE, Mancini, G, van Otterloo, RW, & Farmer, FR (Eds), 1990. *Reliability Engineering & System Safety*, Elsevier, London.

Aven, T, & Porn K, 1998. Expressing and Interpreting the Results of Quantitative Risk Analysis: Review and Discussion, *Reliability Engineering and System Safety*, Vol. 61, Elsevier Science Limited, London, UK, 1998.

Bea, RG, 1974. Selection of Environmental Criteria for Offshore Platform Design, *J. Petroleum Technology*, Society of Petroleum Engineers, Richardson, Texas, 1206-1214.

Bea, RG, 1975. Development of Safe Environmental Criteria for Offshore Structures, *Proceedings Oceanology International Conference*, Brighton, UK.

Bea, RG, 1991. Offshore Platform Reliability Acceptance Criteria," J. of Drilling Engineering, Society of Petroleum Engineers, Richardson, TX.

Bea RG, 1992. *Marine Structural Integrity Programs (MSIP),* Ship Structure Committee, SSC-365, Washington, DC.

Bea RG, 1996a. Human and Organization Errors in Reliability of Offshore Structures, *J. of Offshore Mechanics and Arctic Engineering*, American Society of Mechanical Engineers, New York, Nov. – Dec. 1996.

Bea RG, 1996b. Quantitative & Qualitative Risk Analyses – The Safety of Offshore Platforms, *Proceedings of the Offshore Technology Conference*, OTC 8037, Society of Petroleum Engineers, Richardson, Texas.

Bea, RG, 2000a. *Achieving step change in Risk Assessment & Management (RAM),* Centre for Oil & Gas Engineering, http://www.oil-gas.uwa.edu.au, University of Western Australia, Nedlands, WA.

Bea RG, 2000b. Performance Shaping Factors in Reliability Analysis of Design of Offshore Structures, *J. of Offshore Mechanics and Arctic Engineering*, Vol. 122, American Society of Mechanical Engineers, New York, NY.

Bea, RG, 2002, Human and Organizational Factors in Design and Operation of Deepwater Structures, Proceedings Offshore Technology Conference, OTC 14293, Society of Petroleum Engineers, Richardson, TX.

Bea, RG & Lawson, RB, 1997. *Stage-II Analysis of Human and Organizational Factors*, Report to JIP on Comparative Evaluation of Minimum Structures and Jackets, Marine Technology & Development Group, University of California at Berkeley.

Bea, RG, Brandtzaeg, A. & Craig, MJK, 1998. Life-Cycle Reliability Characteristics of Minimum Structures, *Journal of Offshore Mechanics and Arctic Engineering*, Vol. 120, American Society of Mechanical Engineers, New York, NY.

Bea, RG, Holdsworth, RD, and Smith, C (Eds.) (1996). *Proceedings 1996 International Workshop on Human Factors in Offshore Operations*, American Bureau of Shipping, Houston, Texas.

Bier, VM, 1999. *Challenges to the Acceptance of Probabilistic Risk Analysis*, Risk Analysis, Vol. 19, No. 4.

BP, 2009a, *Initial Exploration Plan, Mississippi Canyon Block 252, OCS-G-32306*, BP Exploration & Production Inc., Houston, TX.

BP, 2009b, *Application for Permit to Drill a New Well*, Form MMS 123A/123S, Lease G32306, Area/Block MC 252.

BP, 2009c, *BP Gulf of Mexico Regional Oil Spill Response Plan*, The Response Group, Houston, TX.

BP, 2010. *Deepwater Horizon Accident Investigation Report*, September.

Buller, A.N., Bjorkum, P.A., Nadeau, P., and Walderhaug, 2005. *Distribution of Hydrocarbons in Sedimentary Basins*, Research & Technology Memoir No. 7, Statoil ASA, Stavanger, Norway.

Carnes, W.E., 2010, Highly Reliable Governance of Socio-technical Systems, Working Paper, Deepwater Horizon Study Group, Center for Catastrophic Risk Management, University of California Berkeley.

Center for Chemical Process Safety, 1989. *Guidelines for Technical Management of Chemical Process Safety*, American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety, 1992. *Guidelines for Investigating Chemical Process Incidents*, American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety, 1993. *Guidelines for Auditing Process Safety Management Systems*, American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety, 1994. *Guidelines for Preventing Human Error in Process Safety*, American Institute of Chemical Engineers, New York.

Committee on Energy and Commerce, 2010. *Testimony Transcripts and Documents*, Legislative Hearing on Legislation to Respond to the BP Oil Spill and Prevent Future Oil Well Blowouts, Congress of the United States, House of Representatives, Washington DC.

Det Norske Veritas, 2010, *Key Aspects of an Effective U.S. Offshore Safety Regime*, DNV Position Paper, Houston, TX.

Dougherty, EM Jr & Fragola, JR, 1986. *Human Reliability Analysis*, John Wiley & Sons, New York.

Dhrenberg, S.N., Nadeau, P.H., and Steen, O., 2008. *A Megascale View of Reservoir Quality in Producing Sandstones from the Offshore Gulf of Mexico,* American Association of Petroleum Geologists Bulletin, Vol. 92, No. 2, New York.

Fischhoff B, 1975. Hindsight Does Not Equal Foresight: The Effect of Outcome Knowledge on Judgment Under Uncertainty, *J. of Experimental Psychology*, *Human Perception, and Performance*, Vol. 1, New York.

Gertman, DI & Blackman, HS, 1994. *Human Reliability & Safety Analysis Data Handbook*, John Wiley &Sons, New York.

Groenewg, J, 1994. *Controlling the Controllable, The Management of Safety*, DSWO Press, Leiden University, The Netherlands.

Haber SB, O'Brien JN., Metlay, DS, & Crouch DA, 1991. *Influence of Organizational Factors on Performance Reliability - Overview and Detailed Methodological Development*, U. S. Nuclear Regulatory Commission, NUREG/CR-5538, Washington, DC.

Hagerty, C.L, Ramseur, J.L. 2010, *Deepwater Horizon Oil Spill: Selected Issues for Congress*, Congressiional Research Service, Washington. DC.

Hale A, Wilpert B, & Freitag M, 1997. *After The Event, From Accident to Organizational Learning,* Pergamon Press, Elsevier Sciences Ltd., Oxford, UK.

Harris D, & Chaney F, 1969. *Human Factors in Quality Assurance*, John Wiley and Sons, New York.

Hartford, D.N.D., 2008. *Legal Framework Considerations in the Development of Risk Acceptance Criteria*, Structural Safety, Elsevier Ltd, London.

Hessami AG,1999. Risk Management: A Systems Paradigm, *Systems Engineering*, John Wiley & Sons, London, UK, 1999.

Hopkins, A. ,1999. *Managing Major Hazards – The Lessons of the Moura Mine Disaster*, Allen & Unwin, St Leondards NSW, Australia.

Hopkins, A.., 2000). *Lessons From Longford – The Esso Gas Plant Explosion*, CCH Australia Limited, Sydney NSW, Australia.

Hopkins, A., 2010. *Failure to Learn – The BP Texas City Refinery Disaster,* CCH Australia Limited, Sydney NSW, Australia.

Houck, O.A., 2010. *Worst Case and the Deepwater Horizon Blowout: There Ought to Be a Law*, Environmental Law Reporter.

International Standards Organization, 1994a. *ISO 9000 Series, Quality Management and Quality Assurance Standards*, British Standards Inst. Publication, London, UK.

International Standards Organization, 1994b. *Quality Systems - Model for Quality Assurance in Design / Development, Production, Installation, and Servicing*, ISO 9001, London, UK.

International Standards Organization, 1994c. *Health, Safety, and Environmental Management Systems*, Technical Committee ISO/TC 67, Materials, Equipment and Offshore Structures for Petroleum

and Natural Gas Industries, Sub-Committee SC 6, Processing Equipment and Systems, London, UK.

International Standards Organization, 2009. *Risk Management – Risk Assessment Techniq*ues, Edition 1.0, IEC/ISO, Paris.

Jones RB, 1995. *Risk-Based Management – A Reliability Centered Approach*, Gulf Publishing Co., Houston, Texas.

Kirwan B, 1994. *A Guide to Practical Human Reliability Assessment*, Taylor & Francis, London, UK.

Klein, G, 1999. *Sources of Power*, MIT Press, Cambridge, Massachusetts, 1999.

Kletz T, 1991. *An Engineer's View of Human Error*, Institution of Chemical Engineers, Rugby, UK.

Knoll F, 1986. Checking Techniques, *Modeling Human Error in Structural Design and Construction*, AS Nowak (Ed.), American Society of Civil Engineers, Herndon, Virginia.

Kontogiannis T, & Lucas D, 1990. *Operator Performance Under High Stress: An Evaluation of Cognitive Modes, Case Studies and Countermeasures*, Report No. R90/03, Nuclear Power Engineering Test Center, Tokyo, Japan, Human Reliability Associates, Dalton, Wigan, Lancashire, UK.

Libuser, C, 1994. *Managing Organizations to Achieve Risk Mitigation*, PhD Dissertation, Andersen School of Business, University of California, Los Angeles.

Montara Commission of Iinquiry, 2010, *Report of the Montara Commission of Inquiry*, Commonwealth Copyright Administration, Attorney General's Department, Barton ACT, Australia.

Malloy, K.P. and McDonald, P. 2008, *A Probabilistic Approach to Risk Assessment and Managed Pressure Drilling in Offshore Applications,* MOHR Engineering Division, Stress Engineering Srvices Inc., Report to Technology Assessment and Research Study 582, U.S. Minerals Management Service, Herndon, VA.

Marsh, G. 2010. *Causative Technical and Operational Elements of Deepwater Horizon Blowout*, Working Paper, Deepwater Horizon Study Group, Center for Catastrophic Risk Management, University of California Berkeley, December.

Matousek M, 1990. Quality Assurance, *Engineering Safety*, D. Blockley (Ed.), McGraw-Hill Book Co., London, UK.

Melchers RE, 1993. *Society, Tolerable Risk and the ALARP Principle*, Proceedings of the Conference on Probabilistic Risk and Hazard Assessment, RE Melchers and MG Stewart (Eds.), The University of Newcastle, N.S.W., Australia,.

Molak V (Ed), 1997. *Fundamentals of Risk Analysis and Risk Management*, CRC Lewis Publishers, New York, 1997.

Nadeau, P.H. 2010. *Earth's Energy Golden Zone: A Triumph of Mineralogical Research*, The Mineralogical Society, Macaulay Insitute.

National Commission (2010). *Preliminary Conclusions – Technical, Preliminary Conclusions – Managerial*, Documents Produced for Hearings on November 8 and 9, Washington DC.

National Academy of Engineering and National Research Council (NAE – NRC) (2010), *Interim Report on Causes of the Deepwater Horizon Oil Rig Blowout and Ways to Prevent Such Events*, November 16, Washington DC.

Parsons, P. 2010. *The Macondo Well,* Energy Training Resources, Houston, TX.

Pritchard, D. and Lacy, K., 2010, Deepwater Well Complexity – The New Domain, Working Paper, Deepwater Horizon Study Group, Center for Catastrophic Risk Management, University of California Berkeley.

Rasmussen J, 1996. Risk Management, Adaptation, and Design for Safety, *Future Risks and Risk Management*, N. E. Sahlin and B. Brehemer (Eds.), Dordrecht, Kluwer Publishers.

Rasmussen J., Duncan K, & Leplat J. (Eds), 1987. *New Technology and Human Error*, John Wiley & Sons, New York.

Reason J, 1990. *Human Error*, Cambridge University Press, London, UK.

Reason J, 1997. *Managing the Risks of Organizational Accidents*, Ashgate Publishers, Aldershot, UK.

Roberts KH, 1989. *New Challenges in Organizational Research: High Reliability Organizations,* Industrial Crisis Quarterly, Vol. 3, Elsevier Science Publishers, Amsterdam, the Netherlands.

Roberts, KH (Ed), 1993. *New Challenges to Understanding Organizations*, McMillan Publishing Co., New York.

Rochlin GI, 1997. *Trapped in the Net: The Unanticipated Consequences of Computerization,* Princeton University Press, Princeton, New Jersey.

Spouge J, 1999. *A Guide to Quantitative Risk Assessment for Offshore Installations*, CMPT Publication 99/100, ISBN I 870553 365, London, UK.

Stewart MG. & Melchers RE, 1988. Checking Models in Structural Design, *J. of Structural Engineering*, Vol. 115, No. 17, American Society of Civil Engineers, Herndon, Virginia.

Swain AD. & Guttman, HE, 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U. S. Nuclear Regulatory Commission, Washington, DC.

Taleb, NN, 2007, *The Black Swan, The Impact of the Highly Improbable*, Random House, NY.

U.S. Coast Guard and Bureau of Energy Management, Regulation, and Enforcement (USCG – BOEMRE), Deepwater Horizon Joint Investigation, Transcripts and Documents from Hearings Held May – November 2010.

Weick, KE, 1995. *Sensemaking in Organizations*, Sage Publishers, Thousand Oaks, CA, 1995.

Weick, KE, 1999. Organizing for High Reliability: Processes of Collective Mindfulness, *Research in Organizational Behavior*, Vol. 21, JAI Press Inc.

Weick KE, 2000. The Neglected Context of Risk Assessment – A Mindset for Method Choice, *Risk Management in the Marine Transportation System,* Transportation Research Board, National Research Council, Washington, DC.

Weick, KE & Quinn, RE, 1999. Organizational Change and Development, *Annual Review of Psychology*, New York.

Weick, KE, Sutcliffe, KM, and Obstfeld, D, 1999. Organizing for High Reliability: Processes of Collective Mindfulness, *Research in Organizational Behavior*, Staw and Sutton (Eds.), Research in Organizational Behavior, JAI Press, Vol 21, Greenwich, CT.

Weick, KE & Sutcliffe, KM, 2001. *Managing the Unexpected*, Jossey-Bass, San Francisco, CA.

Wenk E Jr, 1986. *Tradeoffs, Imperatives of Choice in a High-Tech World*, The Johns Hopkins University Press, Baltimore, MD.

Wenk, E. Jr, 2010. *How Safe is Safe?* Working Paper, Deepwater Horizon Study Group, Center for Catastrophic Risk Management, University of California Berkeley.

Woods DD, 1990. Risk and Human Performance: Measuring the Potential for Disaster, *Reliability Engineering and System Safety*, Vol. 29, Elsevier Science Publishers Ltd., UK.

Woods. DD, Johannesen, LJ, Cook, R.I, and Sarter, NB, 1994, Behind human error: Cognitive systems, computers, and hindsight, Wright-Patterson Air Force Base, OH, Crew System Ergonomics Information Analysis Center.

Wu JS, Apostolakis GE, & Okrent D, 1989. On the Inclusion of Organizational and Management Influences in Probabilistic Safety Assessments of Nuclear Power Plants, *Proceedings of the Society for Risk Analysis*, New York, 1989.