THE MACONDO BLOWOUT

3rd Progress Report

Image Source: United States Coast Guard Visual Information Gallery

The Deepwater Horizon Study Group was formed by members of the Center for Catastrophic Risk Management (CCRM) in May 2010 in response to the explosion and fire at Deepwater Horizon well on April 20, 2010. A fundamental premise in the DHSG work is: we look back to understand the why's and how's of this disaster so we can better understand how best to go forward. The goal of the DHSG work is defining how to best move forward – assessing what major steps are needed looking forward to develop our national oil and gas resources in a reliable, responsible, and accountable manner.

December, 5, 2010

Table of Contents

Deepwater Horizon Study Group Progress Report 3

During May 2010, members of the Center for Catastrophic Risk Management (CCRM[1]) at the University of California Berkeley formed the Deepwater Horizon Study Group (DHSG[2]). The DHSG is an international group (60 members) of experienced professionals, experts, and scholars who have extensive experience in offshore oil and gas facilities and operations, drilling and reservoir engineering, geology, accident investigations, management, organizational behavior, government regulatory affairs, legislative – legal processes, marine ecology and environmental science, and risk assessment and management. The DHSG members have volunteered their time without compensation. A list of the DHSG members who have approved publication of their names and affiliations is provided in Appendix A. The DHSG would like to express its gratitude to all of its members, collaborators and supporters for their contributions to this important work.

The DHSG has three major goals: (1) to produce a final report documenting results from the studies of the failures of the Deepwater Horizon Mississippi Canyon Block 252 well drilling project and the subsequent containment and mitigation activities; 2) to serve as advisors to the public, governments, industry, and environmental advocates who want timely, unbiased well-informed insights and information regarding the failures and what should be done to reduce the future likelihoods and consequences associated with such failures in ultra deepwater and arctic hydrocarbon resource developments, and 3) to develop a central archive and communications system for data and information accumulated during the investigations that can be used by researchers and others for subsequent analysis and documentation of their investigations, studies, and reports.

The first progress report (May 24, 2010) concluded:

> *"This disaster was preventable had existing progressive guidelines and practices been followed. This catastrophic failure appears to have resulted from multiple violations of the laws of public resource development, and its proper regulatory oversight."*

The second progress report (July 15, 2010) concluded:

> *"…these failures (to contain, control, mitigate, plan, and clean-up) appear to be deeply rooted in a multi-decade history of organizational malfunction and shortsightedness. There were multiple opportunities to properly assess the likelihoods and consequences of organizational decisions (i.e., Risk Assessment and Management) that were ostensibly driven by the management's desire to "close the competitive gap" and improve bottom-line performance. Consequently, although there were multiple chances to do the right things in the right ways at the right times, management's perspective failed to recognize and accept its own fallibilities despite a record of recent accidents in the U.S. and a series of promises to change BP's safety culture."*

The first and second progress reports are available for downloading from the DHSG web site.[2]

[1] http://ccrm.berkeley.edu/
[2] http://ccrm.berkeley.edu/deepwaterhorizonstudygroup/dhsg_reportsandtestimony.shtml

The third progress report (December 1, 2010) concludes:

"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)."

"Analysis of the available evidence indicates that when given the opportunity to save time and money – and make money – tradeoffs were made for the certain thing – production – because there were perceived to be no downsides associated with the uncertain thing – failure caused by the lack of sufficient protection. Thus, as a result of a cascade of deeply flawed failure and signal analysis, decision-making, communication, and organizational - managerial processes, safety was compromised to the point that the blowout occurred with catastrophic effects."

"At the time of the Macondo blowout, BP's corporate culture remained one that was embedded in risk-taking and cost-cutting – it was like that in 2005 (Texas City), in 2006 (Alaska North Slope Spill), and in 2010 ("The Spill"). Perhaps there is no clear-cut "evidence" that someone in BP or in the other organizations in the Macondo well project made a conscious decision to put costs before safety; nevertheless, that misses the point. It is the underlying "unconscious mind" that governs the actions of an organization and its personnel. Cultural influences that permeate an organization and an industry and manifest in actions that can either promote and nurture a high reliability organization with high reliability systems, or actions reflective of complacency, excessive risk-taking, and a loss of situational awareness."

Background for these conclusions is provided in Appendices B, C, and F.

Based on currently available data and information, the following summarizes the major findings and conclusions developed by the DHSG since the second progress report was issued. These findings address 'going forward' challenges associated with the Macondo well blowout.

Finding 1 - The oil and gas industry has embarked on an important 'next generation' series of exploration and production operations in the ultra-deep waters of the northern Gulf of Mexico (Appendix D). These operations pose risks (likelihoods and consequences of major failures) much greater than generally recognized. The significant increases in risks are due to: (1) complexities of hardware and human systems and emergent technologies used in these operations, (2) hazards posed by the ultra-deep water marine environment (geologic, oceanographic, metrological), (3) hazards posed by the hydrocarbon reservoirs (high productivities, pressures, temperatures, gas – oil ratios, and low strength formations),[3] and (4) sensitivity of the marine environment to introduction of large quantities of hydrocarbons (Appendix E).

[3] A.N. Buller, P.A. Bjorkum, P. Nadeau, and O. Walderhaug (2005), "Distribution of Hydrocarbons in Sedimentary Basins," Research & Technology Memoir No. 7, Statoil ASA, Norway. S.N. Ehrenberg, P.H. Nadeau, and O. Steen (2008), "A megascale view of reservoir quality in producing sandstones from the offshore Gulf of Mexico," AAPG Bulletin, V. 92, No. 2, New York. R.N. Anderson and A. Boulanger (2009), "Prospectivity of the Ultra-Deepwater Gulf of Mexico," Lamont-Doherty Earth Observatory, Columbia University. P.H. Nadeau (2010), "Earth's energy 'Golden zone': A triumph of mineralogical research," The Mineralogical Society, Macaulay Institute.

Finding 2 - The Macondo well project failures have demonstrated that the consequences of major offshore oil and gas 'system' failures can be several orders of magnitude greater than associated with previous generations of these activities. If the risks of major system failures are to be As Low As Reasonably Practicable, the likelihoods of major failures (e.g. uncontrolled blowouts, production operations explosions and fires) must be two or more orders of magnitude lower than in the BP Mocando project and that may prevail in others planned or underway (Appendix F).

Finding 3 – The Macondo well project failures provide important opportunities to re-examine the strategies and timing for development of important non-renewable product and energy resource. 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.[4] 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.

Finding 4 – Major 'step change' improvements are required to allow offshore exploration, production, and transportation operations in the ultra-deepwater portions of the northern Gulf of Mexico to develop acceptable risks and benefits from this enterprise. Future development of these important public resources require an advanced high competency collaborative industrial - governmental - institutional enterprise based on development of high reliability technical, organization, management, governance, and institutional systems (Appendices F - K).

The DHSG has developed a series of more than thirty Working Papers that provide additional background for these findings and conclusions. These Working Papers are being finalized and will be provided on the DHSG web site during January 2011.

The DHSG will continue its investigations and studies. During the Spring of 2011, the DHSG will issue its final report and provide a web-based public archive for the data, documents, and information obtained and developed during this study.

Professor Robert Bea, PhD, PE
Center for Catastrophic Risk Management
Deepwater Horizon Study Group
212 McLaughlin Hall
University of California Berkeley
Berkeley, CA 94556

[4] International Energy Agency, "World Energy Outlook 2010," Paris, France.

Appendix A

Deepwater Horizon Study Group Members and Affiliations

Thomas Azwell, Doctoral Student, Researcher, Department of Environmental Science, Policy, and Management, University of California, Berkeley.

Michael Baram, LL.B., Professor Emeritus, Boston University Law School, Boston, Massachusetts.

Robert G. Bea, Ph.D., P.E., Professor, Department of Civil and Environmental Engineering, University of California, Berkeley.

Michael J. Blum, Ph.D., Arnold Early Career Professor in Earth and Ecological Science, Department of Ecology and Evolutionary Biology, Tulane University, New Orleans, Louisiana.

K. Florian Buchler, LL.M., ESQ., New Orleans, Louisiana.

W. E. Carnes, M.A., B.S., Practitioner Associate, Center for Catastrophic Risk Management, Haas School of Business, University of California, Berkeley.

Paul Donley, Corporate Trainer, Programer, Web Developer, Relevant Training, Melbourne, VIC Australia.

Yngvar Duesund, Special Advisor to the Center for Information Technology Research in the Interest of Society, The Banatao Institute—CITRIS, University of California, Berkeley.

William E. Gale Jr., Ph.D., P.E., CSP, CFEI, CFII, Forensic Engineering Consultant, President, William E. Gale, Jr., Inc.; Principal, Bundy, Gale & Shields LLC, Novato, California.

Ove T. Gudmestad, Ph.D., Professor, Faculty of Science and Technology, University of Stavanger, Stavanger, Norway.

Anthony Hare, Psy.D., Executive Director, Center for Catastrophic Risk Management, University of California Berkeley.

Samantha Joye, Ph.D., Professor, Department of Marine Sciences, University of Georgia

Jahon D. Khorsandi, M.S.E., Graduate Student Researcher, Center for Catastrophic Risk Management, University of California, Berkeley.

Trevor A. Kletz, D.Sc., Visiting (Adjunct) Professor, University of Loughborough, United Kingdom.

Kennith Kotow, P.E., Senior Associate, Successful Energy Practices International, San Antonio, Texas.

Sindhu Kubendran, B.S., Research Associate, University of California, Berkeley.

Kevin Lacy, B.S., Petroleum Engineering, M.B.A., Senior Vice President, Global Drilling and Completions, Talisman Energy, Calgary Alberta, Canada.

Artin Laleian, Student, Research Associate, University of California, Berkeley

Gary Marsh, B.S.M.E., Retired, Shell Drilling Engineering Advisor, Houston, Texas.

Wayne Needoba, B.S., P.E., Consultant on Drilling, Project Coordination, Learning, Competence Assessment, Labrador Holdings WA, Perth, Western Australia; Managing Director, LIS Thailand Co., Chiang Mai, Thailand.

Scott Nicholson, MSCE, MCP, MLA, Doctoral Graduate Student Researcher, Engineering Policy Analysis and Environmental Planning, University of California, Berkeley.

Michael L. Olson, Ph.D., P.E., Innovation, Sustainability, and Change Management Consultant, Walnut Creek, California.

David M. Pritchard, B.S, P.E., Owner, Successful Energy Practices International LLC, San Antonio, TX

Karlene Roberts, Ph.D., Professor Emeritus, Haas School of Business, Director, Center for Catastrophic Risk Management, University of California, Berkeley.

Emery Roe, Ph.D., Research Associate, Center for Catastrophic Risk Management, Haas School of Business, University of California, Berkeley.

Paul Schulman, Ph.D., Research Associate, Center for Catastrophic Risk Management, Haas School of Business, University of California, Berkeley.

Jon Espen Skogdalen, M.S.E., Research Fellow, Visiting Fulbright Scholar, Department of Civil and Environmental Engineering, University of California, Berkeley; Research Fellow, Doctoral Student, Faculty of Science and Technology, University of Stavanger, Norway.

Liz Taylor, President, DOER Marine, Alameda, California.

John Thomas III., Law Student, Golden Gate University School of Law, San Francisco, California

Marianne Tiffany, B.Sc., School of Psychology, the University of Aberdeen, Aberdeen, Grampian, United Kingdom.

Ingrid B. Utne, Ph.D., Visiting Scholar, Department of Mechanical Engineering, University of California, Berkeley; Professor (Qualification Fellowship), Department of Marine Technology, Norwegian University of Science and Technology, Trondheim, Norway.

Jan-Erik Vinnem, Ph.D., Professor II, Faculty of Science and Technology, University of Stavanger, Norway.

Ed Wenk Jr., Ph.D., Emeritus Professor of Engineering, Public Administration and Social Management of Technology, University of Washington at Seattle, Washington.

LuAnn E. White, Ph.D., DABT, Tulane University School of Public Health and Tropical Medicine, New Orleans. LA

Appendix B

Commentary on Preliminary Technical & Managerial Conclusions Developed by Investigators for the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, November 8 & 9, 2010

Technical Conclusions

Flow path was exclusively through shoe track and up through casing.

This mode of failure was one of the two primary modes of failure analyzed by the DHSG. The preponderance of evidence available at this time indicates the flow path through the bottom casing assembly and cement is the most plausible mode of failure that led to the blowout. The physical evidence (recovered casing head seal assembly), failed negative pressure test, and the post-hoc analysis cement slurry test data (Chevron) support this as the most likely flow path scenario.

Alternatively if the flow path did not develop through the shoe track and up thorough the casing, it could have developed up the outside of the long-string production casing (channeling through or passed fractures in the failed cement), flowing up the annulus and propagating to the production casing hangar at the seafloor. Expanding hydrocarbons could have found their way into the riser through the unsecured casing hangar at the seafloor due to pressures in the annulus; however, absence of external erosion and damage on the outside of the casing hanger seal assembly and its orifices does not support this alternative hypothesis. Another low probability leak path into the production casing bore could have been a breach developed in one of the slim-line production casing connections. A vulnerability was created by not cleaning and inspecting, then protecting metal-to-metal seals in the casing connections when they were deployed.

Cement (potentially contaminated or displaced by other materials) in shoe track and in some portion of annular space failed to isolate hydrocarbons.

The available evidence indicates the 'experimental' nitrogen foamed cement, the pre and post cementing processes (e.g. partial bottoms up circulation, positive pressure testing before cement cure), the hardware used near and at the bottom of the long-string production casing (e.g. minimum centralizers, float collar and shoe, the characteristics of the well at the bottom (e.g. clearance between production casing and weak formation, clearance between the bottom reamer and the bottom of the well – the 'rat hole'), and the reservoir characteristics (high pressures, high temperatures, gaseous hydrocarbons, relatively weak formation) all contributed to failure of the cement near and at the bottom of the Macondo well.

Pre-job laboratory data should have prompted redesign of cement slurry.

The available evidence indicates that the cement slurry ingredients, mixing, placement, and curing characteristics were the result of a series of laboratory experimental and analytical processes that did not develop acceptably reliable results for the Macondo well completion conditions and processes. This design did not meet the Best Available and Safest Technology requirements of the lease and well permit requirements. The use of micro-sized high pressure resistant glass beads rather than nitrogen to achieve a stable lightweight cement mix could have had higher reliability for these conditions. Given the important differences between the prototype conditions at the bottom of the Macondo well and those in the laboratory and simulated on the computer, there should be continuing major concerns for the reliability of this critically important part of wells to produce hydrocarbons in high hazard reservoir environments.

Cement evaluation tools might have identified cementing failure, but many operators may have decided not to run tools at that time and relied only on the negative pressure test.

Without a trip to drill out the float equipment and shoetrack, the Cement Bond Log (CBL) tools could not have been used to evaluate cementing quality except that opposite a few 'stray' sands above the main body of hydrocarbon bearing strata. In addition, it would have been necessary to provide about 72 hours minimum curing time on the cement to have the best chance at a useful log trace. A lot of time and money would have been spent in preparing for and running a CBL log. Although it may have given clues to latent defects, the trace itself is subject to interpretation in many cases. If properly planned, conducted, and interpreted, the negative test could have safely yielded a more direct and therefore more certain assessment of defects.

The critical decisions were: 1) not running the production casing as a liner to provide the best chance of obtaining multiple barriers, and 2) trusting the cement and not having processes and procedures which do not leave safety and reliability to chance in the event the barriers prove faulty.

Had the Macondo well not failed through the inside of the bottom assembly, then another mode of failure could have developed outside of the casing due to channeling through the narrow sheath of cement above the bottom of the well. Failure of the cement outside of the long-string would allow the producing formations to charge the annulus of the long-string with hydrocarbons. In this case, well logging – cement evaluation tools could have provided early warnings of deficiencies in the cement sheath above the bottom of the well which could have been remediated before the well was temporarily abandoned.

There are many possible ways a well 'structure' can fail. Multiple lines of defense – or barriers – should be in place to develop a 'robust' - damage and defect tolerant - structure. In addition, multiple sensing processes should be used to disclose important 'latent defects' so they can be remediated before they are activated to help cause failures.

Negative pressure test(s) repeatedly showed that primary cement job had not isolated hydrocarbons. Despite these results, BP and Transocean treated negative pressure tests as a complete success.

This experience provides a classic example of tests and the analyses of those tests developing 'false positives.' The combination of the signals or data provided by the test and the analyses of those tests falsely indicates there is no significant likelihood of failure in the well structure. This type of 'system' failure involves a combination of factors emanating from the operating teams, their organizations, the hardware (e.g. instrumentation, data displays, communications), procedures (formal, informal), environments (external, internal, social), and interfaces among the foregoing. The information exists, but is not properly accessed and evaluated, or if it is properly accessed, it is not properly understood (unknown knowable). There are a wide variety of reasons for such 'cognitive' (thinking, sensemaking) malfunctions. One of the most important is 'confirmational bias' – what we see and think is what we expect to see and want to think (wishful thinking).

It is debatable whether the cement job ever had a chance to achieve isolation given the large pressure reversal from the top stray zones to the bottom – what is not debatable is understanding the risk of actually executing a successful cement job – and planning mitigants accordingly. Question: was there actually anything in the procedures that presumed an "iffy" cement job, and if so, what next? Answer: no – they presumed it would be successful.

BP's temporary abandonment procedures introduced additional risk

The revised temporary abandonment procedure was proposed to the MMS on April 14, 2010 and approved by the MMS on the same day. Additional changes were made, all of which added to the risks associated with the temporary abandonment procedure. The available evidence and testimony indicates the temporary abandonment procedure had several parts that were of major concern to the Transocean drill crew and Offshore Installation Manager. The revised temporary abandonment procedure was introduced in the final days of completing the drilling of the Macondo well. The temporary abandonment procedure involved major changes from completing the well as an exploratory well to completing it as a production well as the Commission investigators clearly documented in their Master Presentation. Such modifications were made to expedite 'early production' from the prolific hydrocarbon formations that had been discovered at this location.

The temporary abandonment procedure was designed to make the completion activities more efficient (save time and money) by 'early' displacement and offloading of the drilling mud and running of an all-in-one tapered casing string extending from the bottom of the well to the sea floor wellhead. But these plans were not well thought out with little or no objective Risk Assessment and Management (RAM) process in planning, and failure to follow accepted Management of Change (MOC) procedures. The RAM and MOC approaches taken together yield appropriate Process Safety, which in this case was sadly lacking.

The all-in-one tapered production casing string was a 'minimum structure' that did not provide the additional 'barriers' that a liner and tie-back to the casing above would have. This long-string design was thought to save both time and money, but was not thought by BP and the MMS to be

riskier than a liner and tie-back completion structure. If all had gone according to plans and the conditions were as anticipated, then that assessment could have been realized. However, the conditions were not as anticipated and the plans resulted in flaws and defects that defeated this minimum well structure. Minimum structures are not robust structures able to tolerate initial uncertainties and damage and defects introduced during the life of the structure.

The parts of the temporary abandonment procedure that did result in a substantial increase in risk were: (1) the lack of engineering guidance on expected results and interpretation in the planning for the underbalanced test, (2) conducting the test before the bulk of cement had time to develop strength, and (3) the plan to underbalance test with the drill string 10,000 ft off bottom. Whether the surface plug was planned to be 300 ft below mud line or 3300 ft is almost immaterial. A robust underbalance must be used to provide meaningful results in either case to confirm barrier(s) before the heavy mud in the long drill riser can be prudently removed.. This test procedure required that the well be under-balanced – the external (zonal) pressures acting on the well at the bottom would be greater than the internal pressures inside the well structure. If the 'plugs' at the bottom of the long-string well structure (cemented shoetrack and flapper float collar) were reliable, if the external 'seals' (cement sheath, casing body and connections and casing hangar seal, provided for that long-string well structure were reliable, and if no hydrocarbons had been allowed to enter the well bore during the completion work and reside in the drill column, then the temporary abandonment procedure could have worked as expected. However, the evidence indicates that the provisions for isolation at the bottom of the well did not provide a reliable barrier and that hydrocarbons entered the well bore during the long-string completion and temporary abandonment processes. When the well was progressively under-balanced by displacing the heavy drill mud in the upper 8,300 feet with much lighter sea water, the hydrocarbons in the well bore migrated undetected to the surface with ensuing catastrophic effects.

Number of simultaneous activities and nature of flow monitoring equipment made kick detection more difficult during riser displacement.

Important simultaneous activities included work on and around the drill floor and mud pits associated with completion of the temporary well abandonment procedures and preparing for the next well. Activities included transferring drilling mud from the Deepwater Horizon to the Damon Bankston supply vessel, performing a 'sheen' test on 'spacer' (lost circulation materials) intended to avoid contamination of the oil base drill mud, performing and interpreting positive and negative pressure tests, transferring drilling mud between tanks, and working with BP and Transocean 'guests' who were onboard to observe operations and congratulate the Transocean crew for their splendid safety record. Available information and testimony indicates that multiple sensors and alarms that had been installed on the Deepwater Horizon to provide data on important parts of the operations were not 'coordinated,' 'displayed,' or in some cases, such as the general alarm and a critical flow sensor for the final part of the displacement, bypassed. Direct and unambiguous information on volume of fluids going into and out of the well was not readily available. With multiple distractions and ambiguous data difficult to analyze, the crew was not able to detect, analyze, and effectively react to the developing blowout.

Analyses of past accidents repeatedly have shown the 'perils of parallel processing' at critical times and places in operations. The simultaneous oil and gas production operations and critical

maintenance operations prior to the failure of the Occidental Petroleum Piper Alpha platform in the North Sea, and the simultaneous operations carried out onboard the bridge of the Exxon Valdez tanker as it was departing outside the approved shipping lane in Prince William Sound are prime examples of the perils of parallel processing. While each of these simultaneous operations can be 'safe', it is their unexpected and unmanaged interactions and distractions at critical times and places that can provide the impetus for catastrophic failures.

Nevertheless, kick indications were clear enough that, if observed and recognized, these warnings would have allowed the rig crew to have responded earlier.

In hindsight, it is evident that the well was in the process of 'kicking' for almost an hour before it actually blew out. Yet, no one on the rig noticed the evolution until sea water was blown to the top of the drilling derrick, followed quickly by a stream and shower of oil drilling mud, followed by gas and oil that spread across the decks of the Deepwater Horizon. Early detection of the symptoms of a potential crisis situation is critical so that more time is available to analyze and understand those symptoms, analyze alternatives for corrective action, and then implement the alternative or alternatives that can rescue the system. The available evidence indicates that those on the Deepwater Horizon that night were confident that the well was secure and that all was going just fine. They would be wrapping up this "well from hell" in a few hours, moving the rig to a new location, and going home for a much deserved break. The evidence indicates that vigilance and preparations to handle crisis had turned to complacency in the haste to wrap up the Macondo well and move on to another offshore project.

Once the rig crew recognized the influx, there were several options that might have prevented or delayed the explosion and/or shut in the well.

As acknowledged by the Commission investigators, once portions of the rapidly expanding gas and hydrocarbons were in the riser, it was too late to prevent the gas and hydrocarbons from reaching the drill deck. When the gas and hydrocarbons reached the drill deck, immediate activation of the emergency shut down systems for ventilation and diversion of the gas and hydrocarbons directly overboard could possibly have prevented the explosions and fires. Unfortunately, the emergency shut down on ventilation systems apparently had been put on 'inhibit mode' requiring human activation that came too late. Because the large hydrocarbon influx was not detected in earlier stages, the closing of the annular BOP may have been "too little and too late".

The decision was made on the drill floor (perhaps days or weeks before) to divert the well flow to the "poor-boy" mud gas separator that could not handle the flow pressures and volumes, and for reasons to be confirmed, the blowout preventer was not able to be effectively activated to stop the hydrocarbons coming from the bottom of the well.

Once the explosions and fires developed on the decks and in the moonpool of the Deepwater Horizon, the emergency disconnect system to allow the rig to separate the riser and upper BOP from the lower BOP could not be successfully activated. Also, if the annular had been successfully

closed and had stemmed the flow from the well temporarily, it would have reopened and leaked after control signal and power were interrupted by the multiplexer cables (or reel arrangements for them) being damaged or destroyed by the fire. Once the multiplexer signals and power fluid through the rigid conduit were not available to the subsea control pods, one or the other pod should have automatically triggered closing the blind/shear rams using the stack-mounted fluid power accumulator content (Deadman function). Defects in both pods prevented that from happening. The cascade of failures of the multiple emergency systems played major roles in the evolution of this disaster.

Diverting overboard might have prevented or delayed the explosion. Triggering the EDS (Emergency Disconnect System) prior to the explosion might have shut in the well and limited the impact of any explosion and/or blowout.

Immediate diversion overboard of the incoming expanding gas and hydrocarbons might have prevented or delayed the explosion. The low capacity mud – gas separator should not have been left open. However, based on the available testimony and evidence, due to the very rapid developments, sufficient time was not available for the crew to detect and analyze what was happening and take effective action. This 'surprise factor' could have been mitigated by much earlier detection of the hydrocarbon inflow and through the use of an improved overboard diversion system and refinement of protocols (pre-selection of options) for its use.[13,14]

Technical conclusions regarding (the) BOP (Blowout Preventer) should await results of forensic BOP examination and testing.

Available evidence and testimony indicates there were a wide variety of maintenance and modification concerns associated with the BOP. These included leaking hydraulic connections, non-functional battery packs needed to activate the blind shear BOP, 're-plumbing' of the BOP components, and overdue inspections and certifications. Review of the available test and analysis background pertaining to the reliability of the specific make and model of BOP on the Deepwater Horizon clearly shows that the industry and government had major concerns for the reliability of this 'generation' of BOP. [1]

[1] West Engineering Services, "Shear Ram Capabilities Study," Report to U.S. Minerals Management Service, Sept. 2004, "Final Report, Blow-out Prevention Equipment Reliability Joint Industry Project (Phase I-Subsea), Report to U.S. Minerals Management Service May 2009, E. Shanks, "Deepwater BOP Control Systems – A Look at Reliability Issues, Proc. Offshore Technology Conference, 2003, Tetrahedron, Inc., "Reliability of Blowout Preventers Tested Under Fourteen and Seven Days Time Interval," Report to Minerals Management Services, Dec. 1996, J. Melendez, J.J. Schubert, Mamani, "Risk Assessment of Surface vs. Subsurface BOP's on Mobile Offshore Drilling Units," Final Report to Minerals Management Service, August 2006, EQE International, "Risk Assessment of the Deepwater Horizon Blowout Preventer (BOP) Control System, Prepared for Cameron Controls Corp., April 2000, Per Holland, "Reliability of Deepwater Subsea Blowout Preventers," SPE Drilling & Completion, Society of Petroleum Engineers 2000, Per Holand and P. Skalle, SINTEF, "Deepwater Kicks and BOP Performance," Report to Minerals Management Service, July 2001.

No evidence at this time to suggest that there was a conscious decision to sacrifice safety concerns to save money.

Analysis of the available evidence indicates that when given the opportunity to save time and money – and make money – tradeoffs were made for the certain thing – production – because there were perceived to be no downsides associated with the uncertain thing – failure caused by the lack of sufficient protection. Thus, as a result of a cascade of deeply flawed failure and signal analysis, decision-making, communication, and organizational - managerial processes, safety was compromised to the point that the blowout occurred with catastrophic effects.

Time and cost pressures are an inherent part of this type of operation. Operations of this type cost $1 to $1.5 million per day – nearly $1,000 per minute. Income from the operations also provides important pressures. A well like Macondo can produce 50,000 barrels of oil per day – or more. This production has a total value (upstream and downstream) that approaches $10 millions per day or about $7,000 per minute.

The DHSG does not conclude those who worked on the Deepwater Horizon Macondo well project made conscious 'well informed' decisions to trade safety for money. The DHSG analyses of the available evidence indicates they were trading something that was in their estimation unlikely for something that was sure. They were trading sure savings in time and money – and perhaps quicker returns on investments - for the very unlikely possibility of a blowout and its unimagined severe consequences. The risks were erroneously judged to be insignificant. Thus, erroneous tradeoffs between risks (safety) and costs were developed.

The available evidence indicates this crew, the onshore support staffs, and the regulatory agency staffs had never experienced a major accident such as unfolded on the Deepwater Horizon. This failure was beyond their experience – a "failure of imagination. "

The Macondo well permitting documentation clearly shows that both BP and the MMS believed the likelihood of a catastrophic blowout were not significant. Blowout prevention plans were not required (waived). Procedures, processes, and equipment for containment and cleanup of the 'worst case' blowout were deemed to be readily available and would prevent significant negative environmental impacts.

There was significant experience to bolster this over confidence in success. This very complex system had just completed a world record setting operation to the west of the Macondo well – the Tiber well. The Tiber well was drilled to 35,000 feet below the drill deck in more than 4,000 feet of water. The Tiber well led to discovery of more than 3 billion barrels of hydrocarbon reserves. This system had completed 7 years without a reportable - recordable lost time accident. This system was overconfident in its abilities to cope with the challenges posed by the Macondo well – whose risks were judged to be 'insignificant.'

Available evidence and testimony indicates there were multiple (10 or more) major decisions and subsequent actions that developed in the days before the blowout that in hindsight (hindsight does not equal foresight) led to the blowout. There were conscious deliberations about each of the primary decisions and action sequences – on the rig and 'on the beach' (the office staffs). The well permitting documentation contains many detailed flow charts and decision points that were used in

parts of this operation. In each case, these deliberations addressed the likelihoods and consequences of failure (a blowout) – implicitly or explicitly.

This system also had proactive, interactive, and reactive risk management processes that were in place and implemented (well or poorly) before the blowout. The proactive processes included provisions for inspections – maintenance – and repairs of critical pieces of hardware such as the blowout preventer. Interactive processes included formal management of change processes. There were interactive quality assurance and control procedures to address risks during operations such as the procedures for negative pressure testing and setting a barrier 3,300 feet below the seafloor. There were procedures, processes, and hardware for reactive risk assessment and management – automatic shut in systems, blowout preventers, emergency disconnect systems, emergency evacuation systems, and environmental protection systems. This system had a substantial suite of risk assessment and management processes intended to enhance prevention, interception, and reaction to a catastrophic blowout.

When each of the primary decisions and subsequent actions concerning the production well design and temporary abandonment were developed, the available evidence indicates the risk assessments were that there were no significant likelihoods or consequences associated with failure. The available evidence does not indicate that any one person or group was keeping tabs on the accumulation of risk that accompanied the individual decisions and subsequent actions or inactions Thus, apparently it was concluded by those involved in this operation (BP, MMS, Transocean, Halliburton, etc) that there were no significant challenges to 'safety'. A realistic, rigorous Risk Analysis and Management (RAM) process and Management of Change (MOC) process (for changing modes from drilling to completion) appears not to have been performed. The result was a serious compromise of process safety.

However, those involved could easily understand the potential savings in time and money associated with expedited 'efficient' operations. They could easily understand this project was seriously behind schedule (more than 50 days) and over budget (approaching $100 millions). There were significant incentives to 'wrap this job up' as quickly as possible. In addition, there were significant incentives to get this productive well on stream as quickly as possible – the 'last days' decisions and actions to complete the permitted exploratory well as a production well.

The available documentation does not provide any references to guidelines on how their risk assessments were developed and validated. In the majority of cases, judgments of the likelihoods and consequences of failures (e.g. blowout) appear to have been based on unsubstantiated 'feelings.' The available documentation does not indicate that any of the direct participants on the rig or on the beach had significant formal training or qualifications in risk assessment and management of complex systems. Experience has adequately demonstrated that a few hours of training with a 'risk matrix' (plot of likelihoods versus consequences) does not qualify people to perform risk assessments of complex systems. The power of this extensive branch of technology is critically dependent on the knowledge, qualifications, training, experience, and motivations of the people who use it.

The assessments' findings that there were no significant risks is not surprising. The likelihoods and consequences were incorrectly judged by those involved not to be significant. Deeply flawed and deficient risk assessment and management processes were in place and were being used.

Protective barriers were in place and were incorrectly thought to be sufficient and functional. The failures that developed before, during, and after the Macondo well project clearly show these risk assessment and management processes – barriers - were deeply deficient and pervasively flawed. Important things that were supposed to have been done correctly were either not done or were not done correctly. When the system was 'tested' before, during, and after the blowout, it performed miserably.

As described by Exxon-Mobil CEO Rex Tillerson in response to questions before the National Commission, an organization's safety culture takes time (several decades) to develop and has to be grown from within – you can't buy it or import it – it has to be nurtured from within the organization. Exxon-Mobil has been at it now for more than twenty years, after learning the hard way and paying for its complacency and risk management failures that led to the Valdez spill. Since that time, Exxon-Mobil has turned the corner and introduced many positive innovations to improve safety culture, such as their Operations Integrity Management System (OIMS), introduced in 1992 as an integral part of their overall safety management system.

In contrast, at the time of the Macondo blowout, BP's corporate culture remained one that was embedded in risk-taking and cost-cutting – it was like that in 2005 (Texas City), in 2006 (Alaska North Slope Spill), and in 2010 ("The Spill"). Perhaps there is no clear-cut "evidence" that someone in BP or in the other organizations in the Macondo well project made a conscious decision to put costs before safety; nevertheless, that misses the point. It is the underlying "unconscious mind" that governs the actions of an organization and its personnel. Cultural influences that permeate an organization and an industry and manifest in actions that can either promote and nurture a high reliability organization with high reliability systems, or actions reflective of complacency, excessive risk-taking, and a loss of situational awareness.

Managerial Conclusions

Individuals should be trained to repeatedly question data, raise concerns, and double-check assumptions.

Significant resources have been devoted to learning about training people to perform complex operations. One key insight developed from this work is effective training requires effective selection of personnel who will perform specific types of operations. The selection process is intended to identify individuals who have the talents and abilities required to work with a particular system – the *Right Stuff*. Training can then be used to help amplify the required talents and abilities to develop the needed capabilities and competencies. Training needs to address normal, abnormal, and unimaginable situations and developments. Excellent guidelines that address the challenges associated with selection and training of personnel to operate critical systems have been developed for high reliability systems such as commercial nuclear power generation and commercial aviation.

Experience with complex systems has shown these systems live or die based on the assumptions (explicit, implicit) that are made about a system during its lifetime. If the assumptions are valid, the ensuing developments (analyses, actions) if properly performed can produce desirable results. If the assumptions are not valid, then even if the analyses and actions are properly performed, undesirable results (failures) can be expected. Formal structured processes (internal, external) have been developed to validate assumptions and the analytical processes based on the assumptions. These processes should be included in future developments associated with high hazard exploratory drilling and production system operations.

It is important that management understands the overall risks involved in drilling a deepwater well and that they understand what it takes to make a robust deepwater well design. A competent team has the know-how to deal with the tasks in hand, i.e., the team members possess certain measurable skills, sound education, good intuitive judgment, experience, an ability to apply related knowledge to solve problems and a responsible attitude. Stakeholders will trust a professional team based on competence proven on previous track records of the individuals.

The competency of a company's drilling team, whether the team has the right persons for the job or previous success has made them complacent, "making short cuts", should be questioned in case of incidents occurring. Equally so, the competency of those who verify the well design and those who approve the non-conformances or changes should be questioned.

The composition, competency and integration of a team have a significant effect on its success. When management assigns tasks to individuals they assume that the person has the competency and will have "hands on" the work to be carried out. In the oil and gas industry there are long traditions of how a drilling team is composed and there isn't much difference from one oil company to another in how the work is organized. However, risk assessment, planning, and contractual issues may vary considerably and so the performance.

When a drilling team is faced with a situation they didn't contemplate and there are no operating procedures for handling it, then full management attention should be required. If critical, the top management of the organization should be informed. The decision whether to stop a risky operation

or not should be taken by the most competent personnel, i.e., a person or persons who have experienced and handled similar situations. Top management or the regulatory body will normally not have the competency required to handle an unexpected operational issue, but they can contribute, ensuring that best resources and information are made available. The team's ability to handle unexpected situations depends very much on how it has been trained and its ability to communicate incidents or non-conformances in real time to its stakeholders.

Greater attention should be paid to the magnitude of consequences of all anomalies, even seemingly minor anomalies.

Attention is a vital and perishable human resource. Choosing what to pay attention to and what not to pay attention to during the performance of complex tasks requires the skills of discrimination. This is particularly difficult when the signals associated with anomalies are weak in a 'strong noise environment.'

Slowly evolving developments leading to crises frequently are difficult to detect because signals of evolving degradations are drowned out by the noise of normal daily operations. We loose our ability to expect the unexpected thereby frequently losing situational awareness. Values, beliefs, and feelings trump knowledge, logic and good sense and we fail to take appropriate action. Slowly developing crises, if properly detected and evaluated, provide time to develop optimized solutions, experimentation, and correction.

Rapidly evolving developments leading to crises frequently are difficult to manage because of surprise factors – they destroy beliefs - and time pressures that can lead to cognitive lock-up – tunnel vision. In such crises, the challenge is to survive – quickly find and implement a solution that works.

The problems associated with correct diagnosis of clues also pose major challenges in managing crises – correctly connecting the 'dots' (clues) that tell us what causes or problems are causing escalation of the crisis. Flawed mental models (wrong, incomplete), defensive behavior (actions to avoid embarrassment, injury and loss), muddled goals (contradictory), uncertainties, repair service behavior (treating symptoms not causes) and denying unwelcome realities lead to failure to properly connect the dots.

Individual risk factors cannot be considered in isolation but as an overall matrix. Personnel cannot ignore anomalies after believing they have addressed them.

The available evidence does indicate that risk assessments associated with completion and temporary abandonment of the Macondo well were made separately – there was no 'risk memory.' This type of challenge is one of the key reasons for requirements of disciplined formal Management of Change procedures and processes, Safety Cases, and Process Safety analyses. While each step in a proposed process can be judged to be 'safe', due to the uncertainties associated with the conditions and analyses, the accumulation of risk in the process can prove to be fatal.

The need for continuous vigilance during performance of critical processes is an important part of risk assessment and management (RAM) and Management of Change processes to maintain the reliability of complex systems operating in hazardous environments. Interactive RAM processes performed during the time activities are performed take many forms – such as Quality Assurance and Control, Management of Change, and Management of Crises. Early detection of anomalies that can be indicative of failure and risk escalation can provide more time for analyses of the anomalies, mobilization of resources, and implementation of strategies to return a system to a reliable state. Similarly, after the system has been returned to a reliable state, the process of 'observe, orient, decide, act' (OODA) must be continued to confirm that a reliable state has been achieved and is being maintained. The Macondo well pre-failure experience clearly shows an important need to develop more effective interactive RAM processes and systems for all parts of these high hazard systems including concept development, design, construction, operation, and maintenance. Development and implementation of effective systems to facilitate RAM of rapidly (surprise) and slowly (sneaker) developing crises should be given high priority.

There should be greater focus on procedures and training in how to respond to low-frequency, high-risk events. "How do you know it's bad enough to act fast?"

Crises are the complex frequently unforgiving unraveling of the order we try to give the world. Crises destroy beliefs, challenge our expectations and test the power to reason. Crises show weaknesses and strengths that would not otherwise be apparent. Study of recent crises that turned into failures clearly indicates that many are incubated by 'pushing the envelope' often indicated by the business mantra - better, faster, cheaper – doing more with less. Relentless focus on productivity and costs can lead to increases in crisis vulnerability. This focus frequently shows up as departures from safe operating procedures to save time, money and energy. Many times, these departures act to trigger the sequence of events that escalate to an accident or failure.

Another major contributor to many current failures to deal successfully with crises that challenge complex systems is loss of core competencies, particularly those of high quality science, engineering, operations and management. Often the loss of core competencies develops in response to a business mantra: down-sizing and out-sourcing. The enterprise wants to create lean and agile organization and that can be good as long as it does not lead to organizations that bleed to death when scratched. Organizations are tempted to think they can get the expensive expertise needed by outsourcing and miss understanding that the outsource organization does not have the same fundamental goals and objectives as the buyer. It is evident that the organization that outsources must have expertise that equals or exceeds that of the outsourcer. One can not adequately manage what one does not understand or can not do.

The study of near misses and accidents shows that vast majority of events that triggered a crisis are malfunctions of commission: People perform an action on purpose and it either comes out wrong or is performed incorrectly. Even more interesting, most factors that contribute to triggering events are organizational malfunctions that grow out of poor communications and productivity-at-any-cost cultures. At the same time, the vast majority of factors that rescue a crisis from failure involve organizational interactions. Some organizations know how to snatch victory from defeat by being on the constant alert for the early warning signs of crises. They select personnel and develop

highly functional teams based on demonstrated capabilities and talents. They provide hardware support to not only supply early warnings, but also protect people physically and mentally and to avoid overloading and distractions.

These organizations have a strong, top-down, strategic commitment to "quality first." They demonstrate real, long-term care, concern and action, not just top-down but bottom-up. They create norms, rules, and procedures to remove conflicts between quality and production or service; promote continuous improvement; and manage crises. They do not take the health of their system for granted. They reflect, audit, critique, and listen to feedback on the health of both their system and their people. And they practice timely, effective, thorough, and honest communications that effectively bind the individuals, teams, and organization together.

The best organizations prepare by creating systems and people robust enough to tolerate damage and defects and resilient enough to bounce back from trauma while planning the next steps ahead. Such systems embody four important elements: 1) appropriate configurations - they put the right stuff in the right places at the right times, 2) excess capacity - they can carry excessive demands when one or more elements become overloaded, 3) ductility - they stretch and deform with out breaking or loosing capacity; and 4) appropriate association - they morph to fit the situation, turning independent or high associative when required.

Effective crisis management systems focuses on providing people and system supports that promote protection (safety) and reliability. People support is focused on selecting, training, organizing, leading, and managing the right stuff - assuring that the right stuff is in the right amounts and places at the right times and ways. System support is focused on providing serviceable, safe, compatible and durable assemblies of hardware and humanware that are robust, resilient, and sustainable. Strategies that reduce the likelihoods of malfunctions, increase their detection and remediation, and reduce the effects of malfunctions are employed in a continuous process to improve protection and reliability – and maintain productivity.

Selection and training of people to enhance their abilities to successfully address rapidly developing crises is of critical importance. Training consists of much more than developing procedure manuals and guidelines. Prototype hardware and computer simulators that can approximate realistic crisis conditions can provide important skill building experiences. Realistic drills can also provide valuable learning experiences. Much can be learned from communities that must be constantly prepared to deal with rapidly developing crises such as emergency medicine, military operations, fire fighting, commercial nuclear power generation, and commercial aviation.

Communities that succeed in crisis management practice and drill to become near perfect. That starts with communication – effective, timely, understandable – with encouragement of feedback. Crisis managers must learn to clearly explain not just goals, but why they do things so people can work independently and creatively and still move in the right direction. Team members learn to subordinate their personal prominence to achieving successful management of crises. They work within a fluid organization where leadership develops and migrates so the team can do things otherwise beyond their reach. Through experiences and practice, development and maintenance of trust is critical.

Appendix C

Perspectives On Changing Safety Culture And Managing Risk

W.E. Gale, Jr.

1.0 Introduction

To suggest that BP has a history of taking risks is perhaps a gross understatement. In fact, BP owes its success and can claim its place among the other so-called super-majors for that very reason. BP was, and is willing to take risks that other companies have traditionally shied away from…BP has been both commended and condemned because of its risk-prone culture. Much like Tiger Woods trying to change his swing, BP is now trying to change the very thing that made it so successful. Can they succeed and still remain successful?

This paper in brief looks at the history of BP and their recipe for success. The business model that, heretofore, has been embedded in BP's culture has been one of risk-taking, cost cutting, and capital efficiency improvement within the context of *risk management*—risk management of their portfolio of assets. This paper is not meant to be a commentary on "good" or "bad" corporate culture *per se*, but rather seeks simply to reveal some of the underlying issues that organizations must necessarily confront in order to manage risk comprehensively and successfully.

In simplistic terms, safety is the judgment of risk. Something is judged safe when the risk is deemed acceptable—it does not mean that there not any risk—just that the risk can be mitigated or controlled to an *acceptable level*. This applies equally to investors purchasing BP stock and to regulators granting BP permits to operate offshore. In this regard it is important to understand that engineers and managers often look at risk differently. Engineers are apt to suggest that if risk cannot be quantified and measured, then its degree of seriousness cannot be adequately determined—in other words what you can't measure you can't manage—at least not very well. Moreover, engineers generally think of risk in terms of probability and consequence, i.e., how likely is it that something will go wrong and, if it does, what will be the likely consequences. When there is a great deal of uncertainty involved in quantifying risk, engineers tend to be risk-adverse, taking a conservative approach. In the past, this is how safety factors were determined, and more recently, how confidence levels of probability distributions are reflected in limit-state designs.

Managers, on the other hand, tend to think of risk more in terms of "risk and reward"—the bigger the reward, then the bigger the risk that is worth taking.[1] Their concept of risk management

[1] For example, see http://www.riskculture.com/: The Keys to Success**.** Functionally, there are four aspects of financial risk management. Success depends upon a positive corporate culture. No one can manage risk if they are not prepared to take risk. While individual initiative is critical, it is the corporate culture which facilitates the process. A positive risk culture is one which promotes individual responsibility and is supportive of risk taking…. Risk Culture Blog, June 8, 2010.

can differ significantly from that of engineers, and these differences, driven by business goals, can infuse and embed a corporate culture in which risk management is meant to maximize portfolio assets and increase the bottom line. This is not inherently bad—quite the opposite—it is exactly what they should be doing. In fact, in the U.S. it's the law![2] As noted in Forbes Magazine, "U.S. corporate law states that the legal obligation of the directors and officers of a company is to serve the interests of shareholders. Period. Full stop. This is true even when serving the interests of shareholders comes at the expense of its workers, community, or the environment."

It would be difficult to find anyone who would disagree with the proposition that finding and drilling for oil and gas is a high-risk high-stakes business. The risks are enormous and so can be the rewards. In 1968, after a decade of drilling dry wells along the North Slope, BP was on the verge of abandoning its search. Its equipment was already packed up and awaiting shipment when a rival consortium made a suspiciously extravagant offer for BP's Alaska acreage along the edges of Prudhoe Bay. Atlantic Richfield (ARCO) and Humble Oil (Exxon) weren't telling, but they had struck oil in their own last-chance well in the centre of the Prudhoe Bay structure.[3]

After making its Prudhoe Bay Oil Field strike on the Alaskan North slope in 1969, BP has continued to grow to become the largest oil and gas producer in the U.S. and the major supplier of fuel to the U.S. military.[4] Both Tony Hayward and his predecessor, Lord Browne, did a commendable job in advance BP into the realm of the super-major oil companies—a lofty position that took guts, fortitude, and business-smarts to achieve.

Lord Browne, who holds a MS in business from Stanford (1981), having received a BS from Cambridge in 1969, placed huge bets by acquiring the oil companies AMOCO (1998) and ARCO (2000) in a series of mega-deals, while at the same time gained a reputation for cost-cutting and maximizing the bottom line.[5] He quadrupled BP's market capitalization while he was at the helm and was touted as *Tony Blair's favourite [sic] businessman* before being forced to resign in 2007 over a scandal in which he allegedly lied to the court about his homosexuality to protect his privacy. Since then, however, Lord Browne is back in the news, being appointed as the U.K. government's "lead

[2] Jay Coen Gilbert, "A Solution To The BP Problem: Changing The Rules Of The Game," Forbes – The CSR Blog, June 11, 2010, http://blogs.forbes.com/csr/2010/06/11/273/.

[3] BP, "Post war history of BP, 1946-1970," http://www.bp.com/sectiongenericarticle.do?categoryId=9014443&contentId=7027523

[4] Neil King Jr. and Melanie Trottman, "BP Risks Big Fines and Loss of Major U.S. Contracts," Wall Street Journal, May 28, 2010, http://online.wsj.com/article/SB10001424052748703630304575270822261954614.html. "BP is the single biggest supplier of fuel to the Department of Defense, with Pentagon contracts worth $2.2 billion a year, according to government records. BP is also the largest producer of oil on federal waters in the Gulf of Mexico, which makes it a significant contributor of revenue to the government."

[5] At the time there were two companies known as "supermajors" in the oil business—Exxon and Shell. By the end of 1998 there would be a third supermajor, and the trio would be dubbed the "three sisters." In May 1998 Browne called H. Laurance Fuller, the chairman of the board of Amoco, about acquiring Amoco. In August 1998 British Petroleum purchased Amoco for $57 billion, and British Petroleum renamed itself BP Amoco. The purchase of Amoco made BP Amoco's workforce 99,000 employees. In 1999 this number was cut to 89,000. This and other cuts in expenses eventually saved the company $2 billion annually. In 1998 Queen Elizabeth II made him a knight, upholding a British tradition whereby the monarch bestowed honors each year on her birthday. In April 1999 BP Amoco purchased ARCO for $27 billion in BP Amoco stock. ARCO owned 22 percent of Prudhoe Bay, and BP Amoco owned 51 percent, but U.S. government regulators wanted BP Amoco to give up its ARCO Alaskan holdings. BP Amoco sold these holding to Phillips Petroleum for $7 billion, leaving BP Amoco with control of 45 percent of Alaska's oil. http://www.referenceforbusiness.com/biography/A-E/Browne-John-1948.html.

non-executive director," working with Whitehall cabinet ministers to appoint people to cut costs and *improve efficiency* in each department.[6]

Seemingly, neither has his business savvy gone without recognition nor has his parsimonious talents gone to waste. Is it coincidental that in mid-October 2010 the powers that be at Whitehall announced the most severe austerity measures ever taken by the U.K. government in peace-time, proposing to cut 490,000 jobs in the public sector and slashing the budget across the board, including defense and welfare?[7] It is interesting to note that Alan Johnson, Labour's spokesman on economic issues, accused Finance Minister, George Osborne, of economic "masochism"—a term that also has been applied to how the Deepwater Horizon management team seemingly approached drilling risks.[8]

This brings us to Tony Hayward, who has been vilified as the most reviled and hated man in America due to his frequent gaffs and inept handling of *The Spill*.[9] Tony Hayward took charge of BP following John Browne's departure, and vowed to change BP's safety culture in the aftermath of BP's Texas City refinery catastrophe.[10] He also sought to improve BP's bottom line and "close the competitive gap" that had been identified in BP's place among its sister super-majors.

2.0 Closing The Competitive Gap By Portfolio Building And Cost Cutting

On Tuesday, March 2, 2010, a few weeks before the blowout, Tony Hayward updated stakeholders on the success of BP's strategy *to close the competitive gap* that was identified in 2007.[11] He discussed how momentum had been restored to BP's core business and a focus on safe and reliable operations is now strongly embedded in BP, mentioning that they have started to see the benefits of improved performance flowing through to their bottom line. Haywood links 2009's strategic progress to a longer track record over the past decade of building a portfolio of assets of great quality and huge potential. In Exploration and Production (E&P), he touts BP's history of being both an efficient and successful explorer with a record as being among the best in the industry.[12] He

[6] "Ex-BP boss Lord Browne to lead Whitehall reform," BBC News, June 30, 2010, http://www.bbc.co.uk/news/10467532 . Also, Tom Bower, "July Fourth Outrage: British Gov't Elevates Disgraced BP Boss," The Daily Beast, July 1, 2010, http://www.thedailybeast.com/blogs-and-stories/2010-07-01/lord-browne-and-bp-oil-spill-outrage/p/.

[7] "UK Announces 490,000 job cuts: Britain will cut 490,000 public sector jobs over four years under austerity measures designed to reduce the country's record deficit;" The Chronicle, Oct. 24, 2010, http://ghanaian-chronicle.com/business-news/uk-announces-490000-job-cuts/.

[8] Trevor Kletz, "The Root Cause of the BP Leak**,"** DHSG Working Paper, June 2010. "The phenomenon I have described was also a root cause of the 2005 explosion on BP's Texas City plant - the macho culture spread to the whole company, not just the offshore parts - and a similar phenomenon occurred in Buncefield, UK which resulted in the 2005 explosion there."

[9] Maryann Tobin, "BP CEO Tony Hayward: The most hated man in America?," Examiner.com, June 5, 2010, http://www.examiner.com/political-spin-in-national/bp-ceo-tony-hayward-the-most-hated-man-america .

[10] U.S. Chemical Safety Board Final Investigation Report: REPORT NO. 2005-04-I-TX, March 23, 2005, www.csb.gov. Also "Baker report: Recommendations," Financial Times (U.K.), January 16, 2007, http://www.ft.com/cms/s/4429b9d0-a57b-11db-a4e0-0000779e2340.html .

[11] "BP's Strategy Update," Tony Hayward, CEO of BP, http://www.bp.com/sectiongenericarticle.do?categoryId=9021974&contentId=7040780.

[12] BP forecast that in 2010 GOM deepwater operations would account for 35% of their total production; "More than 20% of its production is now in deep water or subsea (that is when production equipment is placed beneath the sea's

compares BP to other "super-majors" in the industry and notes that while their portfolio ranks among the best in the industry, their financial performance has yet to reflect this…"*but there is now a real opportunity to make this portfolio work harder for us and we intend to do just that*."

Hayward explains that their strategy remains unchanged but "we are now embarking on a new phase – to realize the potential of the portfolio built over the last decade." He notes that "*we have considerable scope to pursue section leadership, particularly in costs, capital efficiency and margin quality*." In upstream operations he explains that they will focus on cost and capital efficiency to deliver profitable growth. They will continue to unlock corporate efficiency through a culture of continuous improvement.

He goes on to state that their direction is clear, "*it is the unrelenting pursuit of competitive leadership in relation to cash-costs, capital efficiency, and margin quality*." Their goal over the next few years is to realize their latent potential of their asset base by improving the efficiency and effectiveness of everything they do. "*We will vigorously drive cost and capital efficiency while at the same time maintain our priority of safe and reliable operations. We believe that there is still a considerable prize to be had from embedding a culture of continuous improvement across the organization. We've emerged from 2009 in great shape, with renewed confidence and determination. We can see the prize and believe we are well positioned to capture it.*"

3.0 Black Gold – The Means To The Prize

In his quest to be Number One, Hayward took a number of steps to further profits and improve the bottom line. After a disappointing 4th quarter in 2007 he called in Neil Perry, oil & gas specialist with investment banker Morgan Stanley, who recommended further cost-cutting and austerity measures. Perry told Hayward that BP has failed consistently on upstream project delivery and downstream reliability.He added, however, that the organization was "sitting on a goldmine" of assets that could help it close the gap on competitors. Shortly thereafter Hayward announced BP's intention to cut 5000 jobs and reduce overhead by some 20%.[13] By the end of the cost-cutting that followed, more than 6,500 jobs were eliminated—almost 10 percent of BP's workforce—according to The Wall Street Journal. Insiders are reported to have spoken of "draconian" measures and a heavy emphasis on production targets.[14, 15] Earlier, when retired Coast Guard Captain James Woodle took a job with the Alyeska oil consortium (majority-owned by BP) in Valdez, Alaska, and put in charge of oil spill recovery, he reportedly told Newsweek he was appalled when he arrived on-scene: "They had cut back on equipment, on staff." And when he asked about the cuts, he was told very pointedly: "**Safety doesn't make money**."[16]

surface), a figure which is expected to rise to more than 35% by 2010." http://www.bp.com/sectiongenericarticle.do?categoryId=9025122&contentId=7047805.

[13] David Robertson, "BP to cut 5,000 jobs as profits fall by a fifth,", The Sunday Times, February 5, 2008, http://business.timesonline.co.uk/tol/business/industry_sectors/natural_resources/article3310399.ece, and "BP to cut jobs after profits fall," BBC News, February 5, 2008.

[14] Guy Chazan, "BP's Worsening Spill Crisis Undermines CEO's Reforms," Wall Street Journal, May 3, 2010, http://online.wsj.com/article/SB10001424052748704093204575215981090535738.html

[15] Ravi Somaiya, "The Road to Deepwater Horizon-- BP's oil spill in the Gulf of Mexico was a disaster three decades in the making;" Newsweek, July 13, 2010, www.newsweek.com/2010/07/.../the-road-to-deepwater-horizon.html.

[16] Ibid, Newsweek, July 12, 2010.

As explained in BP's Horizon magazine:[17]

"GROUP chief executive Tony Hayward's admission that in recent years BP has been a 'serial underperformer' was a brutally honest assessment of how the company sits in relation to its competitors. His address at a gathering of the company's top 500 leaders in Phoenix in March, left managers in no doubt that BP had "promised a lot but not delivered very much". Hayward's words still ringing in their ears, delegates were in no doubt that if BP is to close the current performance gap to its competitors, then it must implement the forward agenda, which was set out in October last year. One part of that agenda is the new leadership framework. For BP's executive team, the new, single framework is key to making a sustainable change of leadership behaviours across the company."

Hayward also instigated a bonus system linked to how much money an employee could save the company, thereby, perhaps inadvertently, creating a cultural incentive across the workforce to "*do it quicker and do it cheaper*." [18]

> *"At a federal hearing this week, an investigator revealed that BP's top manager on a drilling rig is given a performance evaluation that includes the category "Every Dollar Counts and Simplification." Of 13 employee evaluations reviewed by investigators, 12 had documented ways they had saved the company large sums of money, typically six-figure amounts, and one had put together a spreadsheet showing that he could account for $490,000 in savings, said Jason Mathews, an investigator for the Bureau of Ocean Energy Management, Regulation and Enforcement, which is conducting the joint inquiry with the Coast Guard."*

This was recently changed following Bob Dudley's replacement of Hayward to a reward system based on achieving safety goals.[19] Faced with accusations that BP precipitated the Gulf of Mexico oil spill by placing profits before safety, Dudley reportedly sent an internal memo to the staff directing that safety would be the sole criterion for rewarding employee performance in its operating business for the fourth quarter; however, this change has been received with considerable skepticism as a way of effecting change in corporate safety culture—but certainly is a step in the right direction.

Hayward's CEO of Exploration and Production – the bread and butter producer of the bottom line, made it clear that BP was at the frontier and ready to take on risks that other companies would pass on. BP placed its bets and rolled the dice for the biggest rewards, encouraged by their own success, even though these plays involved the deepest waters and riskiest oil reservoirs—High Pressure High Temperature (HPHT) fields that are much more problematic to safely drill in and to complete wells. The risks are enormous but so are the rewards, and they were making a ton of money to prove it because they had the know-how and guts to take it on. Perhaps it was gold-fever, or perhaps they sincerely believed they knew what they were doing—in any event, the perspective was lost and its consequent price is enormous.

---

[17] Greg Goodale, "A new framework for success," Horizon—The Global Publication for BP People, Issue 3, May 2008, 3, http://nw-assets.s3.amazonaws.com/pdf/horizon_magazine_issue_3_2008.pdf.

[18] Joel Achenbach, "At BP, safety vs. cost-saving," Washington Post, October 9, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/08/AR2010100806687.html.

[19] Guy Chazan and Dana Mattioli, "BP Links Pay to Safety in Fourth Quarter," Wall Street Journal, October 19, 2010, http://online.wsj.com/article/SB10001424052702303496104575560422023190664.html. http://online.wsj.com/article/SB10001424052702303496104575560422023190664.html?mod=WSJ_topics_obama.

On February 1, 2007, the Board of BP announced that it had appointed Andy Inglis as a managing director of the BP Group.[20] He also succeeds Tony Hayward as chief executive of BP's Exploration & Production (E&P) business. Inglis, who is a Chartered Mechanical Engineer, a Fellow of the Royal Academy of Engineering, and a Fellow of the Institution of Mechanical Engineers, put forth E&P's vision in a speech later that year at the Sanford Bernstein 4th Annual Strategic Decisions Conference.[21] Much like the fictitious Captain James T. Kirk, Commander of the Starship Enterprise, whose mission was to explore space...*the final frontier*, so too is BP's.[22] Remember how it goes:

> *These are the voyages of the Starship Enterprise. Its five-year mission: to explore strange new worlds; to seek out new life and new civilizations; to boldly go where no man has gone before…*

During his short tenor at the helm of E&P, Inglis often struck a similar note in his speeches. He spoke in terms of BP's frontier expertise and experience. For example, at the aforementioned 4th Annual Strategic Decisions conference, he explained:

"…BP operates on the frontiers of the energy industry - geographically, technically and in terms of business partnerships. Challenges and risks are our daily bread. We can't be sure what the next challenge will be, but the important thing is to have the capability to meet multiple challenges. I have confidence that BP has that capability and I hope I can pass that confidence on to you today…. Companies like BP increasingly work in extreme weather conditions, in increasingly deep water and in complex rock formations. Our projects get more complex and multi-layered every year…"

"How BP's Implements The Five Competitive Advantages. The critical thing is to exploit the distinctive advantages that the IOC[23] experience brings with it. And I think there are five key advantages. ***First, taking major risks*** *(emphasis added); second, assembling large and diversified portfolios; third, building deep intellectual and technical capability; fourth, making best use of global integration; and finally, forging long-term, mutually beneficial, partnerships."*

> *"So let me move on to look at those potential advantages of being an IOC – and how BP is seeking to implement them. So first – risk. As a leading IOC, we take and manage* ***big risks for commensurate rewards*** *(emphasis added). We take exploration risks, capital risks and ongoing operations risks…"*
>
> *"And another example of risk taking is the Gulf of Mexico. Twenty years ago we could drill in water depths of 1,500 ft to reservoirs at 15,000 ft. Today we are drilling in over 10,000 ft of water and reaching reservoirs nearly 35,000 ft deep. Pushing the technical boundaries is not without challenges, as we have found with the recent issues with the Thunderhorse (sic) Project.* ***This is right at the edge of the technical envelope*** *(emphasis added) and providing many lessons for other projects."*

---

[20] BP Press Office, "Andy Inglis Joins BP Board And Succeeds Tony Hayward as Head of Exploration & Production," http://www.bp.com/genericarticle.do?categoryId=2012968&contentId=7028141.

[21] Andy Inglis, "The role of an International Oil Company in the 21st Century," Sanford Bernstein 4th Annual Strategic Decisions Conference, Sept. 25, 2007, http://www.bp.com/genericarticle.do?categoryId=98&contentId=7037044.

[22] The sophistication of deepwater oil exploration and drilling technology is often compared to that of NASA and the space program.

[23] International Oil Company (IOC)

Once again being at the frontier in large basins has enabled us to create incumbent positions for the future. As this slide shows, the deep-water Gulf of Mexico resources have increased more than 100 fold since 1985, from less than 150 million barrels to nearly 19 billion barrels, with BP holding over 20 percent share. And there are an estimated 25 to 40 billion barrels yet to be found."

In the aftermath of The Spill, however, the spokesman for this bold vision became a casualty of overzealous risk-taking. The news-byte read: Exploration and Production division head Andy Inglis will leave the company as part of a broad restructuring designed to improve safety and rebuild confidence after the disastrous Gulf of Mexico blowout and oil spill, BP said Wednesday. [24] Is this the beginning of a new safety culture?[25] Well perhaps, but then again, Mr. Dudley is in denial that cost-cutting had anything to do with causing The Spill—at least in print. Perhaps he truly believes this or perhaps he is simply holding true to BP's party-line response as developed by their own investigators under the purview of the BP legal department—time will tell.

And, in the aftermath of *The Spill*, Hayward admitted that BP did not have all the equipment needed to stop the leak from its Macondo well. Six weeks after the blowout, Tony Hayward mused that "What is undoubtedly true is that we did not have the tools you would want in your tool-kit." He accepted it was "an entirely fair criticism" to say the company had not been fully prepared for a deep-water oil leak, but was quick to add that the containment effort on the surface, he said, had been "very successful" in keeping oil away from the coast (…after all, *the GOM is a very big ocean*). "Considering how big this has been, very little has got away from us," Mr. Hayward boasted. But in trying to plug the leak, BP had been reaching for many of the same techniques used to control the Ixtoc 1 blow-out in the Gulf of Mexico 31 years ago.[26] They found themselves in very deep water, relying on old oil boom technology and untried oil collection *inventions* that, in desperation, they were making-up as they went along. The ongoing criminal probe will consider, *inter alia*, BP's drill permit that grossly misrepresented the size of a spill that BP was prepared to handle. Moreover, former Administrator of the Environmental Protection Agency Carol Browner and Congressman Ed Markey (D-MA) both accused BP of having a vested financial interest in downplaying the size of the leak in part due to the fine they will have to pay based on the amount of leaked oil.[27]

It should be now patently obvious that Mr. Hayward's attempt to put a smiley-face on spill containment, BP's disingenuous press releases about estimated flow rates, BP's utter lack of preparedness, and, following in the footsteps of the Royal Navy's Admiral Horatio Nelson in the 1801 battle of Copenhagen—who continued to press-on by *turning a blind eye to the risk*, Tony Hayward set the course for his own downfall—and an assignment in Siberia. But will his departure change BP's safety culture?

---

[24] James Herron, "BP's E&P Boss Steps Down In Major Safety Shakeup," Dow Jones Newswire, Sept. 29, 2010, http://online.wsj.com/article/BT-CO-20100929-708863.html.

[25] According to Bob Dudley, "*BP is a company that is coming back from a near-death experience*," Mr. Dudley said in a telephone interview, one of several he gave on Thursday to introduce himself and describe his vision for the company. "*We are not going to run away from risk. We are going to make sure we are among the best in the world at managing risk going forward.*" Clifford Krauss, "New BP Chief Seeks a 'Fast Evolution," New York Times, Sept. 30, 2010, http://www.nytimes.com/2010/10/01/business/01bp.html.

[26] Ed Crooks, "BP 'not prepared' for deep-water spill," Financial Times, June 2, 2010, http://www.ft.com/cms/s/0/e1e0e21c-6e53-11df-ab79-00144feabdc0.html.

[27] "Government, BP spar over size of oil leak," CNN.com, May 31, 2010, http://edition.cnn.com/2010/US/05/30/oil.spill.bp.government/.

In response to the continued delay and time involved for design and fabrication of the ill-conceived "Top Hat" containment contraption in the midst of *The Spill*, University of Texas engineering professor Paul Bommer, a member of the Coast Guard team and head of the *Flow Rate Technical Group* that was trying to determine how much oil was actually leaking, put it this way, "It's not something you just go to Wal-Mart and buy." True, but then again, the RMS Titanic was unsinkable…who needs lifeboats…full speed ahead…we need to set the record…and so forth.

But does this make Andy Inglis, Tony Hayward, and Lord Browne "bad men," or for that matter, Titanic's Captain Edward Smith (at least he went down with his ship)? Professor Bob Bea doesn't think so […*these are not bad men*…60 Minutes, May, 16, 2010], nor does CBS's Steve Tobak[28] think so…as he puts it:

> *"…is BP's **Tony Hayward** a bad CEO? Has he handled the gulf oil spill crisis poorly? I don't think so. I may be the only person on the planet with that opinion, aside from Hayward's family, but I really don't think so. Frankly, I think Hayward has found himself in the mother of all no-win situations."*

In a Washington Post news-byte[29] headlined, "Oil spill reveals the dangers of success," Bob Samuelson notes that before the accident, deepwater drilling seemed to be a technological triumph. About 80 percent of the Gulf of Mexico's recent oil production has come from deepwater operations, defined as water depths exceeding 1,000 feet, and accounts for about 30% or more of U.S. production. In the wake of accusations of cost-cutting by BP, careless rig operators and lax regulators as plausible culprits in the blowout, Samuelson raises the question of whether the success of deepwater drilling led to failure. Did success sow overconfidence? Did continuing achievements obscure the dangers? As he observes:

> *"One theory of the oil spill is that the deepwater technology is inherently so complex and dangerous that it can't really be understood or regulated. The safety record before the BP spill seems to rebut that. The problem is that the system broke down. Careless mistakes were made. Or regulators were co-opted by industry. Judgments were botched. Something. The post-crisis investigations will presumably fill out the story. But they may miss the larger question of why… It is human nature to celebrate success by relaxing. The challenge we face is how to acknowledge this urge without being duped by it."*

Is it just deepwater drilling and ill-defined risk, or is the problem more systemic? Following on the heels of BP's Texas City refinery tragedy, Jordan Barab, deputy assistant secretary for the U.S. Occupational Safety and Health Administration said OSHA zeroed in on safety problems at the nation's refineries.[30] The results were "deeply troubling." Inspectors found a significant lack of compliance and the same violations repeated at refinery after refinery. "We are sick of the industry bragging about their safety record when children are burying their parents." Obviously, the status quo is not working. Cost-cutting and deferred maintenance have been offered as the root cause of

[28] Steve Tobak, "In Defense of BP CEO Tony Hayward," CBS BNET Blog, June 10, 2010, http://www.bnet.com/blog/ceo/in-defense-of-bp-ceo-tony-hayward/4780.

[29] Robert Samuelson, "Oil spill reveals the dangers of success," Washington Post, June 7, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/06/AR2010060602925_pf.html.

[30] Les Blumenthal, "*Safety record of oil and gas industry is weak, OSHA says*," Miami Herald, June 10, 2010, http://www.miamiherald.com/2010/06/10/v-print/1674080/safety-record-of-oil-and-gas-industry.html.

not only the Deepwater Horizon incident, but also for the 2005 Texas City refinery explosion and the 2006 Alaska Pipeline Oil spill.[31]

Joe Nocera of the New York Times[32] writes:

"We have to get the priorities right," the chief executive of BP said. "And Job 1 is to get to these things that have happened, get them fixed and get them sorted out. We don't just sort them out on the surface, we get them fixed deeply." The executive was speaking to Matthew L. Wald of The New York Times, vowing to recommit his company to a culture of safety. The oil giant was adding $1 billion to the $6 billion it had already set aside to improve safety, the executive told Mr. Wald. It was setting up a safety advisory panel to make recommendations on how the company could improve. It was bringing in a new man to head its American operations — the source of most of the company's problems — who would make safety his top priority. And on, and on."

"That interview didn't take place this week — a week in which BP was excoriated in Congress for the extraordinary safety lapses that led to the Deepwater Horizon rig disaster, while also being strong-armed by President Obama into putting $20 billion in escrow to compensate victims. No, the interview took place nearly four years ago, after BP's previous disaster on American soil, when oil was discovered leaking from a 16-mile stretch of corroded BP pipeline in Prudhoe Bay in Alaska. And that was just a year after a BP refinery explosion in Texas City, Tex., killed 15 workers and injured hundreds more."

"Nor was the chief executive in question Tony Hayward, who spent Thursday before a Congressional panel ducking tough questions and evading personal responsibility — while insisting, absurdly, that as head of the company he had been "laser-focused" on safety. No, the interviewee was his predecessor and mentor John Browne, who had spent nearly 10 years at the helm of BP before resigning in May 2007."

"Do you remember the Prudhoe Bay leak and the Texas City explosion? They were big news at the time, though they quickly faded from the headlines. BP was fined $21 million for the numerous violations that contributed to the Texas City explosion, and it was forced to endure a phased shutdown of its Alaska operations while it repaired the corroded pipeline, which cost it additional revenue."

"In retrospect, though, the two accidents represented something else as well: they were a huge gift to the company. The fact that these two accidents — thousands of miles apart, and involving very different parts of BP — took place within a year showed that something was systemically wrong with BP's culture. Mr. Browne had built BP by taking over other oil companies, like Amoco in 1998, and then ruthlessly cutting costs, often firing the acquired company's most experienced engineers. Taking shortcuts was ingrained in the company's culture, and everyone in the oil business knew it."

"The accidents should have been the wake-up call BP needed to change that culture. But the mistakes and negligence that took place on the Deepwater Horizon in the Gulf of Mexico — which are so profound that everyone I spoke to in the oil business found them truly inexplicable — suggest that the two men never did much more than mouth nice-sounding platitudes."

[31] Abrahm Lustgarten, "Furious Growth and Cost Cuts Led To BP Accidents Past and Present," ProPublica, October 26, 2010, propublica.org.

[32] Joe Nocera, "BP Ignored the Omens of Disaster," New York Times, June 18, 2010, http://www.nytimes.com/2010/06/19/business/19nocera.html?ref=joe_nocera&pagewanted=print.

Figrue 3.1 – BP Thunder Horse platform in the GOM severely listing and in danger of sinking.

Are these incidents just a part of *the normal cost of doing business* in the myopic eyes of management – the byproduct of seeking to close the competitive gap at all costs and *claiming the prize*? Was it worth the risk of nearly sinking the Thunder Horse platform, BP's largest producer and one-of-a-kind drilling and production facility in the GOM,[33] when poor QA/QC and HOE was nearly their undoing? [34]

Sarah Lyall of the New York Times writes:[35]

"Towering 15 stories above the water's surface, Thunder Horse was meant to be the company's crowning glory, the embodiment of its bold gamble to outpace its competitors in finding and exploiting the vast reserves of oil beneath the waters of the gulf. Instead, the rig, which was supposed to produce about 20 percent of the gulf's oil output, became a symbol of BP's hubris. A valve installed backward had caused the vessel to flood during the hurricane, jeopardizing the project before any oil had even been pumped."

"Other problems, discovered later, included a welding job so shoddy that it left underwater pipelines brittle and full of cracks. "It could have been catastrophic," said Gordon A. Aaker Jr., a senior engineering consultant on the project. "You would have lost a lot of oil a mile down before you would have even known. It could have been a helluva spill — much like the Deepwater Horizon."

"The problems at Thunder Horse were not an anomaly, but a warning that BP was taking too many risks and cutting corners in pursuit of growth and profits, according to analysts, competitors and former employees. Despite a catalog of crises and near misses in recent years, BP has been chronically unable or unwilling to learn from its mistakes, an examination of its record shows."

[33] The BP operated Thunder Horse started production in 2008. With the capacity to process more than a quarter of a million barrels of oil per day and 200 million cubic feet per day of natural gas, Thunder Horse is currently the largest single producing field in the Gulf of Mexico. Today, with seven wells online, it is producing around 300,000 mboed . "Deep-water production," http://www.bp.com/sectiongenericarticle.do?categoryId=9025122&contentId=7047805. Million Barrels Oil Equivalent per Day (mboed).

[34] QA/QC = Quality Assurance/Quality Control; Human and Organizational Errors (HOE)

[35] Sarah Lyall, "In BP's Record, a History of Boldness and Costly Blunders," New York Times, July 12, 2010, http://www.nytimes.com/2010/07/13/business/energy-environment/13bprisk.html?pagewanted=3.

"They were very arrogant and proud and in denial," said Steve Arendt, a safety specialist who assisted the panel appointed by BP to investigate the company's refineries after a deadly 2005 explosion at its Texas City, Tex., facility. "It is possible they were fooled by their success."

"Indeed, there was a great deal of success to admire. In little more than a decade, BP grew from a middleweight into the industry's second-largest company, behind only Exxon Mobil, with soaring profits, fat dividends and a share price to match."

Atlantis, Neptune, Mad Dog, Holstein, and Crazy Horse (later re-named Thunder Horse) are some of the names given to the GOM's richest deepwater fields—exploration successes credited to BP's adoption of an "elephant-hunt" strategy that focuses only on potentially the biggest and most lucrative prospects while ignoring the rest.[36] BP's oil explorers decided on this new strategy that focuses all the company's energy on seeking big reserves, dubbed "elephants," and the company put big resources behind this new approach to ensure its success. Following in the wake of the Thunder Horse problems, Kenny Lang, BP's head of Gulf of Mexico operations reportedly observed, "We're operating at the edge of what is known," and "When you're at the edge, you're creating knowledge. And when you create knowledge, you sometimes stub your toe." So what caused the Thunder Horse to almost sink—*an unlikely chain of events.*[37] And why did much of the subsea production piping and manifolds have to be replaced—bad welds due to *an unforeseen chemical reaction.*[38]

When you've pushed "the envelope" too far, bad things will happen. Knowing when you've crossed "the line" is difficult if you don't know where the line is in the first place, and in deepwater frontier, there are many lines to cross. The dearly paid-for history of lessons learned from a long lineage of industrial catastrophes can serve as a chart in unknown waters and provide guidance for safe operations when exploring the frontiers of knowledge. However, preventing *impossible failures* takes a bit more than reliance on past experiences—be they good (successes) or bad (failures). Both *lagging and leading* indicators must be fully considered and evaluated.

4.0 Impossible Failures

Before BP's Alaska North Slope and GOM oil spills, Professor Bea[39] wrote:

"*Most failures involved never-to-be-exactly-repeated sequences of events and multiple breakdowns or malfunctions in the components that comprise a 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 barriers had not been breached, then the accident or failure would not have occurred. Experience adequately showed that it was extremely difficult, if not impossible, to recreate accurately the time sequence of the event that actually 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 conformational biases are common as are distorted recollections. Stories told from a variety of viewpoints*

[36] David Greising, "Troubles Run Deep on Gulf Oil Platform**,"** Chicago Tribune, May 28, 2007, http://www.redorbit.com/news/science/948325/troubles_run_deep_on_gulf_oil_platform/index.html.
[37] Ibid., Greising.
[38] Ibid., Greising.
[39] Robert G. Bea, "Learning from Failures: Painful Lessons from the Recent History of Failures of Engineered Systems," University of California, Berkeley, December, 2005

involved in the development of a failure were the best way to capture the richness of the factors, elements, and processes that unfold in the development of a failure."

The tragic and preventable explosion and fire aboard the Deepwater Horizon drilling rig was, in the minds of some, an ***impossible failure***—it was characterized as 'inconceivable,' 'unprecedented,' and 'unforeseeable.'[40] In the immediate aftermath, the failure of the so-called last-resort "fail-safe" device, the Blowout Preventer (BOP), was targeted as the cause: "If that would've worked," a senior oil industry executive said of the blind shear ram, "that rig wouldn't have burned up and sunk."[41] However, as one member of the DHSG astutely observed, "isn't that like blaming a malfunctioning fire sprinkler for causing the fire that burns down your house?" World renowned loss prevention expert and contributing member of the DHSG, Professor Trevor Kletz, recently presented a paper[42] addressing errors commonly made in accident investigation. Professor Kletz observed that one of the most common errors is to report that such an event has never occurred before. Moreover, simply placing the blame on human error, blaming individuals, or even worst, thinking of a possible cause and then seeking evidence to support it, will not produce meaningful results. The most important aspect of incident investigations is arriving at needed "actions."

Figure 4.1 – 1999 BP Advertisement

So as the investigation of the Deepwater Horizon tragedy continues to unfold and the causes of this *impossible failure* are illuminated, we should ask ourselves how much more spill oil will have to wash up on American shores before we get it right? And, more importantly how do we get it right – how can we measure and manage the associated risks of deepwater oil drilling and production? Are the risks acceptable and can the risks be successfully managed? Can we do this safety?

The answer is, I think, YES, we can IF we can hold true to a common vision and apply common sense. We know better – we do know, or ought to know, how to go about assessing hazards and

[40] "BP calls blowout disaster 'inconceivable,' 'unprecedented,' and 'unforeseeable,'" ClimateProgress, May 4, 2010, http://climateprogress.org/2010/05/04/bp-calls-blowout-disaster-%E2%80%98inconceivable%E2%80%99-%E2%80%98unprecedented%E2%80%99-and-unforeseeable/.

[41] Michael Moss and Henry Fountain, "Regulators Failed to Address Risks in Oil Rig Fail-Safe Device," New York Times, June 20, 2010, http://www.nytimes.com/2010/06/21/us/21blowout.html.

[42] Trevor Kletz, "Some Common Errors in Accident Investigations," SARS Conference, London, October 14, 2010.

managing risk…and we are smart enough to know when there is insufficient data and evidence to support risky decisions. And we know how to characterize high reliability organizations (HROs). The problem, of course, is rooted in the perception of risk solely in terms of reward, i.e., in terms of only good consequences and not the potential catastrophic ones…by those decision-makers who, with a dutiful but perhaps lustful eye on the bottom line and, in the glimmer of black gold, with one eye on the prize and crossed fingers behind their backs, and buoyed by the hubris of past successes, may wrongfully decide that the best course to set is full speed ahead…and damn the torpedoes…because it has always worked before…well at least most of the time. We should know by now that "*If it ain't broke, don't fix it*" doesn't work! And we should also know that "*Organizations have no memories.*"[43] What we seem to lose track of, however, is the meaning of prudence.

Following BP's Texas City refinery explosion – characterized as *the worst industrial accident in a decade*,[44] CSB Chairman Carolyn W. Merritt said:[45]

> *"It is my sincere hope and belief that our report and the recent Baker report will establish a new standard of care for corporate boards of directors and CEO's throughout the world. Process safety programs to protect the lives of workers and the public deserve the same level of attention, investment, and scrutiny as companies now dedicate to maintaining their financial controls. The boards of directors of oil and chemical companies should examine every detail of their process safety programs to ensure that no other terrible tragedy like the one at BP occurs."*

Figure 4.2 – The Deepwater Horizon Platform.[46]

[43] Trevor Kletz, Lessons from Disaster: How Organizations Have No Memory and Accidents Recur (Houston: Gulf Professional Publishing, 1993).

[44] **"**BP chided in report on fatal Texas fire: Internal papers show oil company aware of hazards before 2005 explosion at refinery;" CNNMoney.com, October 31, 2006, http://money.cnn.com/2006/10/30/news/companies/bp_refinery/index.htm. "*Internal BP documents reveal the oil company's knowledge of "significant safety problems at the Texas City refinery," months or years before the March 2005 explosion that killed 15 workers and injured more than 170 others, according to preliminary findings released Monday by the U.S. Chemical Safety Board*."

[45] "U.S. Chemical Safety Board Concludes "Organizational and Safety Deficiencies at All Levels of the BP Corporation" Caused March 2005 Texas City Disaster That Killed 15, Injured 180," U.S. Chemical Safety Board, March 20, 2007, http://www.csb.gov/newsroom/detail.aspx?nid=205.

As Professor Bea has pointed out, the human and organizational factor (HOF) challenge to designing and maintaining high-level quality and reliably engineered systems is not an engineering problem *per se* but rather is considered a management problem. Often, the discrimination has been posed as technical and non-technical. Case histories of recent major failures clearly indicate that both engineers and management have a critical role to play if the splendid history of successes and achievements is to be maintained or improved. Through integration of technologies from the physical and social sciences, engineers and management can learn how to better recognize, measure, and manage risk. The challenge is to wisely apply what is known. In the end, the broader *lessons learned* from the Macondo blowout may not turn out to be *new lessons*, but rather *newly relearned* ***lessons***—a repeat of what has been shown to be a commonality in all impossible failures. To continue to ignore the human and organizational issues as an explicit part of engineering is to continue to experience things that engineers, regulators, industry, and the public do not want to happen, and the occurrence of which can be more effectively reduced and managed *looking forward.*

BP's own internal report,[47] released on September 8, 2010, concluded that:

> *The accident on April 20, 2010, involved a well integrity failure, followed by a loss of hydrostatic control of the well. This was followed by a failure to control the flow from the well with the BOP equipment, which allowed the release and subsequent ignition of hydrocarbons. Ultimately, the BOP emergency functions failed to seal the well after the initial explosions.*

The BP investigation team was headed by Mark Bly, BP's head of safety and operations and who was recently elevated to a vice president. In a subsequent news briefing after the report was released, investigation leader Bly was asked whether BP sacrificed safety to save money, as other investigators have alleged. Bly replied that his team did not find anything to support that conclusion.[48] Instead Bly pointed to Transocean and noted that the rig crew *"failed to recognize and act on the influx of hydrocarbons into the well"* when it might still have been possible to cut off the flow. Moreover, with regard to well design, Bly noted that "*based on the report it would appear unlikely that the well design[49] contributed to the incident*, *as the investigation found that the hydrocarbons flowed up the production casing through the bottom of the well.*"

On November 8, 2010, the lead investigator and chief counsel for the National Commission[50] investigating the BP oil spill, Fred H. Bartlit, Jr., Esq., a prominent trial lawyer and who has defended oil giant AMOCO more than once in the past, announced to the commissioners that he found no evidence that anyone involved in drilling the doomed well had taken safety shortcuts to save money. [51] This disputes findings of other investigators, including members of Congress,[52] who have previously charged that BP and its contractors, Transocean and Halliburton, had cut corners to

---

[46] photo credit: thehistorypages.aimoo.com

[47] "Deepwater Horizon Accident Investigation Report," BP PLC, September 8, 2010.

[48] Steven Mufson and Joel Achenbach, "In its report on the gulf oil spill, BP spreads the blame," Washington Post, September 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/08/AR2010090807789.html.

[49] Well design and completion is addressed in Section 2 of "Deepwater Horizon Accident Investigation Report," BP PLC, September 8, 2010.

[50] http://www.oilspillcommission.gov.

[51] Steven Mufson and Joel Achenbach, op. cit.

[52] Congressman Edward Markey; *"When the culture of a company favors risk-taking and cutting corners above other concerns, systemic failures like this oil spill disaster result without direct decisions being made or tradeoffs being considered."* Rep. Edward J. Markey (D-Mass.), a senior member of the House Energy and Commerce Committee. **markey**.house.gov/

speed completion of the well, which cost $1.5 million a day to drill. Bartlit stated that "To date we have not seen a single instance where a human being made a *conscious decision* to favor dollars over safety" (emphasis added). Nevertheless, Commission Co-chair William Reilly earlier Monday (November 8th) declared that *"safety concerns took a back seat to the pursuit of the remarkable returns available offshore."* [53] And this morning at the outset of the second day of the panel's two-day hearing, Reilly said *"Whatever else we learned and saw yesterday, it was emphatically not a culture of safety on that rig."* [54]

Bartlit announced he has accepted BP's claim that its decision to use fewer barriers to protect the sides of the well likely had little to do with the direct cause of the accident.[55] However, commission investigators also reportedly said the decision to use the cheaper design, called a long string, still could have had serious implications in leading to the disaster. The long-string design, rather than a liner raised the risk of mud contaminating the cement that was supposed to seal the well closed and also may have forced BP to use less cement than advisable because of concerns about heat and pressure. However, Reilly summed it up this way, saying the commission probe has revealed a "ghastly" story of *"one bad call after another,"* including the decision to proceed after failed cement tests, well pressure tests that were mistakenly judged a success and others. And Bob Graham, in a separate statement, added, *"The problem here is that there was a culture that did not promote safety, and that culture failed."*[56]

5.0 Conclusion

As described by Exxon-Mobil CEO Rex Tillerson in response to questions before the National Commission, an organization's safety culture takes time to develop and has to be grown from within—you can't buy it or import it—it has to be nurtured from within the organization. Exxon-Mobil has been at it now for more than twenty years, after learning the hard way and paying for its complacency and risk management failures that led to the Valdez spill. Since that time, Exxon-Mobil has turned the corner and introduced many positive innovations to improve safety culture, such as their Operations Integrity Management System (OIMS), introduced in 1992 as an integral part of their overall safety management system.

In contrast, at the time of the Macondo blowout, BP's corporate culture remained one that was embedded in risk-taking and cost-cutting—it was like that in 2005 (Texas City), in 2006 (Alaska North Slope Spill), and, as discussed herein, remained unchanged in 2010 (GOM, "The Spill"). Perhaps there is no clear-cut "evidence" that someone in BP made a *conscious decision* to put costs before safety; nevertheless, that misses the point. It is the underlying "***unconscious mind***" [57] that

[53] Steven Mufson, "Cost didn't drive decisions on oil rig, spill panelist says," Washington Post, November 9, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/08/AR2010110806296.html.

[54] Ben Geman, "Spill panel: BP, firms made 'egregiously bad' decisions, need revamp," The Hill, November 10, 2010, http://thehill.com/blogs/e2-wire/677-e2-wire/128319-spill-panel-chief-bp-transocean-and-halliburtion-need-top-to-bottom-reform.

[55] David Hammer, "Oil Spill Commission: Gas that blew out BP well shot up center, not open side space," Times Picayune, November 8, 2010, http://www.nola.com/news/gulf-oil-spill/index.ssf/2010/11/oil_spill_commission_gas_that.html.

[56] Siobhan Hughes, "Spill Panel Says Rig Culture Failed on Safety," Wall Street Journal, November 10, 2010, http://online.wsj.com/article/SB10001424052748704635704575604622510434324.html.

[57] The unconscious mind is that part of the mind which gives rise to a collection of mental phenomena that manifest in a person's mind but which the person is not aware of at the time of their occurrence, generally attributed to 18th century German philosopher Sir Christopher Riegel.

governs the actions of an organization and its personnel. Cultural influences that permeate an organization and manifest in actions—actions that can either promote and nurture a high reliability organization (HRO), and that are indicative of a strong safety culture, or actions reflective of complacency, risk-taking, and a loss of situational awareness from pushing the envelope too far in trying to close the competitive gap.

The lessons are there to be learned if only the student would pay attention and take them to heart. Sometimes the lessons are taken to heart and meaningful changes are effected, and sometimes the lessons are ignored—the *why* this is not so much of a mystery—effecting meaningful organizational-behavioral change is the tricky part...a conundrum that regulators, researchers, and 'teachers' are seeking answers to as America and the world keep demanding more and more black-gold. Lets' redouble our efforts to keep it out of the Gulf of Mexico—after all, nobody wants to kill anymore of those endangered GOM walruses—they are getting very hard to find!

Figure 5.1 – Walrus.[58]

[58] Photo Credit: *NOAA-walrus.*

Appendix D

Deepwater Well Complexity – The New Domain

David M. Pritchard and Kevin D. Lacy

1.0 Forward

In light of the Macondo blowout and in order to ensure safer deepwater operations this paper suggests there is an industry need to better assess risks and monitor well operations in addition to standardizing the design of complex deepwater wells.

Examining the metrics of deepwater operations in the Gulf of Mexico indicates that there routinely have been difficulties with some categories of complex deepwater wells.

Given the severe consequences of failure the Deepwater Gulf of Mexico (GOM) industry should be guided by the principles established by Professor Andrew Hopkins wherein high-performing organizations that cannot suffer failures must fully exhibit "collective mindfulness," of major failures in conducting their work.[1]

The drilling culture that has been relatively successful in taking on new technical challenges and avoiding major incidents has historically accepted some level of failure that either time or cost can mitigate. As seen by the severe consequences of the Macondo incident the approach to drilling deepwater wells has to fundamentally change. Frequently culture is called "the way we work" and in that vein the current drilling culture is fundamentally flawed when we impose a zero failure approach.

It is further evident that in some categories of deepwater wells (Section 4.0), industry performance has become worse and the final proof is the Macondo catastrophe itself. It is clearly understood that there are many causal factors around this incident. Have wellbore instability incidents become so routine that they were actually deemed normal? Did this relax the Human Controllable Factors? Did this lead to unwise management decisions? Did this result in the lack of supervision and the failure to monitor the real time data? Some of these issues may never be resolved which is why it is even more incumbent on the industry to recognize where the problems exist and design wells which deal with the uncertainties of the safe drilling margin[2] and address these risks accordingly. It is fundamental to understand that uncertainties drive risk and the narrower the range of uncertainties in operations, the easier to manage the risk. Risk can never be eliminated, but it can be successfully managed.

[1] Andrew Hopkins, bio web page, http://www.professorandrewhopkins.com/biography.
[2] David M. Pritchard and Kenneth Kotow, "The New Domain in Deepwater Drilling: Applied Engineering and Organizational Impacts on Uncertainties and Risk," SPE/IADC Joint Sessions, February 2010.

The discussions herein indicate that in some categories of complex wells, wellbore stability events are as high as 10 % of the total deepwater well time. Blowout prevention equipment was never intended to become a routine execution tool and in some of the more complex deepwater wells, time spent on the BOP's has been increasing dramatically.

2.0 The Consequence Of Failure

The Macondo catastrophe clearly indicates the industry does not fully grasp the riskiness of Deepwater nor have we adequately estimated the consequence of failure.

One of the challenges of applying traditional static risk analysis to something as dynamic and uncertain as the deepwater subsurface environment and complex operations is the lack of truly statistical meaningful data. The industry cannot continue to accept any quantifiable risk in Deepwater (DW) as miniscule.

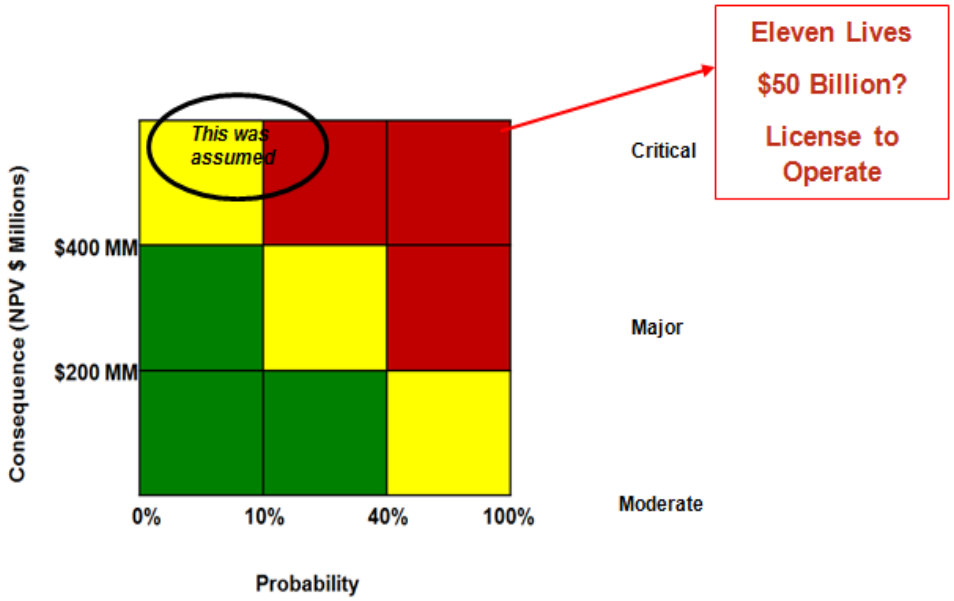


Figure 2.1 – Traditional Overview of GOM Deepwater Risk and Consequence.[3]

While it is debatable what the actual numerical value of the risk is for a major blowout in DW we have evidence it is not zero. Additionally the outcome of a full blow out, loss of rig and complete loss of well control for 87 days is a scenario no one saw as remotely possible. This appreciable risk and significant negative outcome is unacceptable and clear evidence for change.

People make rationale choices given their surroundings and perception of the risks and the possible personal consequences. With certainty, the BP employees and contractors involved did not intentionally underestimate the risk. However in hindsight there is absolute evidence many decisions were not consistent with the true risks and the potential consequences. We need no further evidence to support the need for major change.

[3] Kevin D. Lacy, "Restoring Integrity to the GOM Deepwater," SPE Deepwater Drilling and Completions Conference, Presentation, Galveston, Texas, October 5-6, 2010.

Where does the industry begin to recognize the problem, risk and consequences – the metrics – the industries own measures of success - or failure?

3.0 The Macondo Incident And Organizational Issues

In order to think past the Macondo incident and restore confidence to the DW industry, we must consider the following: This new DW domain has no industry standards and yet is our most technically demanding.

The DW rig fleet has increased by 300 %. Has competency and reliability increased in the same manner?

There is persistently high Non-productive time in DW operations as further discussed in this paper.

- Are these challenges and warning signs being ignored?
- Why does the industry accept the current failure rate on BOP's and controls?

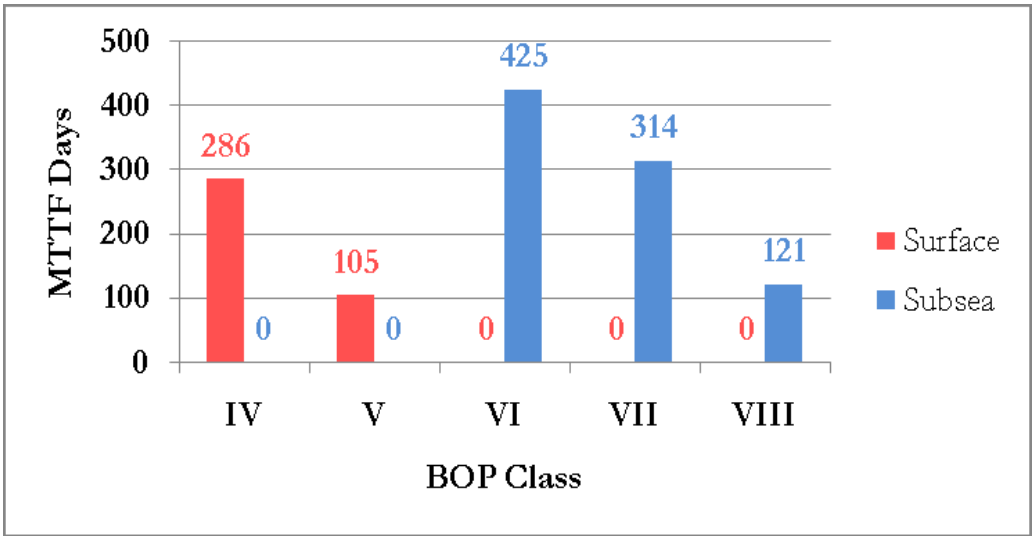


Figure 3.1 – MTTF by BOP Class.[4]

In 2008, several industry groups created a task force to define the work scope for a joint industry project to study BOP reliability experienced for wells drilled in the US Gulf of Mexico from 2004 to 2006. The high level result of the study indicated that even though improvements were noted over time, and that subsea systems actually had better failure rates than surface systems. Nonetheless the question must be asked and answered: Given the consequences of failure demonstrated by the Macondo incident, are the rates noted in Figure 3.1 – MTTF by BOP Class acceptable? There is also a degradation of failure rates by the more complex, deeper water systems as delineated by Class VIII systems: the most complex of deepwater systems.

[4] Jeff Sattler, "JIP study on BOP reliability 2004-2006: subsea control systems were most prone to failure," Drilling Contractor, September 8, 2010, http://drillingcontractor.org/jip-study-on-bop-reliability-2004-2006-subsea-control-systems-were-most-prone-to-failure-6875.

Table 3.1 – BOP Systems Defined by Class.[5]

Installation	Class	Annulars	Rams
Surface	**IV**	**1**	**3**
	V	**1**	**4**
Subsea	**VI**	**2**	**4**
	VII	**1**	**6**
	VII	**2**	**5**
	VIII	**2**	**6**

- Why are our critical systems so heavily people dependent?
- Can the industry really expect to be safe and successful with the current relationship model between:
- Operators and Drilling Contractors?
- The regulatory agencies being undermanned and technically thin in DW experience.?
- Operators and other service providers?
- Failing to recognize that the operator is in fact… the operator and fully accountable?

In regard to the regulatory agencies the relationship has now become very openly political and the "genie is out of the bottle" – it will become even more political and more prescriptive. That will be a major problem as the competency to develop a DW GOM standard does not reside within the reformed BOEMER. In fact it is already thin within Operator ranks and likely part of the root cause of the Macondo incident.

An excerpt from a portion of the BP program actually relies on default approvals, and this is not uncommon in GOM DW operations:

9.2.4 Surface Cement Plug

1. If cement job is not successful: (no returns or lift pressure seen).

• Set wear bushing

• Run IBC-CBL log

• Wait on decision to do remedial work (MMS and BP)

2. If cement job is successful (partial returns or lift pressure seen) or IBC/CBL log and required remedial work is completed.

3. RIH to 8367' and displace to seawater:

• Run 3-1/2" (1000'+) stinger x 5-1/2" DP to above the wellhead (no mule shoe I open ended pipe)

• Ensure MMS Departure to set deeper plug is approved (if departure does not get approved, displacement & 300' cement plug will be completed after LOS is set at 5800?)

• Monitor well for 30 minutes to ensure no flow

[5] Sattler, op. cit.

• Pull wear bushing if it was set

4. Set a 300' cement plug from 8367' - 8067' (if approved)

5. Wait on cement to set and tag top of cement with 15k down

• Pump a nerf ball behind cement job

6. POOH retrieve wear bushing

7. Prepare to run lead impression tool and lockdown sleeve

Note: Drilling program will be updated with actual plug depths if MMS departure is not approved.

Rev. H.

The justified motive of profits versus reliable safety standards are sometimes conflicting and a primary goal of regulations should be to enforce rigor to safety, reliability and standards. While it is commendable that operators address reliability and safety, the industry must realize "trust" is not the issue: cooperation with regulators and industry transparency to ensure a safe environment is.

The phrase "trust us" will not work and our multiple appearances in front of congressional and regulatory bodies have done little to improve our situation. All companies, not just BP, are no longer trusted.

The industry cannot expect to continue to make risk based decisions in DW involving well control and process safety by using traditional risk analysis and NPV or cost drivers. It should have never been that way to begin with and that is where company leadership must step up and demonstrate a new approach – in that regard, the industry has "blown it."

Another issue which significantly impacts reliability is the natural conflicts of cost cutting and scheduling. Complex DW drilling operations must not be schedule driven.[6] An excerpt from this reference:

> *From an organizational perspective, drilling management equals risk management. As Cunha has observed:*[7]
>
> *"It is clear to me that drilling management is related closely to risk management"… and… "The correct assessment of all risks involved in drilling operations will provide better planning and will consequentially improve operational results". Furthermore, "A proficient drilling–management process is now more important than ever. This process must permeate all phases of a project, from early planning to final execution. Risk assessment of all operations must become a routine"...*
>
> *Indeed, risk assessment of all operations must become routine; however, it must also be performed in a mindful-manner – NOT as a matter of routine or with a "compliance-mentality." Drilling performance and safety is a multidisciplinary responsibility. Managing risks begins with well planning and clearly stated objectives agreed to by all stakeholders and by setting forth clear lines of responsibility and accountability in the decision-making process.*[8]

[6] Pritchard, op. cit.

[7] J.C. Cunha, "Drilling Management," Society of Petroleum Engineers, JPT, September 2010, 72.

[8] David M. Pritchard, et al., "Drilling Hazard Management: Excellent performance begins with planning," World Oil, August 2010.

…. It is important to fully realize how well-drilling objectives and their associated uncertainties are linked to safe drilling…. How the ***Rig Schedule*** *plays into routinely ignoring warning signs and how risk-taking behavior can insidiously infect a risk-adverse goal. The symptoms of this infection of an otherwise healthy safety management system can lead to operator manipulation of both company design practices and also regulatory requirements and complacency. Schedule driven decisions create a dynamic characterized by a tendency to overlook or possibly ignore essential design requirements to ensure a safe drilling margin and properly manage* ***uncertainties and ancillary risks.*** *Like a virulent virus, as the contagion spreads, it can and has escalated into an unhealthy co-dependent relationship between operators and regulators, contaminating the intended system of checks and balances in favor of doing it cheaper and faster.*

Catastrophes are caused by forces that penetrate or negate protective barriers. Once that occurs it is almost always too late.

As presented by Lacy[9]:

…. "As I mentioned earlier maintaining well control and avoiding major incidents is essentially a process safety framework. It is my experience that the E&P segment has a lot to learn from our counterparts in the chemical and refining side of the business. It is also my opinion based on experience that while our drilling contractors have made good progress as it relates to personal safety they are still well behind the Operators in that area and therefore even further behind as it relates to understanding the concepts of process safety. DW operations demand a higher standard than the norm.

"….The graphic shown is a model (Figure 3.2 – Penetration of Protective Barriers Regarding Safety and Reliability) I have used to explain to senior management the principles of well control and how it relates to process and personal safety. To keep people safe and free from major incidents we must maintain the barriers installed to safeguard against unintended releases of pressure, hydrocarbons, noxious gases, or stored energy. It is these forces that when released inadvertently or allowed to penetrate a protective barrier that result in fatalities, fires, and explosions, It needs to be pointed out that these barriers are not only mechanical such as steel, cement, and drilling fluids but also barriers that are human in terms of proper design standards, verification, quality assurance, supervision, and audits. Once the first set of barriers are penetrated we only have the vigilance of the work crews on site which must rely on their competence and training to spot and address a non routine condition, alarm, or warning sign. Finally our last failsafe is our well control equipment and fire and gas suppression systems.

The "elephant in the room" is all the mixed or unintended messages we send the crews when we are behind schedule, over cost, or behind on production. IF we don't clearly keep personal and process safety as an un yielding value in our words and more importantly visible behaviors and decisions we ultimately will not withstand the risk or test of time and we will certainly suffer a fatality or major incident. Senior non technical management cannot allow these barriers to be breached and I offer they hold the ultimate accountability if they are breached…."

[9] Kevin D. Lacy, "Restoring Integrity to the GOM Deepwater," SPE Deepwater Drilling and Completions Conference, Galveston, Texas, October 5-6, 2010.

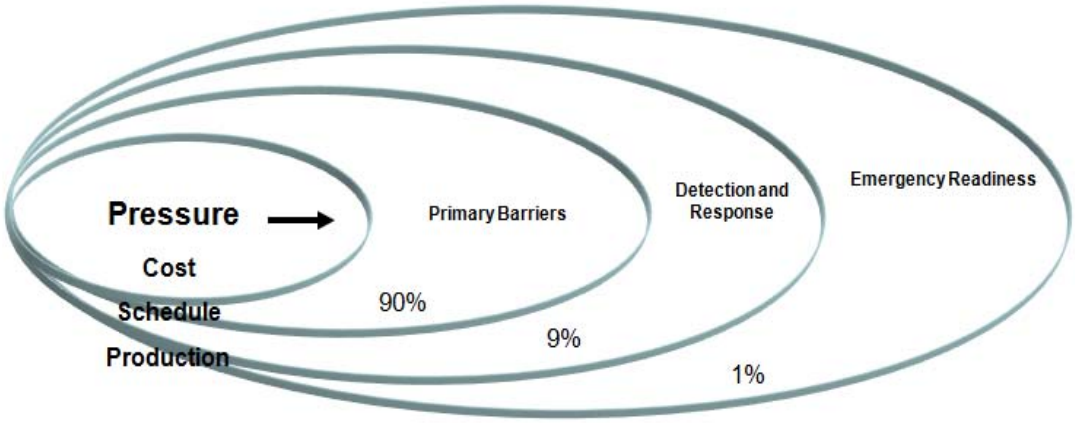


Figure 3.2 – Penetration of Protective Barriers Regarding Safety and Reliability.[10]

4.0 A Starting Place – The Metrics of Deepwater Drilling in the Gulf of Mexico

To establish a basis for targeting wells which have been problematic in Gulf Of Mexico Deepwater drilling, it is first necessary to understand whether or not there have been categories of wells or operations which have been problematic, and if so, what are they and to what extent. This is also important to understand and develop a robust risk profile for objective analysis.

The James K. Dodson Company has been the leading provider of metrics databases for GOM operations. This data base is populated by most operators in GOM operations. These metrics are categorized according to what Dodson has developed as the Mechanical Risk Index (MRI).[11] Deepwater wells are bracketed according to depth of water, total well depth, numbers of casing strings, and salt penetration. The following table and figures summarize each of these categories.

A review of the drilling performance of exploration and appraisal wells drilled in the GOM since 1993 indicates that there has not been sustained improvement in drilling performance for deepwater complex wells. Many operators have focused upon operational efficiency for improvement but, as evidenced, the expected improvement has not occurred. This has been noted in the lack of improvement in the well drill times as well as failing to achieve well objectives (Section 6.0), specifically in the highly complex wells.

Figure 4.1, Figure 4.2, Figure 4.3, Figure 4.4, and Figure 4.5 (Dodson MRI 1, 2, 3, 4, 5) illustrate clearly that as the complexity of the deepwater wells increase, learning is not occurring or at the minimum not sustained.

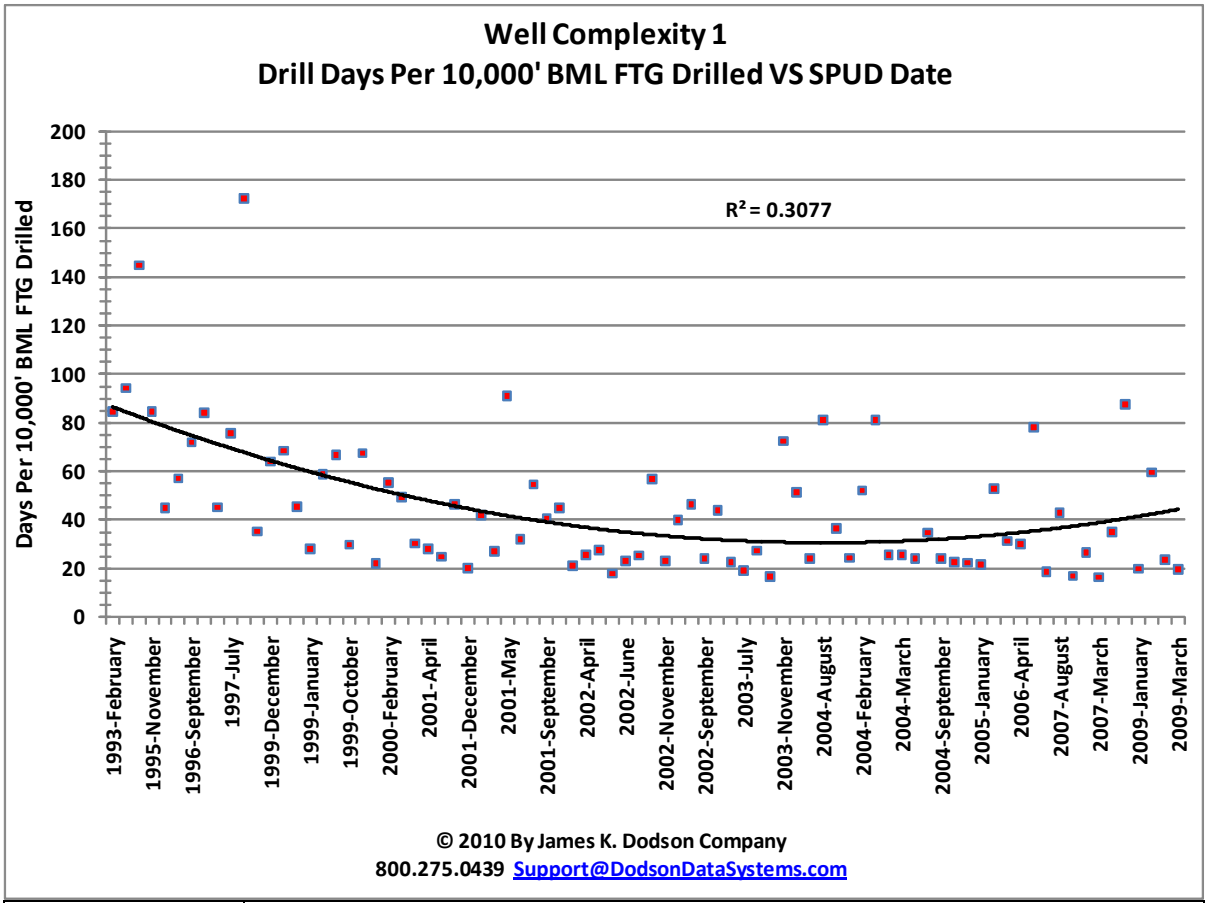
So, what is the problem? We often hear that "the industry has drilled 50,000 wells in the Gulf of Mexico", implying that no real problem exists. The metrics do not support that statement and demonstrate that only Forty-three (43) MRI 3, 4, and 5 wells have been drilled through year-end

[10] Kevin D. Lacy, "Restoring Integrity to the GOM Deepwater," SPE Deepwater Drilling and Completions Conference, Galveston, Texas, October 5-6, 2010, 7.
[11] The Mechanical Risk Index is an algorithm developed and owned by the James K. Dodson Company.

2009. These are the industries' numbers. So what is the real risk of occurrence of catastrophic failure relative to the BP Macondo based on Figure 2.1, Figure 3.1, Figure 3.2, Figure 4.1, and Figure 4.2? Is it 1/50,000 or is it ***now*** 1/43? This reality poses a totally different perspective on the issue of risk management. The following figures demonstrate levels of learning across wells of higher complexity in the GOM.

Table 4.1 – Key Well Criteria for Dodson Rankings.

	Key Well Factors - Median			
Dodson MRI Complexity Level	**Water Depth (WD) ft**	**Well Depth ft KB**	**Number of Casing Strings**	**Percent of Population penetrating salt.**
1	3,200	19,000	5	78
2	4,300	23,000	5	72
3	4,400	28,000	5.5	81
4	6,000	29,500	6	85
5	6,700	30,000	7.5	100

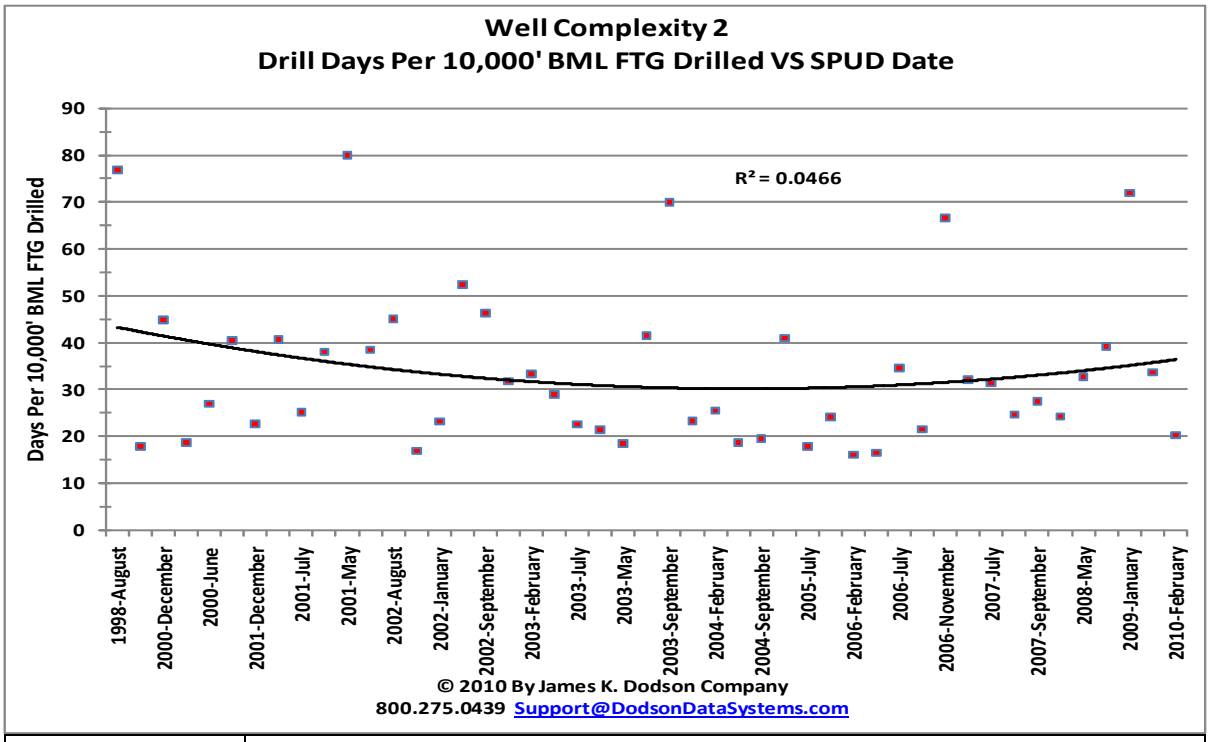


Ref. Figure 4.1	Key Well Factors - Median			
MRI	**WD ft**	**Well Depth ft KB**	**Casing Strings**	**% thru salt**
1	3,200	19,000	5	78

Figure 4.1 – Dodson MRI 1.[12]

[12] https://www.dodsondatasystems.com/Default.aspx

Figure 4.1 is a graph of Dodson MRI 1, indicating a slight decrease of drilling performance across this category. Learning across the general population has not been sustained.

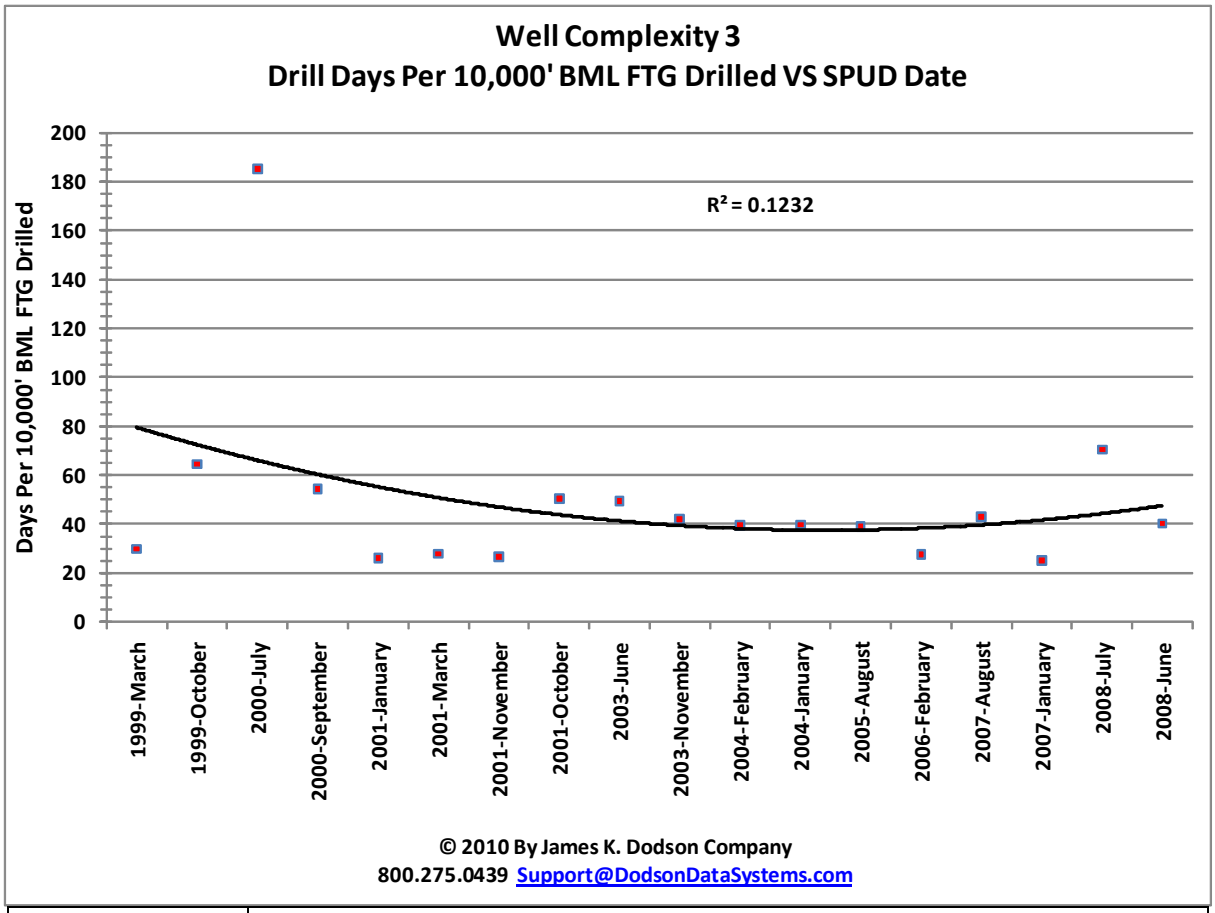


Ref. Figure 4.2	Key Well Factors - Median			
MRI	WD ft	Well Depth ft KB	Casing Strings	% thru salt
2	4,300	23,000	5	72

Figure 4.2 – Dodson MRI 2.[13]

Figure 4.2 indicates learning is scattered and at the minimum, and again, not sustained.

[13] https://www.dodsondatasystems.com/Default.aspx.

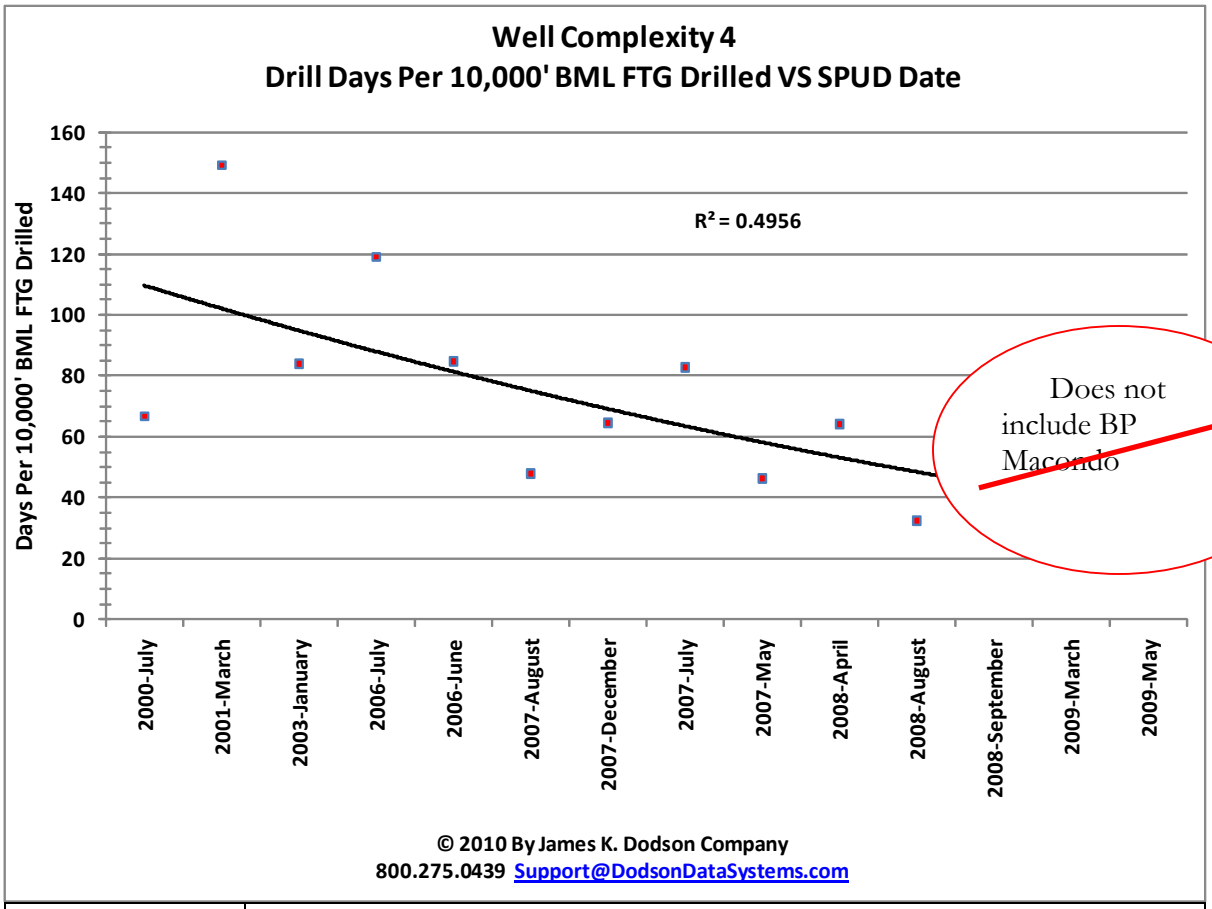


Ref. Figure 4.3	Key Well Factors - Median			
MRI	WD ft	Well Depth ft KB	Casing Strings	% thru salt
3	4,400	28,000	5.5	81

Figure 4.3 – Dodson MRI 3.[14]

Figure 4.3 indicates a lack of sustained learning.

[14] https://www.dodsondatasystems.com/Default.aspx.

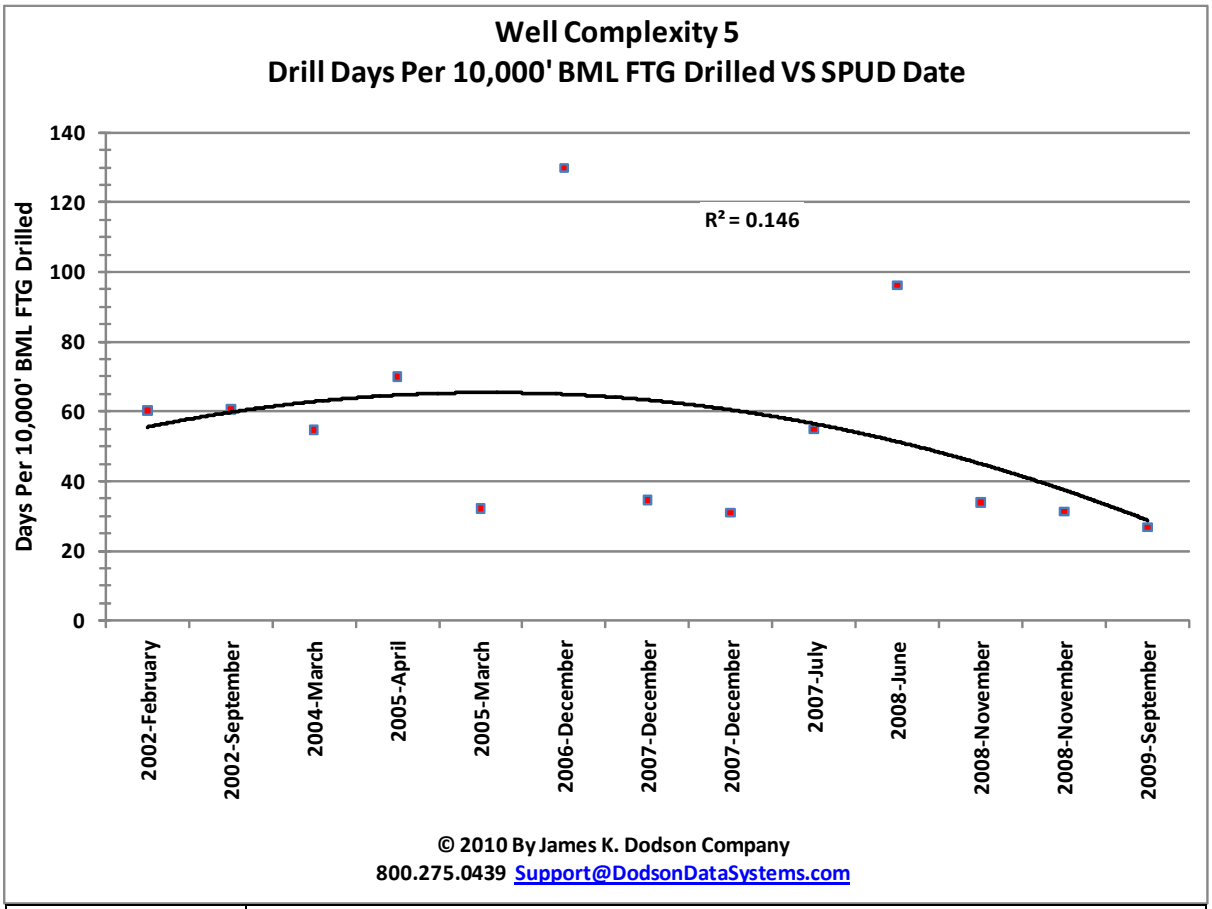


Ref. Figure 4.4	Key Well Factors - Median			
MRI	WD ft	Well Depth ft KB	Casing Strings	% thru salt
4	6,000	29,500	6	85

Figure 4.4 – Dodson MRI 4.[15]

Figure 4.4 indicates perhaps some learning, but trend reversal is beginning to show from 2008 to May 2009 (last available data). The BP Macondo well would represent between MRI levels of 3+ -4 and is not included in the above metrics.

[15] https://www.dodsondatasystems.com/Default.aspx.



Ref. Figure 4.5	Key Well Factors - Median			
MRI	WD ft	Well Depth ft KB	Casing Strings	% thru salt
5	6,700	30,000	7.5	100

Figure 4.5 – Dodson MRI 5.[16]

Figure 4.5 indicates that in the most severe well complexity group, level 5, it is clear that there is a decrease in drilling performance, albeit the well population is small. The BP Macondo well would represent at least an MRI level of 3+, and the industry trend is to drill more wells of this still higher MRI 5 complexity.

5.0 Well Instability Incident Trends

For the purposes of this paper, wellbore instability incidents are considered as stuck pipe, fluid losses, and general instability. Kicks and the totality of these trends are represented in the following figure which tracks the number of wellbore stability incidents per well drilled in each MRI. This is further explained in Section 7.0.

[16] https://www.dodsondatasystems.com/Default.aspx.

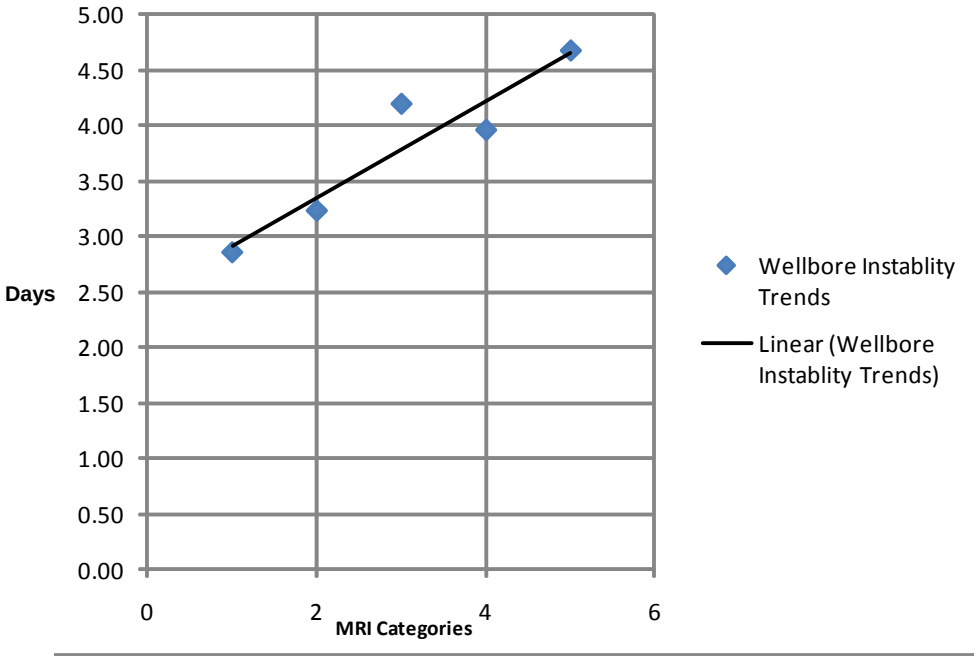


Figure 5.1 – Wellbore instability incident trends by MRI category.

Analysis of wellbore instability incident trends over the MRI populations is revealing in that the trend almost doubles from MRI 1 to MRI 5. At the minimum, these are clear indicators and warning signs of problematic wells.

6.0 Well Objectives

The drilling metrics represents only part of the problem since failure to meet well objectives is more common than it should be, and it is one of the main issues for the operator asset teams, in addition to the high cost of their wells. Failure to meet well objectives is not counted in the metrics – this is simply attributed or added to exploratory finding costs to the assets. Thus, the "metrics" are rosy and optimistic at best.

In the case of exploration wells, attaining well objectives may be more critical to the operator at that juncture than excellence in drilling performance. That is, it is more important in these wells to define the geo-scientific aspects of the well; however, this is not routinely happening in the more complex wells. Achieving objectives and excellence in drilling performance are not, and should not be mutually exclusive. The history of attaining deepwater well objectives has not been very good amongst the GOM operators. Table 6.1 is a summary of the experience of an anonymous GOM operator, which may apply to most GOM operators.

Table 6.1 – Typical well objectives achievement.

Well		High		Medium		Total (High + Medium)	% Completed
	Type	No.	Number Completed	No.	Number Completed		
GOM DW #1	Expl	Same as GOM DW#3				4	0
GOM DW #2	Expl	Same as GOM DW#3				4	0
GOM DW #3	Expl	3	1	1	0	4	25
GOM DW #4	Appr	7	5	6	6	13	85
GOM DW #6	Appr	4	2	7	3	11	45
GOM DW #7	Expl	4	2	5	4	9	67
GOM DW #8	Expl	3	3	2	2	5	100
Updated to January 26, 2009				Weighted Average Completed			56

This data indicates that this operator accomplished only 56 % of their high and medium rated exploration well objectives. Is it acceptable to accomplish only 43 % of well objectives in an exploration program? What is the real cost of failing to achieve objectives? Are we going to continue to accept 43 % of our objectives relegated to "train wrecks", "junked" or unusable wells?

7.0 Analyzing The Risk Of Deepwater Drilling – The Metrics Of Wellbore Instability

To further analyze the metrics of wellbore instability related events, **Error! Reference source not found.** summarizes time spent on Deepwater wells in less than 600 ft of water, the wells in non-subsalt wells in water depths greater than 3000 ft and subsalt wells greater than 3000 ft water depth. The primary bulk of MRI 3-5 wells are constituted of 65 subsalt wells in water depth greater than 3000 ft.

Table 7.1 – Days of wellbore instability as a % of total time (exclusive of weather).

Events related to Wellbore Instability	General Populations: 263 wellbores< 600 ft of water	65 subsalt wells: WD > 3000 ft	99 non subsalt wells WD > 3000 ft
Stuck pipe	2.20 %	2.90 %	0.70 %
Wellbore stability	0.70 %	2.90 %	0.90 %
Loss circulation	2.30 %	2.40 %	2.00 %
Kick	1.20 %	1.90 %	0.80 %
Total (%)	6.40 %	10.10 %	4.40 %
Total Wellbore Instability (days)	2.24 days	9.797 days	2.376 days
Total NPT Days	**4**	**29**	**9**
Instability % of NPT Days	**56.00 %**	**33.78 %**	**26.40 %**
Average Days to Drill	**35**	**97**	**54**
Kick Days	**0.42**	**1.843**	**0.432**

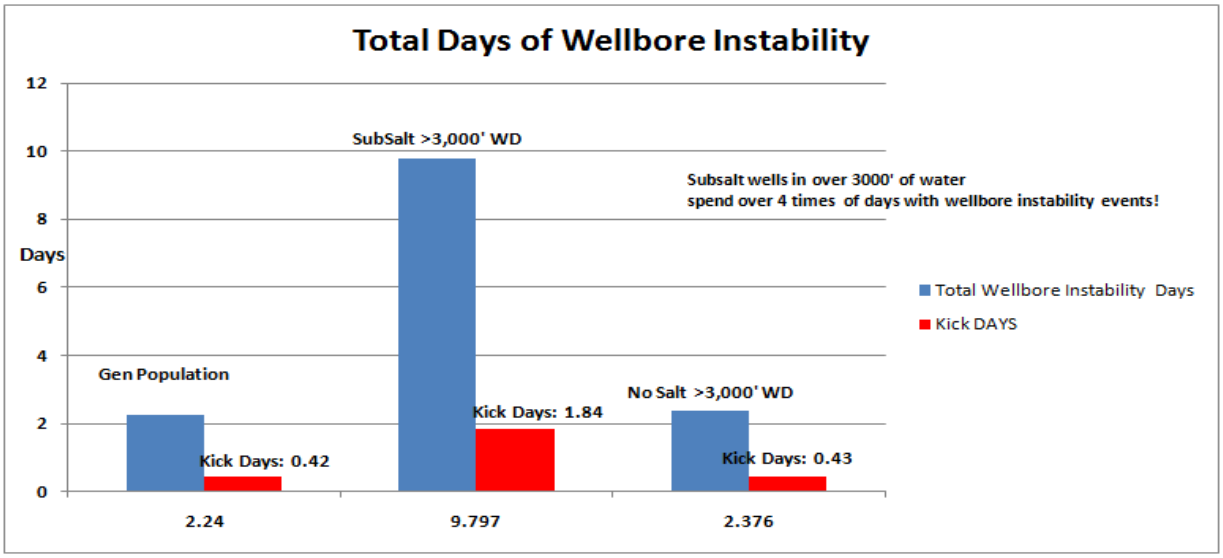


Figure 7.1 – Graphic of total days of wellbore instability.

Over four times as much time is spent on the more complex wells combating wellbore instability events. Even more revealing is that over 4 times as much time is also spent on the BOP's combating kicks.

Referencing the previous Figure 5.1, a look at the incidents indicates that there was an average of 2.85 days spent on wellbore instability for the average MRI 1 well, versus 4.67 days for MRI 5. The trend is approximately equal at MRI's 1 and 2 and jumps to over 4.1 for MRI 3.

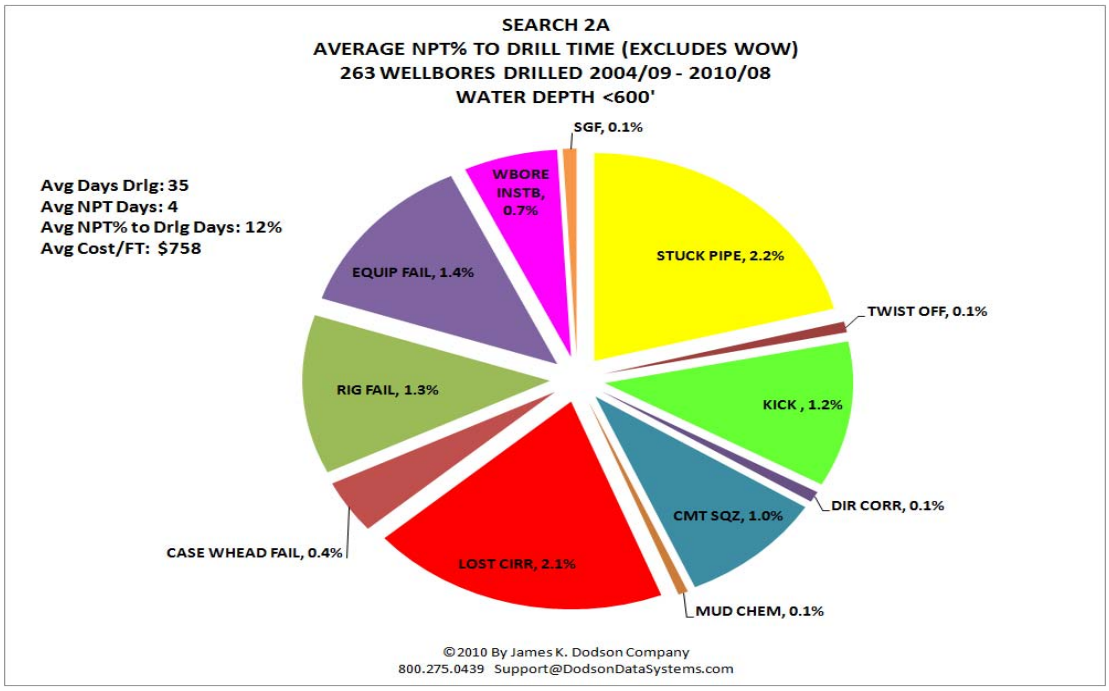


Figure 7.2 – NPT for 263 wells drilled in less than 600 ft of water.[17]

[17] James K. Dodson Company

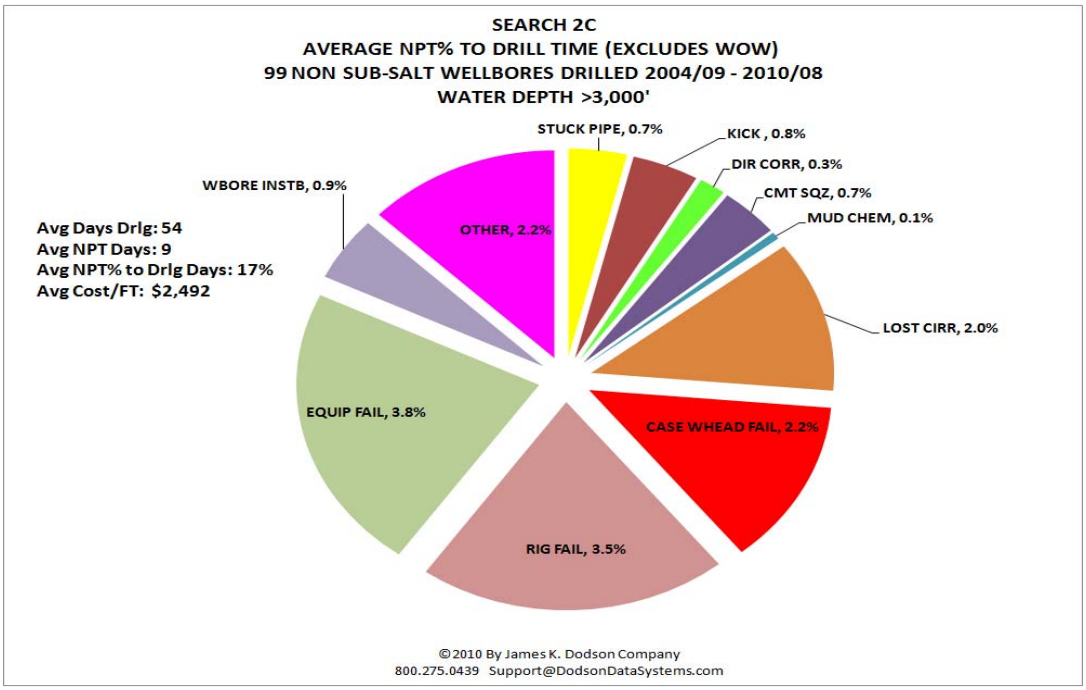


Figure 7.3 – NPT for 99 non subsalt wells drilled in greater than 3000 ft of water.[18]

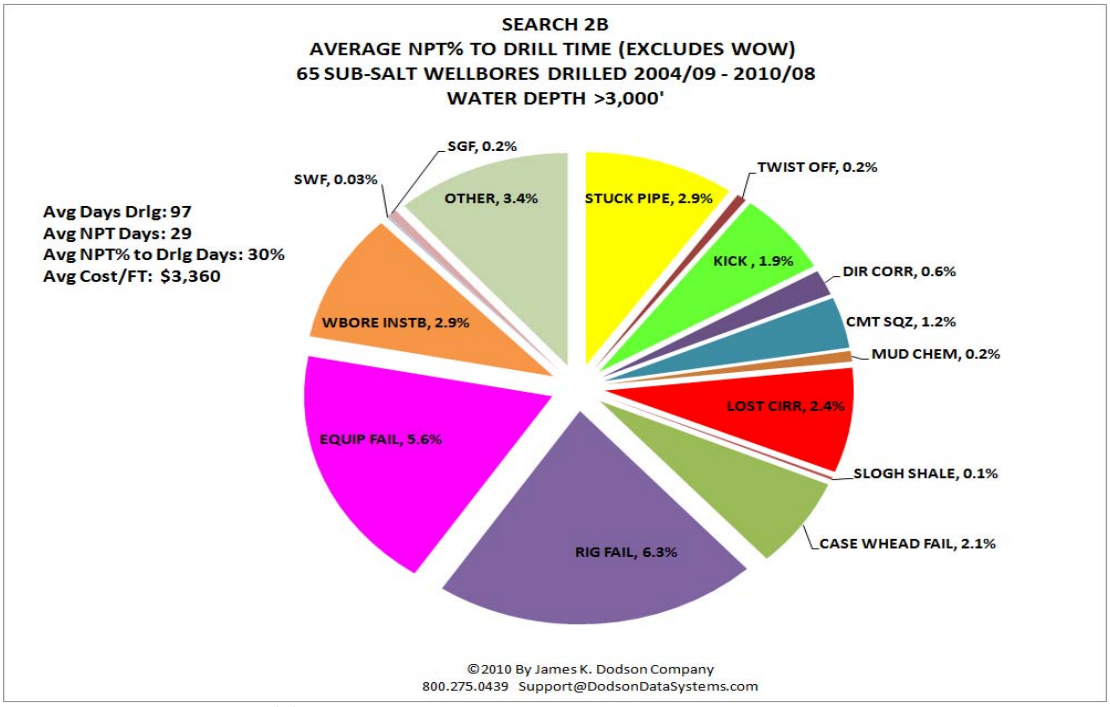


Figure 7.4 – NPT for 65 subsalt wells drilled in greater than 3000 ft of water.[19]

Any event of wellbore instability has the potential of becoming a well control event.

[18] Dodson, op. cit.
[19] Dodson, op. cit.

8.0 Conclusion

Restoring integrity to the DW environment requires a higher standard:

- The Operator is the Operator…….
- Transparent industry standards need to be established with better verification.
- The drilling contractor must be accountable for their people, equipment, and hold each Operator to an industry standard.
- US Regulators must be assisted to be more effective.
- Dollar consequences for failure are inadequate.

It is imperative that the industry adopt standards which ensure process safety around design and execution and there are some very basic and cumulative actions which must be considered for absolute well control:

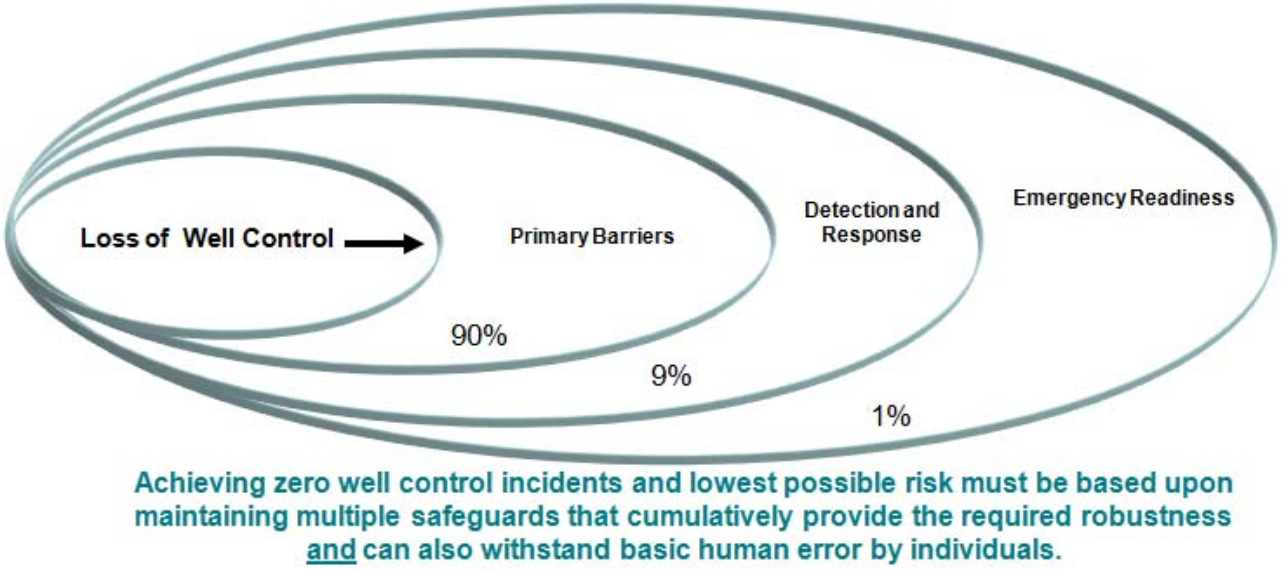


Figure 7.5 – The cumulative basics for incident free operations.[20]

As further pointed out by Lacy:

….. *"To summarize the industry has seriously failed to adequately implement appropriate risk assessments and the standards required to mitigate the risks in DW. More importantly our industry has had a significant peer fail to adequately protect people and the environment in spite of high quality process and people and deep experience. It is a failure that was imminently preventable and therefore wholly unacceptable.*

While I do expect BP to be the company that takes responsibility for the incident I fully expect the entire industry to own the learnings and the responsibility for implementing a significantly better system and way of working in highly complex environments.

[20] Lacy, op. cit., 9.

While the details of the incident are unique the failures are not – we know them well. We must accept responsibility for those failures. The only acceptable outcome is a new system that precludes any similar incident from happening in the future. We owe the public and the eleven families that have suffered a loss a commitment to not allow it to happen again."

The BP tragedy in the Gulf of Mexico (GOM) has clearly revealed two major categories of the consequences of risk—the incident itself and the resultant environmental disaster. These risk consequences are quite obvious. Risk in any endeavor cannot be eliminated entirely, but it can be successfully managed if it is recognized and the consequences are fully understood.

In order to have a meaningful outcome for future deepwater drilling, the Hopkins mindsets must be addressed, and one must first understand that there is a problem, and then focus on solving the problem.

Avoiding a repeat of the current situation and changing the climate of denial can be achieved with a dose of common sense. Solutions must consider and actively apply the following:

- Look at the facts of the metrics in context of well complexity.
- Work together and collaborate as an industry.
- Recognize where the problems really are and address them from a risk management perspective.
- Focus on solving those problems and work with regulators to focus on the solutions.

The current design and exertion model must be challenged. Sound and unbiased engineering design is the fundamental precursor to process safety, sustained success and full life cycle reliability. If we solve the problem wells, then by definition of risk management, the rest of the well population is mitigated.

Appendix E

Environmental Issues Associated with the Macondo Well Blowout

T. Azwell and A. Laleian

1.0 Introduction

Based on the estimated 4.9 million barrels of oil discharged during the 89-day ordeal, the Deepwater Horizon Oil Spill was one of the worst environmental disasters in US history.1 Although, the effective environmental consequences of a catastrophic oil spill are difficult to quantify, it is possible to qualify the impact. Such a perspective on the initial environmental impact of the spill is necessary to the formation of future policy and decision-making related to risk management, fine assessment, and appropriate oil spill response. Therefore, it is essential to identify all the variables that contribute to the development of a comprehensive environmental impact assessment.

Three key components of the Gulf oil spill's cumulative environmental impact, which have not yet been considered, are:

a. The addition of natural gas to total petroleum discharge. Including methane and other hydrocarbon gases, the total petroleum discharge amounted to more than 6.9 million barrel of oil equivalents, 2 million of which were natural gas.
b. The inclusion of oily and non-oily waste materials resulting from cleanup efforts disposed of in local landfills. These waste materials include 11 million feet of absorbent boom, oil, sand and sediment from shorelines, marine animal carcasses, personnel materials such as Tyvek suits and gloves, vegetation, and other debris.
c. The release of chemical dispersants into the oceans, and the air pollution resulting from in-situ burning of oil.

2.0 Emulsification of Crude Oil

When oil enters the environment from spills, ruptures, or blowouts it undergoes a continuous series of compositional changes that are the result of a process known as weathering. During the weathering process much of the oil, especially heavier oil, will typically mix with water and emulsify to form a viscous mixture fairly resistant to rapid weathering changes. Thus, it is slower to degrade and more persistent in the environment than non-emulsified oil. Emulsified oil is generally less environmentally dangerous than fresh oil in a slick because it is a mostly sticky material that causes damage through covering or smothering as opposed to toxic interactions, unless ingested.

[1] "Deepwater Horizon MC252 Gulf Oil Budget", *NOAA*, 4 August 2010, http://www.noaanews.noaa.gov/stories2010/PDFs/DeepwaterHorizonOilBudget20100801.pdf.

Emulsified oil cannot be effectively recovered by skimming technologies or absorbent booms, chemically dispersed, or burned. Thus, recovery efforts must take place prior to significant emulsion of oil.

The oil from the Deepwater Horizon spill contained high quantities of natural gas which caused oil dispersion in the deep Gulf waters. The oil exiting the wellhead was also mixed with chemical dispersant causing further dispersion at depth. The net effect of both natural and chemical dispersion is that much of the oil was broken into very tiny droplets with diameters less than 100 microns. Droplets of this size or smaller face significant flow resistance from the water column in their effort to rise to the surface, and are trapped in the deep Gulf environment until degraded by bacteria. This dispersed oil is diluted as it moves away from the wellhead. Some components dissolve into the water column and are available for fairly rapid biodegradation, while the residual oil is more slowly broken down by microorganisms. Because the concentration of the dispersed oil is well below the concentration of oxygen in the deep Gulf, no significant oxygen depletion has been observed from the degradation of the oil in the deep Gulf waters.

3.0 Dispersion of Oil

The oil from the Deepwater Horizon spill contained high quantities of natural gas that caused oil dispersion in the deep Gulf waters. In addition, a chemical dispersant was mixed with the oil exiting the wellhead, which caused further dispersion at depth. The net effect of both the natural and chemical dispersion is that much of the oil was broken into tiny droplets, whose diameters are less than 100 microns. Droplets of this size or smaller face significant flow resistance from the water column, in their effort to rise to the surface. They become trapped in the deep Gulf environment until degraded by natural bacteria. The dispersed oil becomes diluted as it moves away from the wellhead, which allows some of its components to dissolve into the water column and become available for biodegradation. The residual oil degrades at a much slower rate. Because the concentration of the dispersed oil is well below the concentration of oxygen in the deep Gulf, no significant oxygen depletion has been observed from the degradation of the oil in the deep Gulf waters.

4.0 Chemical Dispersants

Chemical dispersants are petroleum solvents that move oil from the water surface to the water column by breaking an oil slick into small droplets. Their use does not reduce the total volume of oil in the environment, but rather changes its location and physical properties. The use of chemical dispersants has been described as a "risk-based paradigm"[2] in which tradeoffs between environmental benefits and harms must be weighed prior to their application. The benefits of chemical dispersant use include more rapid biodegradation of oil and protection of shorelines. The former removes oil from the environment while the latter prevents it from reaching sensitive ecosystems. The harms of their use include greater exposure of oil to subsurface marine life, no possibility of oil recovery in the dispersed form, and when applied beneath the water surface, larger dispersed oil plumes of uncertain fate and environmental impacts.

[2] Coastal Response Research Center. "Research & Development Needs for Making Decisions Regarding Dispersing Oil." Durham, New Hampshire: University of New Hampshire, 2005.

Effective oil cleanup implements those technologies that are effective at both removing oil and reducing the spill's environmental impact. Whether or not chemical dispersants satisfy these criteria is yet to be determined. Because tradeoffs exist between environmental costs and benefits, the balance between the two needs to be assessed locally for each situation before decisions are made. For example, an instance in which chemical dispersant use would be favorable is one in which surface oil presents to a shoreline ecosystem an imminent threat that is greater than the adverse impact of chemical dispersant application in the open ocean. In this situation, chemical dispersant use may be necessary and the most effective cleanup technology.

The use of chemical dispersants as a first response, as supported by the Joint Industry Oil Spill Preparedness and Response Task Force[2], assumes net environmental benefit from the outset. However, available data suggests that such an assumption may not be justified. Oil recovery is preferable to chemical dispersion as a first response, because it removes oil from the environment and minimizes the potential for increased ecological and human toxicity.

5.0 In-Situ Burning of Surface Oil

The combustion of crude oil forms a mixture of compounds in solid, liquid, and gaseous phases. The minor components released, including particulate matter (PM), carbon monoxide (CO), sulfur dioxide (SO_2), and nitrogen oxides (NO_x) are capable of the most direct impact on human health. Volatile organic compounds (VOCs), which evaporate without ignition soon after reaching the surface, are also harmful if inhaled. The U.S. Environmental Protection Agency (EPA) considers benzene, toluene, ethylbenzene, and xylene as the "key toxic VOCs"[3].

Tracking atmospheric changes due to in-situ burning is necessary and points to some of the hazards of in-situ burning. The dispersal of an airborne plume is controlled by local environmental factors, primarily wind speed and direction. Barnea (2005) documented that in previous oil spills where air quality was monitored following burning, concentrations of toxic gases beyond two miles from the burn fell to approximately background levels. If such dispersal is a general trend and burning takes place more than two miles offshore, harm to the general public, with respect to the aforementioned gases, will not be increased greatly by in-situ burning. Response workers near the burn, however, will risk greater exposure to toxic gases, necessitating the use of onboard monitoring technologies. Furthermore, the burning of oil on the water surface represents a lost opportunity in oil recovery and subsequent energy production.

[3] Joint Industry Oil Spill Preparedness and Response Task Force. "Draft Industry Recommendations to Improve Oil Spill Preparedness and Response." 2010.

6.0 Occupational Risk

Studies of tanker oil spill responses have reported adverse health effects in response workers.[4,5,6,7] These studies may underestimate the health effects on the Deepwater Horizon response personnel because the spill's magnitude and duration are unprecedented. Fresh oil is generally less toxic than weathered crude oil because the concentration of volatile organic compounds (VOCs) decreases with weathering. Still, weathered oil contains harmful compounds that can cause irritant reactions, and there is a potential risk for oil to be aerosolized into respirable airborne droplets or volatilized by activities such as pressure washing. Even though detection of hydrocarbon odors is common in areas contaminated by oil, odor is not a reliable indication of a health hazard. Some individuals, though, are bothered by odors and can develop symptoms requiring medical evaluation. Overall, there is an incomplete understanding of the cumulative human health toxicity associated with the particular characteristics of this spill, including a large volume of continuously-flowing oil, extensive dispersant use, and in-situ burning.

According to the Louisiana Department of Health and Hospitals, from April 25 to September 18, 2010, there were 411 reports of health complaints believed to be related to exposure to pollutants from the oil spill.[8] 325 of these reports came from response personnel and 86 from the general population. The most frequently reported symptoms were headache, dizziness, nausea, vomiting, weakness/fatigue and upper respiratory irritation. Due to a lack of chemical-specific air monitoring, especially for cleanup workers in vessels, direct correlations between chemical exposure and health complaints cannot be determined. For example, the USEPA's air monitoring at several fixed sites used a technology known as photoionization detection (PID) that can only measure total VOCs, not specific compounds such as benzene, toluene, ethylbenzene, and xylene. In fact, there are no USEPA records of samples obtained from vessels in which cleanup workers were present.

7.0 Waste Management

Senate Bill (SB) 583 entails the creation of a comprehensive debris management plan with the goal to "reuse and recycle material, including the removal of aluminum from debris, in an environmentally beneficial manner and to divert debris from disposal in landfills to the maximum extent practical and efficient which is protective of human health and the environment (SB 583)."[9] SB 583 prioritizes waste management practices for debris in this order: "recycling and composting;

[4] U.S. Environmental Protection Agency and Centers for Disease Control and Prevention. "Odors from the BP Spill." Washington D.C., 2010.

[5] Barnea, Nir. "Health and Safety Aspects of in-Situ Burning of Oil." edited by National Oceanic and Atmospheric Administration. Seattle, WA, USA, 2005..

[6] Zock JP, Rodriguez-Trigo G, Pozo-Rodriguez F, Barbera JA, Bouso L, Torralba Y, Anto JM, G FP, Fuster C, and Verea H. Prolonged Respiratory Symptoms in Clean-Up Workers of the Prestige Oil Spill Am J Respir Crit Care Med, 176:610-616, 2007.

[7] Aguilera F, Mendez J, Pasaro E, and Laffon B. Review on the Effects of Exposure to Spilled Oils on Human Health. J. Appl. Toxicol. 30:291-301, 2010.

[8] Perez-Cadahia B, Mendez J, Pasaro E, Lafuente A., Cabaleiro T, Laffon B. Biomonitoring of human exposure to Prestige Oil: Effects on DNA and endocrine parameters. Environmental Health Insights 2:83-92, 2008.

[9] "Weekly Waste Tracking Cumulative Report," *BP International, Ltd.*, 17 Oct 2010, http://www.bp.com/genericarticle.do?categoryId=9034343&contentId=7063466

weight reduction, volume reduction; incineration or co-generation and land disposal" to the extent they are "appropriate, practical, efficient, timely, and have available funding (SB 583)."

The Deepwater Horizon spill and its subsequent clean-up methods generated 80275.5 tons of solid waste and 956,350 BBLs of liquid waste as of October 17, 2010[10]. This waste can be separated into categories based on its material make-up. These categories include solid waste, recovered oil, oily water and liquid waste, and animal carcasses. Solid waste includes oil contaminated material such as sorbents, debris and personal protective equipment, as well as non-contaminated solids, such as those materials required by the support operations. In the period ending October 26, 2010, 71,844.1 tons of oily solids and 9,512.1 tons of solid waste were collected and taken to municipal solid waste landfills[10].

Detailed waste management plans were created to ensure the disaster waste was disposed of properly. Waste plans were approved by the EPA, the Coast Guard, Unified Area Command and the Gulf States directly affected by the spill. Louisiana in particular has new regulations promoting waste diversion and the reduction of materials entering landfills, since the 15 million tons of disaster debris generated by Hurricane Katrina.

A significant portion of the generated waste was sorbents and booms. Despite the above-mentioned regulations, it is important to note that the waste created by these clean-up technologies did not have to amount to such a magnitude. There exist alternative technologies for clean-up operations that are more facilitative to recycling and composting. For example, natural fiber booms and loose absorbents can be used to absorb the oil and then be composted, resulting in degradation of the oil hydrocarbons and an end product that can be used or sold as a soil amendment. The State of Louisiana is the largest sugar cane producer in the United States, generating more than 3 million tons of natural fiber waste (known as bagasse) per year.[11] Preliminary research at UC Berkeley has demonstrated bagasse's high absorption rate and ability to degrade oil naturally. The use of bagasse to fill booms and as a loose absorbent, would not only decrease the tonnage of material entering landfills, it would help solve a waste problem for the sugarcane industry and would reinvest revenue spent on cleanup back into the local economy.

Loose sorbents, another environmentally beneficial clean-up technology, can be left in the environment and utilize hydrocarbon-degrading bacteria to eliminate the crude oil. This provides a cleanup solution that requires little manpower and can reduce ecosystem disturbances. Currently, National Contingency Plan (NCP) regulation dictates that all sorbents must be removed from oil spills and be disposed of properly. Organic loose sorbents, however, can degrade naturally with the oil and should be reconsidered for their sustainable and low-impact properties. Despite the fact that they are included in Subpart J on the NCP[12], natural sorbents were an unlikely choice during the response effort, due to their absence on the product schedule.

[10] Rodríguez-Trigo G, Zock JP, Isidro Montes I. Health effects of exposure to oil spills. Arch Bronconeumol. Nov;43(11):628-35, 2007.

[11] Waste, Oil Recovery, and Disposal Summaries," *BP International, Ltd.*, 26 Oct 2010, http://www.bp.com/genericarticle.do?categoryId=9034343&contentId=7063466

[12] "Recovered Oil/Waste Management Plan Houma Incident Command"

8.0 Fine Assessment in Oil Spill Legislation

There are a number of laws the Courts may utilize to assess fines against the party or parties responsible for the explosion of the Deepwater Horizon and subsequent oil spill. These laws will direct how the damage is analyzed and will steer our future environmental policies. The Oil Pollution Act (OPA) is likely to set the foundation for the litigation surrounding the Deepwater Horizon accident. The OPA was established in 1990 in response to the Exxon Valdez oil spill. It instituted fines for oil pollution and established cleanup response plans and funding mechanisms in the event of an oil spill disaster[13]. The Clean Water Act (CWA) is another likely source of law. The CWA was enacted in 1977 as an amendment to prior legislation. It established water quality standards, as well as an enforcement plan for maintaining these standards[15].

An important difference between these two acts is that the CWA allows a per-barrel fine for damages while the OPA imposes liability for environmental and economic damages established by expert study. Both the OPA and CWA establish caps on liability for damages. This cap, however, does not apply if the spill was a result of gross negligence.

A comprehensive environmental and economic impact assessment will be a fundamental ingredient in determining fines under any of the laws. Aside from oil spilled, there are two important considerations that should not be overlooked by the assessment:

1. The release of natural gas from the well. An estimated two million barrels of natural gas escaped and has had a significant impact on water quality in the Gulf. Under the CWA, natural gas can be included under the per-barrel fines for oil spilled. Under the OPA, the harmful impact of the natural gas should be a key component of the environmental damage analysis.
2. The use of dispersants and in-situ burning to combat the spill. The use of two million gallons of dispersants and burning of 10.3 million gallons of oil should be categorized as hazardous substances under the OPA. The impacts of subsea dispersant use is not yet clear, but it is clear that effects of dispersant use should be considered as part of the environmental impact assessment.

Fine assessment currently does not include the three critical components outlined above. In the future, the release of natural gas should be included, as it falls under the per-barrel fines of the CWA and the environmental damage analysis of the OPA. Similarly, the use of dispersants and in-situ burning may be categorized as hazardous substances under the OPA. Lastly, spill-related waste also should be considered to represent environmental damage under both the OPA and CWA.

[13] Gravois, Kenneth. Louisiana's Sugarcane Industry. Louisiana Agriculture, Fall 2001.

9.0 Conclusion

Current oil spill environmental impact assessment is incomplete. It does not include the discharge of natural gas, the disposal of waste materials related to the spill and its cleanup, and the environmental impacts of cleanup technologies, such as chemical dispersant application and in-situ burning. The release of natural gas contributes to the adverse environmental impacts of the spill, and therefore, it should be included in the total petroleum discharge used to determine the fines paid by responsible parties. The disposal of a significant volume of waste materials related to the spill impacts local landfills by introducing oily, hazardous waste. Current and future clean-up plans need to take this fact into consideration and utilize methods that minimize waste. The benefits of chemical dispersant application are coupled with costs. The net result of this cost-benefit scale still is unknown. In-situ burning moves oil pollution in the water to pollution in the atmosphere. Although safe to the general public, response personnel may face the risk of adverse health effects from in-situ burning. This should be taken into consideration when developing future response plans.

Appendix F

Risk Assessment & Management: Challenges Of The Macondo Well Blowout Disaster

Robert. G. Bea

1.0 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.

2.0 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.

3.0 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).

4.0 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 has 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.

5.0 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).

6.0 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 2000). This means additional efforts are needed to understand what causes these errors or malfunctions so 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 2005).

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.

7.0 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).

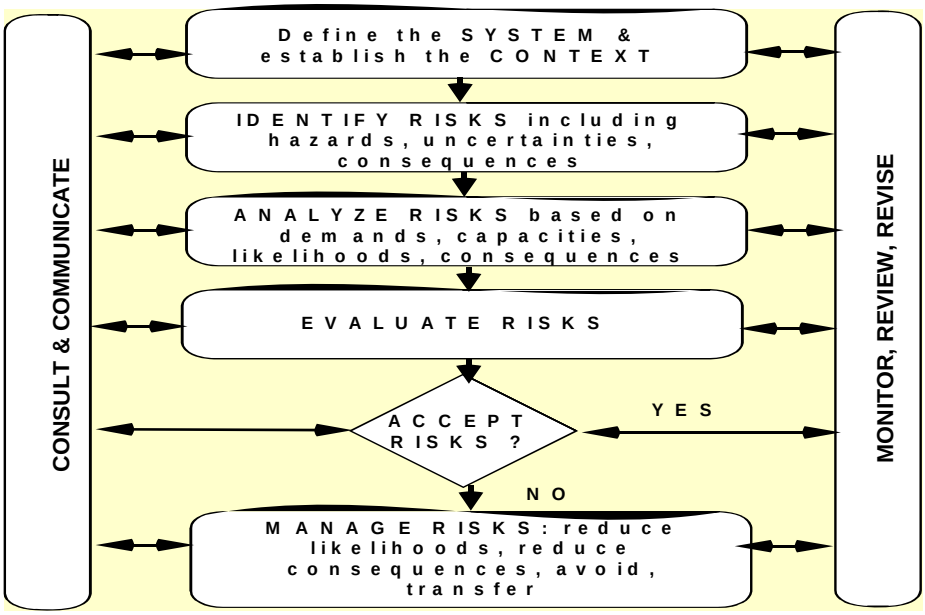


Figure 7.1 – RAM process

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 1988) 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.

8.0 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 2000). 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).

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 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 that is 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").

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 of 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 2000). 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.

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 (equipment, structure) related malfunctions 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 compounds 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 Cap Ex 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.

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.

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 (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.

9.0 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 malfunctions 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.

10.0 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 confirmational 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 2000, Hopkins 1999, 2000, 2010).

11.0 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 2001, Ehrenberg, Nadeau, Steen 2008, 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 3,000 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 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.

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 – 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, clean-up) 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.

12.0 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.

13.0 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 definition and characterizations 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 Association 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).

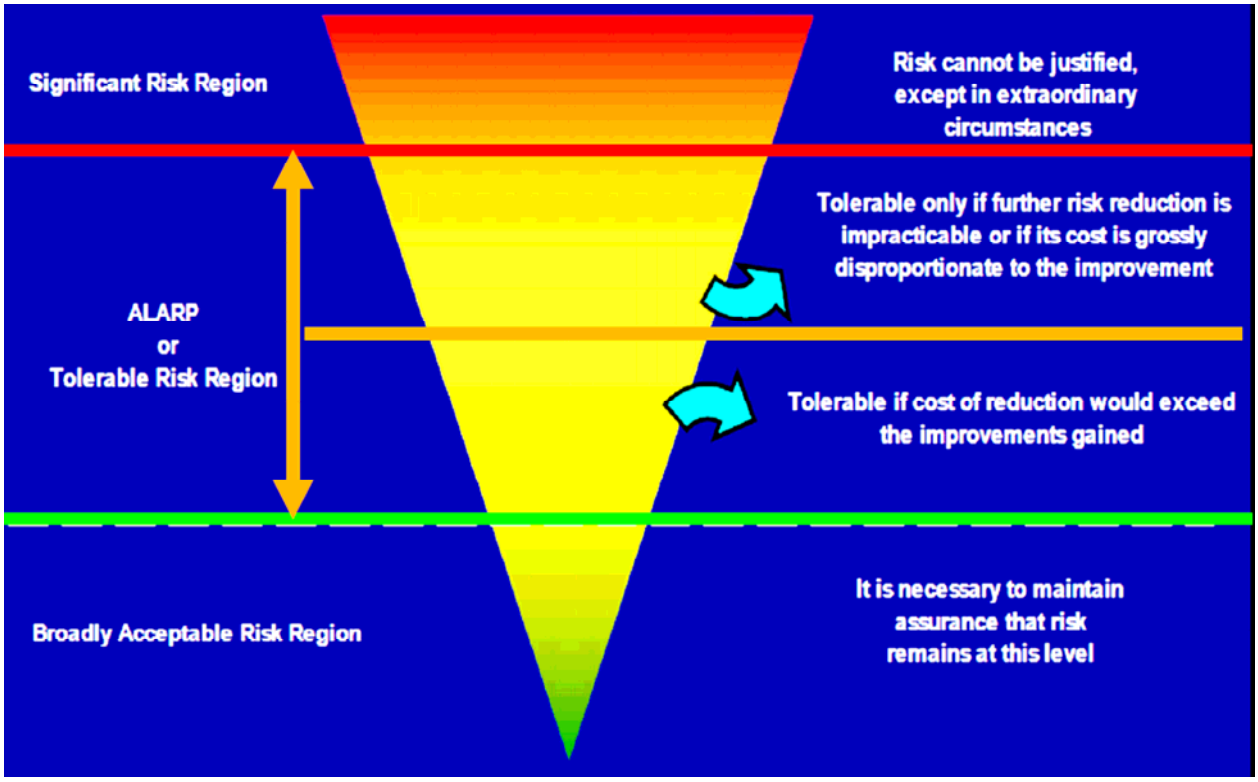


Figure 13.1 – As Low As Reasonably Practical risk regions (after Malloy and McDonald 2008).

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 cost of reduction would exceed the improvements gained.

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, environmental and property damage, 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). 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.

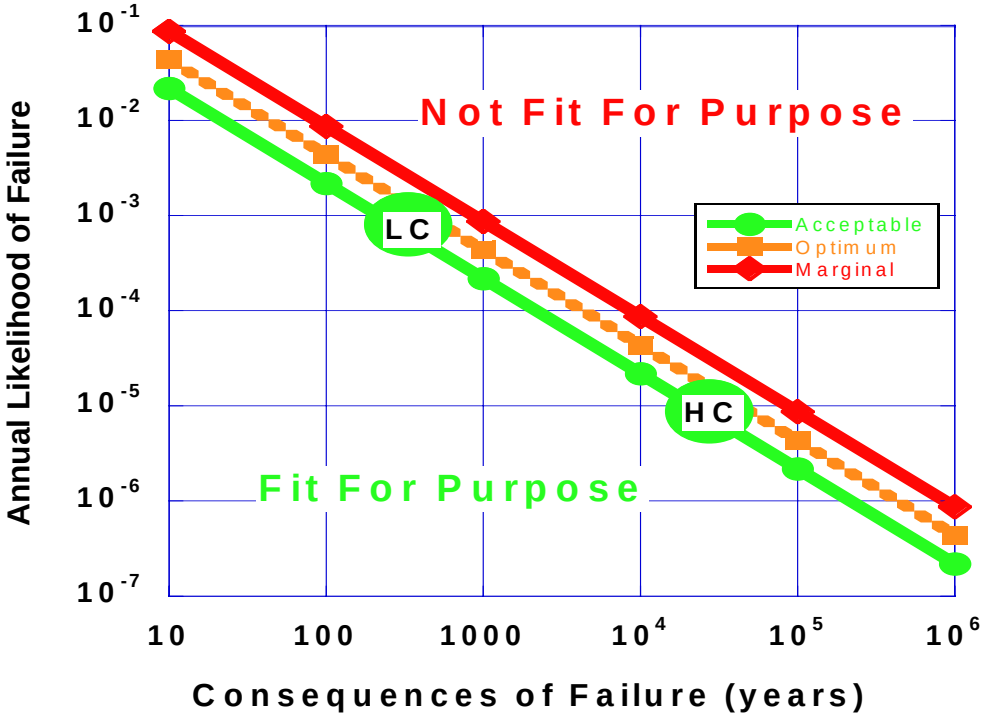


Figure 13.2 – Developing systems to achieve acceptable risks

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 Association 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.

14.0 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 Association 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.

15.0 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; Soares, 1998; Vinnem, 1998). 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, 1998; Bea, 2000a) 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) has 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, that 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, then 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).

16.0 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 developed 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., confirmational bias, organizational 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 (Faber, 1997; 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 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.

17.0 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,
- 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'.

18.0 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.

19.0 References & 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 & 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.

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 Techniques*, 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., *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.

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.

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.

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.

Appendix G

Deepwater Well Design, Competency – Management of Risks

Yngvar Duesund and Ove T Gudmestad

It is important that management understands the overall risks involved in drilling a deepwater well and that they understand what it takes to make a robust deepwater well design. Is this issue all a matter of competency?

The competency of a company's drilling team, whether the team has the right persons for the job or previous success has made them complacent "making short cuts", should be questioned in case of problems and equally so by those who verify the well design and approve the non-conformances.

More than twenty years of drilling experience doesn't necessarily mean that a person is competent to enter new territories in deepwater drilling. For example a pilot who has been flying a Boeing 737 has to take on extensive training before a sufficient level of competency is reached to fly a Boeing 777. Bearing in mind the statement of Capt Chesley Sullenberger (with 40 years of experience as pilot) who landed the US Airways flight 1549 on Hudson River on January 15, 2009:

"I can speak for the entire crew when I tell you we were simply doing the job we were trained to do."

Sullenberger had trained beyond standard requirements. We know that an expert makes most decisions intuitively, based upon previous experience and training. But how will a good decision be made when a new unexpected situation occurs that has not been experienced or trained for? Referring to the Berkeley Professors Hubert and Stuart Dreyfus' concept of "Beyond Expertise" [1]:

"A related alternative road to mastery presents itself to experts whose skill demands that they sometimes must respond to novel situations without time for deliberation. Such an expert, if motivated to excel, not only will assess the situation spontaneously and respond immediately, but will experience elation if the assessment and response is successful and dissatisfaction if it seems to him disappointing."

When an organization/team is very successful a kind of complacency will ride the organization/team and important issues may easily be overlooked, reference to BP's Macondo well and the Norwegian Contractor's Sleipner incident.[2] It is only a professional management team and very competent personnel who will continuously manage to deal with unexpected issues. We will in this paper discuss what characterizes a professional team and competent personnel. It must also be

[1] S-E. Dreyfus; Bulletin of Science, Technology & Society; February 2009: vol 29, 1: pp 38, S.E. Dreyfus and H.L. Dreyfus, "A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition," 1980. Unpublished report supported by the Air Force Office of Scientific research (AFSC), USAF, University of California at Berkeley. Cited in P. Benner, From Novice to Expert, (Menlo-Park, California: Addison-Wesley Publishing, 1984).

[2] W. K. Rettedal, O. T. Gudmestad, and T. Aarum, "Design of Concrete Platforms after Sleipner A-1 Sinking," in S.K. Chakrabarti, C. Agee, H. Maeda, A.N. Williams and D. Morrison, eds., Offshore Technology Proc. 12th Int. Conf. on Offshore Mechanics and Arctic Engineering (OMAE), **1**, ASME, New York, (1993), 309-319.

recognized that a professional team must be given the opportunity to act as such within the organization and the limits of its responsibility and authority. An organization where the top management only accepts reports of successes can never learn from failures or near misses.[3]

1.0 Introduction

The composition, competency and integration of a team have a significant effect on its success. When management assigns tasks to individuals they assume that the person has the competency and will have hands on the work to be carried out. In the oil and gas industry there are long traditions how a drilling team is composed and there isn't much difference from one oil company to another how the work is organized, however, risk assessment, planning, and contractual issues may vary considerably and so the performance.

In the Middle East a drilling team spent 56 days to drill and complete a well while another one spent 132 days drilling in the same geological formation, both team using the same drilling rig. Why did one team perform more than twice as good as the other? The major reason was that the successful team performed risk assessment and planning very seriously and hence, they could deal with all logistical challenges, interfaces, and change management. This team had the necessary competent personnel with excellent communication skills and knew the risks and challenges to overcome. Their work was considered at the time as best practice in that region. The result was outstanding and other companies wanted to copy the way they organized the work, but so far no other team have managed to be equally successful. The manner the teamwork was carried out and how communication and cooperation with contractors was dealt with made the big difference and those are factors that cannot be easy to paste and copy, i.e., the personal "touch" can never be copied. But careful planning and a humble approach to new challenge should be a trait for all teams to handle acceptable risk and be prepared for unexpected events.

When a drilling team is faced with a situation they didn't contemplate and there are none operating procedures for handling it, then full management attention should be required. If critical, the top management of the organization should be informed. The decision whether to stop a risky operation or not should be taken by the most competent personnel, i.e., a person or persons who have experienced and handled similar situations. Top management or the regulatory body will normally not have the competency required to handle an unexpected operational issue, but they can contribute, ensuring that best resources and information are made available.

[3] O. T. Gudmestad and M. Tiffany, "Issue Management, Treatment of "Bad News" On the Incorporation of Risk Analysis Results and Messages from the "Floor" in a Project." (working paper prepared for "Deepwater Horizon Study Group", University of California at Berkeley, CA, USA, 2010).

2.0 The Professional Team

A competent team has the know-how dealing with the tasks in hand,, i.e., the team members possess certain measurable skills, sound education, good intuitive judgment, experience, an ability to apply related knowledge to solve problems and a responsible attitude. The stakeholders will trust a professional team based on competence proven on previous track records of the individuals. A newly composed team must have the ability to be a learning team. Referring to M. P. Senge[4]:

> *"Organizations learn only through individuals who learn. Individual learning does not guarantee organizational learning. But without it no organizational learning occurs."*

The excellent drilling team mentioned above was a learning one that produced results beyond all expectations. They continuously improved their skills building on the individuals' strength.

In most organizations there is always an issue finding the right person for the task. Who is available, what should be prioritized, who knows who etc. The leader must therefore:

- Have a clear understanding of risks and change management,
- Establish clear roles and responsibilities,
- Follow a rigorous selection process of team members,
- Take on experienced and functional leaders,
- Ensure alignment of the team with outside functions,
- Establish a system and a formal methodology of working and good reporting routines,
- Handle interfaces with other organizational functions, authorities, contractors and suppliers, and
- Communicate situations in real time to superiors.

Figure 2.1 illustrates a typical team process in the oil and gas industry.

[4] M. P. Senge, The Fith Discipline, The Art & Practice of The Learning Organisation, revised edition (UK: Random House, 2006).

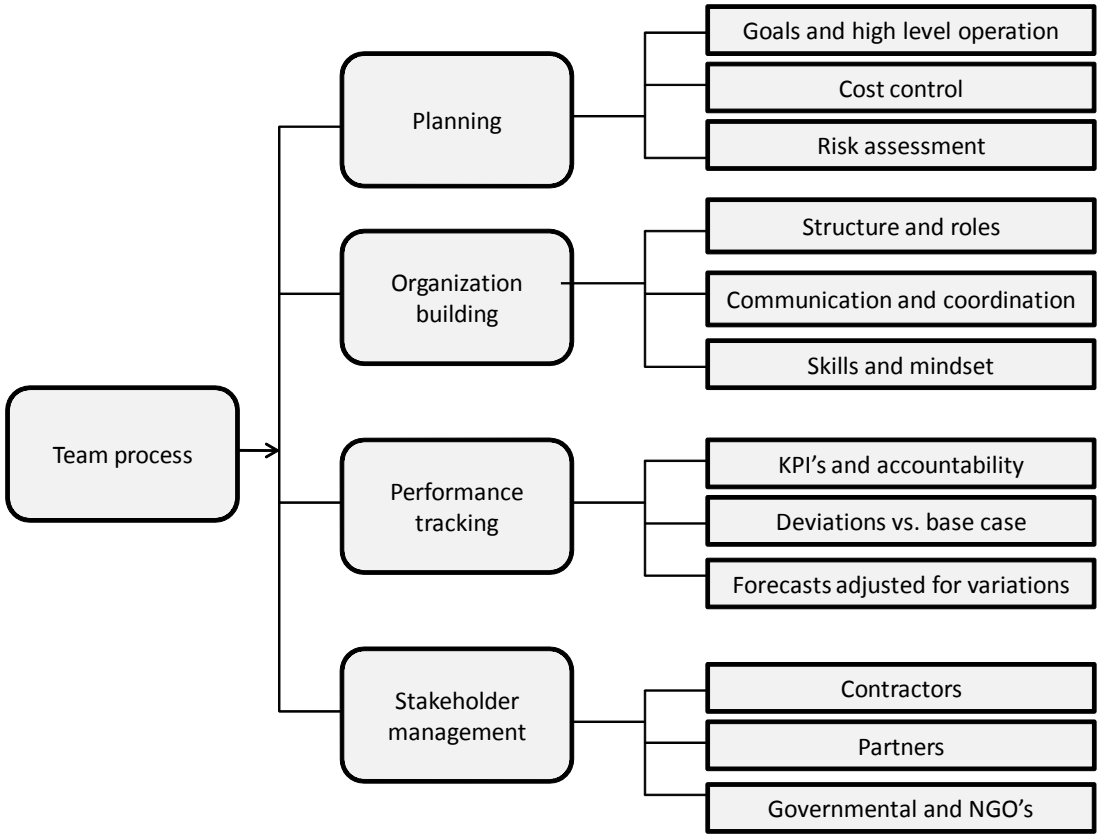


Figure 2.1 - Team process in the oil and gas industry.

2.1 Handling unexpected events

The team's ability to handle unexpected situations is very much dependent on its ability to communicate situations in real time and how the team has been trained for emergency preparedness and whether it has established necessary contingency planning (ISO/PAS 22399,[5] see Figure 2.2). A system for detecting incidents in real time should be in place, i.e., an electronic log including levels of alert pending seriousness of the incident that can be viewed by competent personnel.

[5] ISO/PAS 22399:2007, "Societal security — Guideline for Incident Preparedness and Operational Continuity Management," International Standardization Organization (2007)

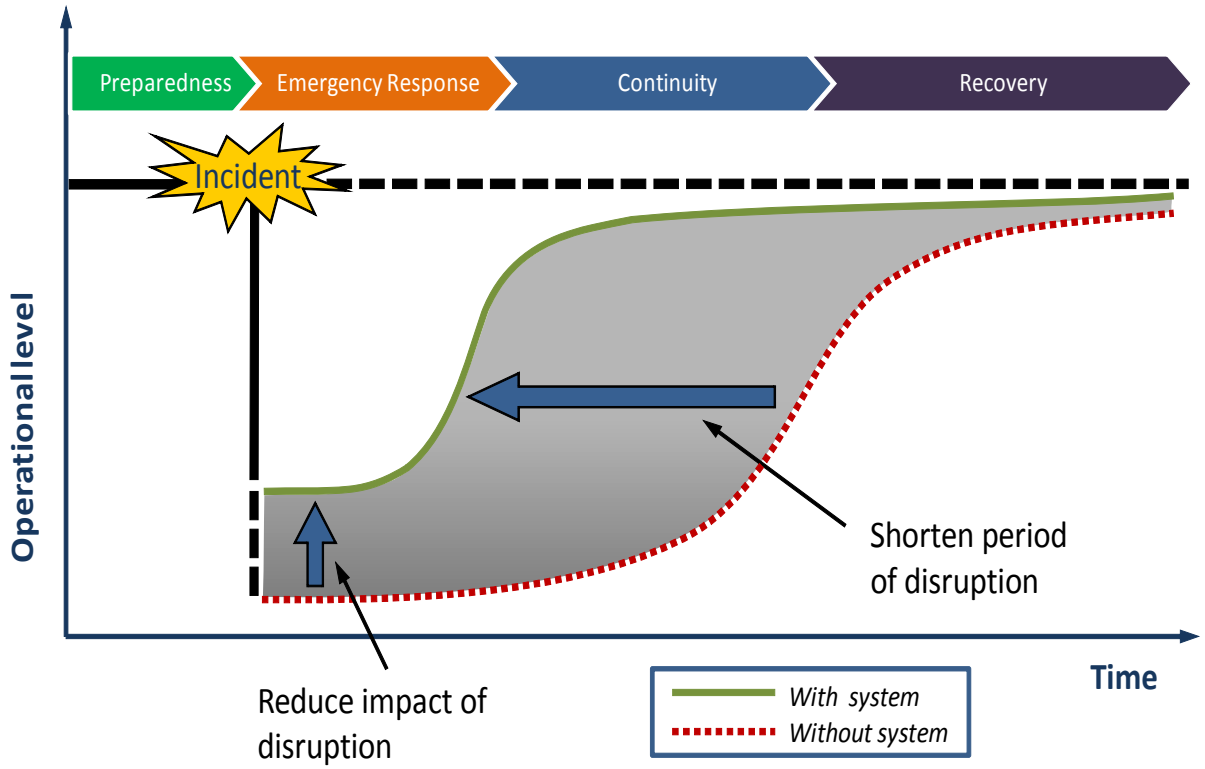


Figure 2.2 - A holistic management process.

The team's ability to handle unexpected situations is dependent upon ability to communicate, on training and on whether contingency planning is established.[6]

Referring to James and Wotten's research,[7] this has demonstrated that the interaction between technology and other nontechnology resources influences performance. Information technology can play a clear role detecting early warnings in order to prevent incidents escalating into crisis.

The team's performance and its ability to make decisions will be pending upon the working environment. In order to learn from experience, people need sufficient feedback about the accuracy and consequences of their judgments. This works well when the uncertainty is low. In the case of deepwater drilling there has been less opportunity to learn from experience. High task uncertainty (resulting from uncertainty in the external environment and uncertainty introduced by the information system) leads to poor cognitive performance.[8] Ultimately, it is the team leader competency to analyze and act before, during, and after an incident occur that determines the outcome. For large capital projects it has been proven that success rate is very much depended upon the Project Leader's competency.[9]

[6] ISO/PAS 22399:2007, op. cit.
[7] E. H. James and L.P. Wooten, Leading Under Pressure (New York London: Routledge, 2010), 39-65.
[8] D. Sarewitz (T. R. Stewart), Prediction, Decision Making, and the Future of Nature (Island Press, 2000), 41.
[9] L. Geoghegan and V. Dulewics, Project Management Journal, Vol 39 (Project Management Institute: John Wiley and Sons), 58-67.

Do note that people tend to discount the possibility of unprecedented risks. Because all the swans they have seen are white, they assume black swans do not exist. A black-swan event is beyond the realm of normal expectations and tends to be discounted, even by experts.[10]

2.2 Design – Risk Assessment

For deepwater wells with high pressure and high temperature there are no clear design criteria regarding the robustness of pressure barriers. Best practice is often from the latest well that has been drilled and completed. Authority regulations worldwide are basically made on hindsight and are generally not performance based and hence, all the major oil companies fulfill the general authority requirements. The oil and gas industry recognizes the challenges of securing pressure barriers, though many have experienced "near misses". The authorities in general, have not made changes to well design requirements for operating in deep water. It appears that the regulators have an "out of sight, out of mind" attitude to risks that seldom happen and have little competence with respect to the pressure barrier issue The Oil and Gas industry is well aware of that there are no recognized methods for "top-kill" other than drilling another appraisal well; hence, this is an acceptable risk by the industry. Who represents the best competency regarding well design? Is that the Oil and Gas Company, the drilling contractors, or the consultants?

When performing risk assessment the team will generally recognize worst case scenarios, but how will this ensure that the team is staying focused and pay attention to important details in everyday operations? Again, this will depend very much on the team leader competency.

When incident occurs it is often situations or issues that the designers did not contemplate, and for which there is therefore no possibility of having a "Standard Operating Procedure". This requires that the operators think and act independently. Their skills and experiences determine the success of handling the unexpected situation.

2.3 Outsiders looking in

A drilling team will be exposed to Quality Audits, Design Reviews, Peer-reviews, and third party verifications. Who perform these activities and what competency do they represent? For the Sleipner A, the concrete substructure that sunk during a controlled ballast test operation, August 1991, none of these outsiders managed to detect what was wrong with the design, even though the weaknesses of past design of other substructures were known and described in design basis documents. Was this due to lack of engineering acumen in these audit, review, and verification teams? In general the large consulting companies who perform verification or certification activities do not take on any responsibility what happens to the item being verified. So, do the oil and gas companies and regulators buy flawed insurance? How do you ensure that the right competency is present for the tasks to be performed and what price are you willing to pay?

The Interim Final Rule to Enhance Safety Measures for Energy Development on the Outer Continental Shelf[11] requiring submittal of certification by a professional engineer that the casing and

[10] S. Deming, Challenging Complacency – NASA – Ask Magazine issue 23, Spring 2006, http://askmagazine.nasa.gov/pdf/pdf_whole/NASA_APPEL_ASK_23_Spring_2006.pdf

cementing program is appropriate for the purposes for which it is intended under expected wellbore pressure. The professional engineer's competence requirement is not stated.

2.4 Key Personnel competency

A drilling team will be composed of a group of specialized drilling engineers, who should fulfill competence requirements with respect to education (theoretical background to understand the situation), experience (practical experience from solving difficult situations) and communication skills (ability to solve any upcoming questions as team work).

The team must be given authority to carry out the work in a professional way by being given the funds and time needed to do the work. A pressure on costs or schedule could easily result in shortcuts (like impatience to wait for the cement to cure) or skipping tests that costs money. Cooperation with auditors and persons who perform verifications is important

We will suggest that the team be composed of a group having the following competence requirement:

- The manager; experienced, preferable with a university degree, good track records and good communication skills, knows the overall criticalities.
- The supervisor; experienced, subject acumen, good planning skills, knows the criticalities.
- The engineer; deep understanding of the tasks in hand and knows the risks involved.
- The operator; well trained and experienced sees and reports deviations immediately.
- The auditor must be equally competent as the personnel being audited

The person(s) who verify should generally have a competence level that is beyond the personnel performing the tasks. Regardless of the team competence, however, the team cannot be expected to function adequately should there be pressure from the top company management to carry out the work in an unprofessional way, such as demanding shortcuts to be taken. "If you will not do as we request, you are on the next helicopter to land."

2.5 Build-up of competence

An organization must build up their competence in a strategic way. The novices must learn from the experienced thus ensuring that the organization has a long learning experience. There is a huge difference between 30 years of experience that can be shared and 1 year of experience repeated 30 times (different individuals). An efficient way to share experience is the identification of mentors for newcomers, ensuring that information is delivered to next generation "hands on."

[11] BOEMRE, "The Drilling Safety Rule, An Interim Final Rule to Enhance Safety Measures for Energy Development on the Outer Continental Shelf," (Office of Public Affairs, Bureau OF Ocean Energy Management, Regulation and Enforcement, 2010). http://www.doi.gov/news/pressreleases/loader.cfm?csModule=security/getfile&PageID=45792.

How can a team of committed managers with individual IQ's above 120 have a collective IQ of 63? The discipline of team learning confronts this paradox.[12] When teams are truly learning not only do they produce extraordinary results, but the individuals members are growing more rapidly than could have occurred otherwise. Regularly training to be prepared to handle unexpected situation should be a "must" for personnel being exposed to critical situations. Bear in mind the reality that a driver who obtained a license may not be the one you would like to drive your car or even who you would employ as a driver. A certificate or a license is no guarantee for excellent performance.

The oil and gas industry has the last decade been marred with "retirement/severing packages" offered to senior personnel in the companies. Latest example is when Statoil acquired Norsk Hydro's oil and gas division. All personnel above 58 years of age were offered very generous "pension packages" regardless of the criticality of their competence to the organization. The transfer was quickly executed (probably to show strength to the capital market) and 2100 people left the company at a total costs of 1.3 B US$.[13] The consequence was that a large number of less experienced personnel were left idle without sufficient guidance that is considered to have caused considerable uncertainty in the organization.

3.0 Conclusions

To ensure that the organization behaves like a high reliability organization,[14] an organization that is conducting relatively error free operations over a long period of time making consistently good decisions resulting in high quality and reliability operations, competence is required.

Deepwater well design and operation is a high "cutting edge" technology in which the predominant factor is learning by doing. It appears that some operating teams and organizations have not changed sufficiently to successfully address the challenges from operating on the continental shelf to deepwater.

Competence (both theoretical and experience) is considered critical to an organization and in particular in the teams formed when planning and executing deep water drilling. Furthermore, it is of utmost importance that the competent team be allowed to utilize their competence to avoid that corners are cut. The team members must recognize their strength and weaknesses and any lack of team competency must be acquired.

Stakeholders' competency must be recognized and one should have realistic expectations to regularities bodies.

[12] Senge, op. cit.
[13] Aftenblad Stavanger (2010). http://www.aftenbladet.no/energi/arbeidsliv/1115124/Over_2100_tok_gullpakken.html.
[14] K. H. Roberts, "Some Characteristics of One Type of High Reliability Organization," Organization Science, Vol. 1, No. 2 (March-April 1990): 160-176.

Appendix H

Looking back and forward: Could Safety Indicators Have Given Early Warnings About The Deepwater Horizon Accident?

Jon Espen Skogdalen, Ingrid B. Utne and Jan Erik Vinnem

1.0 Introduction

The Deepwater Horizon rig was considered to be a safe and efficient drilling unit. On April 20, 2010, BP officials visited the rig to praise seven years with no personal injuries.[1] In the evening of that very same day, gas exploded up the wellbore onto the deck and the rig caught fire. The explosions left eleven workers dead and 17 others injured. Two days later, the Deepwater Horizon rig sank.[2] The resulting oil spill gushed out of the damaged well for two months and caused the worst environmental disaster in US history, with impacts on local economies, sensitive coastlines and wildlife throughout the Gulf region.[3]

Systematic feedback on accident risk is of major importance to prevent accidents.[4] Often, hindsight shows that if early warnings had been revealed and managed in advance, the undesired incident could have been prevented.[5] Safety management of industrial systems, such as an offshore drilling rig, requires monitoring of safety performance, including the use of safety indicators. The term indicator may be defined in several ways. In this paper we define a safety performance indicator as "*a means for measuring the changes in the level of safety (related to major accident prevention, preparedness and response), as the result of actions taken*". (The definition is close to the OECD definition [6]).

In Norway, the risk level of the offshore petroleum industry is analyzed and presented on an annual basis. The first report was published early in 2001, based on data for the period 1996–2000. The methods used to collect data and analyze the risks were developed through the "risk level project" (RNNP). RNNP uses statistical, engineering and social science methods in order to provide a broad illustration of risk levels, including risk due to major hazards, risk due to incidents that may represent challenges for emergency preparedness, and risk perception and cultural factors.[7]

1.1. Objective of paper

To determine whether the Deepwater Horizon accident is a symptom of systemic safety problems in the deepwater drilling industry is difficult, unless the risk level related to major accident prevention, preparedness, and responses of the oil and gas industry is measured and evaluated over time. The Deepwater Horizon rig is subject to US legal and regulatory conditions, which do not require annual updates of the offshore petroleum industry's risk level in the same manner as the RNNP. Therefore, the question arises whether the indicators used in the RNNP could have given early warnings of a major accident, such as that on the Deepwater Horizon rig.

The objective of this paper is to assess safety indicators in the RNNP project and determine their relevance as early warnings for drilling accidents, including the Deepwater Horizon blowout. In addition, the paper discusses possible extensions and supplements with respect to drilling. The paper focuses on well integrity during drilling, and not on well production (hydrocarbon production, water and gas injection and well interventions) or emergency responses.

This paper is intended to be understandable for non-experts of drilling also. Therefore, we have in some places included short explanations. In addition, we advise the reader to use http://oilgasglossary.com for further explanations.

1.2 Structure of paper

The first part of the paper shortly describes deepwater drilling, principles and regulations related to well integrity, and possible causes to the Deepwater Horizon accident. Then, RNNP in relation to deepwater drilling is described, followed by discussions about possible extensions and conclusions.

2.0 Deepwater Drilling And The Deepwater Horizon Accident

Deepwater drilling[1] are complex operations in which engineering and commissioning mistakes, along with major workovers, can cost tens of millions dollars. Integrated operations (IO) are an important part of deepwater drilling, based on advances in information and communication technology (ICT). IO entails changes to organization, staffing, management systems and technology – and to the interaction between them. Increasingly, activities on land and offshore are being merged into a single operations unit. This means that work is controlled and organized in real time, often in different parts of the world.[8]

Many prospects in the deepwater GoM pose a unique combination of challenges when compared to deepwater wells in other parts of the world: Water depths of 3000 m, shut-in pressures of more than 690 bars, bottom hole temperatures higher than 195 °C, problematic formations with salt zones and tar zones, deep reservoirs at more than 9000 m true vertical depth, tight sandstone reservoirs (< 10 micro-Darcies (mD)) and fluids with extreme flow assurance issues.[9] Therefore, deepwater drilling is characterized by narrow drilling margins, and the narrower the margin; the more difficult to execute drilling operations.

In summary, some important challenges with deepwater drilling are:

- Huge costs
- Integrated operations
- Using the latest technology (depending on software/hardware)
- Complex casing programs
- Narrow drilling margins
- High pressure and high temperatures (HPHT)
- Tight sandstone reservoirs and fluids with extreme flow assurance
- Subsea operations

[1] Deepwater drilling refers to water depths greater than 1000 ft. Ultra-deepwater drilling refers to water depths greater than 5000 ft.

- Problematic formations
- Uncertain seismic
- Lack of experienced personnel

2.1 Well integrity and barriers

Well integrity is the application of technical, operational and organizational solutions to reduce risk of uncontrolled release of formation fluids throughout the life cycle of a well.[10.

The main undesired incidents related to well operations are (a) unintentional well inflow, (b) well leakage, and (c) blowout. The first is an unintentional flow of formation fluid into the wellbore (kick). The second is characterized by unintentional fluid flowing up through the BOP for a limited period of time until stopped by the existing well equipment or by defined operational means. A kick is instability in the well as a result of the well taking in gas, oil or water, and may lead to a blowout.[11, 12] A blowout in turn is defined as an unintentional flow of formation fluid from the well to surroundings or between the formation layers after the defined technical barriers, and the operation of those, have failed.[13]

Blowouts and underground blowouts are a result of loss of well control (LWC). A LWC incident is an uncontrolled flow of subterranean formation fluids, such as natural gases, oil, saline water, etc. and/or well fluids into the atmosphere or into an underground formation. A LWC incident or blowout can occur when formation pressure exceeds the pressure applied to it by a column of fluid such as a drilling fluid, cement slurry, cement spacer fluid, brine completion fluid, or any combination thereof in the column of fluid.[11] The risk of a blowout will vary with the design of the well, the type of flowing fluid, and formation characteristics.[13]

Barriers are required to ensure well integrity during drilling. Safety barriers are physical or non-physical means planned to prevent, control, or mitigate undesired incidents or accidents. Barriers may be passive or active, physical, technical, or human/operational systems. Barriers have been defined in terms of three characteristics[14, 15]:

- Barrier function: A function planned to prevent, control, or mitigate undesired incidents or accidents.
- Barrier element: Part of barrier, but not sufficient alone in order to achieve the required overall function.
- Barrier influencing factor: A factor that influences the performance of barriers.

Barriers are vital for maintaining safety in day-to-day operations. A well should have at least two barriers. The primary well barrier is the first obstacle against undesirable flow from the source (kick). On the detection of an influx, the well should be closed by activation of the secondary well barrier. The secondary well barrier prevents further unwanted flow if the primary well barrier fails.[13] The well control measures should be activated to remove the influx from the well to re-establish pressure overbalance, before the well operation can be resumed.

An overbalanced mud column is used to exercise a fluid pressure in the well in excess of the formation pore pressures to be encountered. The Macondo well, which the Deepwater Horizon rig was drilling, was performed as overbalanced operations, which is a common drilling, completion,

intervention, and workover operation method. The pore pressure is the pressure of the fluid inside the pore spaces of a formation or the pressure exerted by a column of water from the formation depth to the sea level, whereas the fracture gradient is the strength of the rock.[16] Such a mud column prevents influx of formation fluids into the well. In overbalanced operations, the mud column and system components support containment and are considered the primary well barrier. The secondary well barrier in overbalanced operations is the well containment envelope consisting of selected components of the BOP, or the BOP stack in total. The BOP has valves which can close around the drill string, and in an emergency sever the string and plug the wellbore.

2.2 The Deepwater Horizon accident

Deepwater Horizon was a 5th generation drilling rig commissioned in 2001, and outfitted with advanced drilling technology and control systems. In February 2010, the Deepwater Horizon rig, owned by Transocean and contracted by BP, took over drilling an exploratory well at the Macondo Prospect about 66 km off the southeast coast of Louisiana, USA. The water depth at the site is around 1,500 m, and the well to be drilled was 5500 m below sea level. After drilling, the plan was to plug the well, but the plans were changed during drilling and the well was changed to exploration to a production well.[1]

In the evening of April 20, 2010, a well control incident allowed hydrocarbons to escape from the Macondo well onto Transocean's Deepwater Horizon rig, resulting in explosions and fire, lasting for 36 hours until the rig sank.[17]

There are several investigations of the accident, and all point to no single cause of failure, but multiple violations at safety barriers. When this paper was written, the official investigation by the Presidential Commission had not been completed. Summarized are some findings to date[3, 17]:

- The annulus cement barrier did not isolate the hydrocarbons
- The shoe track barriers did not isolate the hydrocarbons
- The negative-pressure test was accepted although well integrity had not been established
- Influx was not recognized until hydrocarbons were in the riser
- Well control response actions failed to regain control of the well
- Diversion to the mud gas separator resulted in gas venting onto the rig
- The fire and gas system did not prevent hydrocarbon ignition
- The BOP emergency mode did not seal the well

These findings are debated and do not present the overall picture with respect to human and organizational causes. However, the remaining gaps do not alter the discussion or conclusions of this paper.

2.3 Barriers and legislation

In Norway, there is a requirement for a systematic application of two independent and tested well barriers in all operations. A similar requirement was adopted by the newly created US ***Bureau of Ocean Energy Management, Regulation and Enforcement*** (BOEMRE) in The Drilling

Safety Rule that requires two independent test barriers across each flow path during well completion activities. The barriers must be certified by a professional engineer.[18]

An important principle in the Norwegian Petroleum Safety Authority (PSA) Activities (AR Sec. 76) and Facilities (FaR Sec. 47) regulations is the concept of well barriers and their control. If a barrier fails, no other activities should take place than those to restore the well barrier. Activities regulation (AR Sec. 77) states that if well control is lost it shall be possible to regain the well control by direct intervention or by drilling a relief well. The operator is also required to have an action plan on how well control can be regained. In the U.S., 30 CFR 250 does not use the terminology or concept of well barriers. One paragraph, however, asks the question (30 CFR §250.401): "What must I do to keep wells under control?" The answer is somewhat in accordance with the barrier principle.[19]

In Norway, an overall requirement in the regulations (Management Regulations Section 1 and Section 2) is that the operator shall establish barriers and know the barrier functions. The operator must know the performance requirements related to the barriers that have been defined with respect to the technical, operational or organizational elements necessary for the individual barrier to be effective. Those barriers shall be established to reduce the probability of undesired incidents. The barriers shall also be tested. It will also be known which barriers are not functioning or have been impaired, and the responsible for the operation of a facility shall establish indicators to monitor changes and trends in major accident risk. The party responsible will take necessary actions to correct or compensate for missing or impaired barriers.[19]

The major points of the Norwegian barrier principle, legislation and guidelines for wells are, in summary:

- Failure criteria (leak rate) and test intervals shall be established for each barrier element.
- To the extent possible, the barrier elements shall be tested in the direction of flow.
- Integrity status of the barrier shall be known at all times when such monitoring is possible.
- The well should withstand the maximum anticipated differential pressure it may become exposed to.
- All elements for the two barriers shall be defined.
- The function of the barrier and its elements shall be defined.
- It shall be possible to activate the two barriers separately.
- The well should withstand the environment for which it may be exposed to over time.
- Single failure of well barrier elements shall not lead to uncontrolled outflow.
- The position of the barrier shall be known all the time.
- A single failure shall not simultaneously eliminate both barriers.
- It is possible to re-establish a lost well barrier or another alternative well barrier.

The Risk Level Project (RNNP) has been and is an important supplementary tool for the oil and gas industry to document compliance with Norwegian regulations related to major hazards.

3.0 The Risk Level Project (RNNP)

The Norwegian Petroleum Directorate (NPD), now the PSA Norway, initiated RNNP ("the Risk Level Project") in 1999. Its overall objective is to establish a realistic and jointly agreed picture of trends with respect to health, environment, and safety (HES) in the oil and gas industry. The first report was presented early in 2001, based on data from the industry for the period 1996–2000.[7] Annual reports have been published since then.[2]

RNNP aims at measuring the impact of safety-related work in the oil and gas industry, and helps identify areas critical for safety, including major hazard risks. Further, the understanding of the causes to undesired incidents and accidents, and their relative significance in the context of risk, is enhanced.[20] In addition, RNNP aims to create a reliable decision-making platform for the industry and authorities to enable joint efforts towards preventive safety measures and emergency preparedness planning.[7]

3.1 Major hazard risk in RNNP

Since no single indicator is able to express all the relevant aspects of HES, triangulation was needed in RNNP, i.e., utilizing several pathways to converge on the status and trends of HES levels. Thus, a decision was made to use various statistical, engineering and social science methods in order to provide a broad illustration of risk levels, applied to[7]:

- Risk due to major hazards
- Risk due to incidents that may represent challenges for emergency preparedness
- Occupational injury risk
- Occupational illness risk
- Risk perception and cultural factors

The risks related to major hazards are the focus of this paper. The major hazard risk components for employees working on offshore oil and gas installations are[7]:

- Major hazards during stay on the installations.
- Major hazards associated with helicopter transportation of personnel; for crew change purposes every two weeks, and with respect to shuttling between installations.

There are two different groups of indicators for major hazard risk in RNNP[7]:

- Incident indicators; i.e., indicators based on the occurrence of incidents and precursor incidents ("near-misses").
- Barrier indicators; i.e., indicators that measure the performance of barriers installed to protect against major hazards and their consequence potential.

[2] See http://www.ptil.no/trends-in-risk-level/category155.html?lang=en_US.

None of the indicators were available as data sets collated by the industry prior to the RNNP. The basic concepts of the methods in the RNNP are discussed extensively.[7]

3.2 Incident indicators in RNNP

RNNP has collected major hazard precursor data from the oil and gas industry for almost ten years with an accumulated data period of almost 15 years, covering the period from 1996 to the present. The term "precursor" is used for incidents that have occurred and potentially could lead to major accidents. Relevant major hazards for personnel on the installation are addressed in QRA studies, and QRAs were one of the main sources when indicators first were identified in RNNP.

In RNNP, categories of hazard precursor incidents are denoted "DFUs," which may be translated as, "Defined situations of hazard and accidents". The DFUs were selected according to the following criteria[20]:

- The DFU is an undesired incident/situation which has led, or may lead, to loss (of life and other values), and hence represents a risk contribution.
- The DFU must be an observable incident/situation, and one which it is feasible to record accurately.
- The DFUs must (as far as possible) cover all situations that can lead to loss of life.
- The DFUs are important for motivation and awareness, since they are utilized in the planning and dimensioning of the emergency preparedness.

Table 3.1 gives an overview of the categories of the DFUs related to major hazards included in RNNP. The values shown represent all oil and gas production installations and mobile drilling units which have operated on the Norwegian Continental Shelf (NCS) in 2003-2008:

Table 3.1 – Overview of major hazard precursor incident categories (DFUs).[3]

Major hazard precursor incident (DFU)	Frequency (annual average 2003-08)
Non-ignited hydrocarbon leaks	16.7
Ignited hydrocarbon leaks	0.
Well kicks/loss of well control	16.2
Fire/explosion in other areas, flammable liquids	2.5
Vessel on collision course	33
Drifting object	0.8
Collision with field-related vessel/installation/shuttle tanker	0.7
Structural damage to platform/stability/anchoring/positioning failure	7.8
Leaking from subsea production systems/pipelines/risers/flowlines/loading buoys/loading hoses	2.8
Damage to subsea production equipment/pipeline systems/diving equipment caused by fishing gear	2.2

3.3 Barrier indicators in RNNP

Adopting barrier indicators in RNNP occurred after the incident indicators had been fully established in 2002. The main emphasis was put on barrier elements associated with the prevention of fire and explosion, but structural barriers were included to some extent.[20]

Selected barrier data related to processing, wells, and structural integrity are provided through the RNNP survey. Companies report the availability and reliability for the barriers on the basis of periodic testing of chosen components. Any specific barrier comprises several interacting systems or elements. A leak must be detected before ignition sources are disconnected and emergency shutdown initiated. In other words, the sum of technical, operational, and organizational factors is crucial for determining whether barriers are functioning and effective at all times. The PSA, which has seen that barrier breaches cause accidents and incidents, pays particular attention to seeing that companies establish and develop systems for managing safety-critical barriers.[21] Barrier indicators in RNNP are based on the periodic testing of barrier elements as part of preventive maintenance schemes, using "man made" activation signals or stimuli (such as test gas releases).

[3] Standards_Norway, *NORSOK STANDARD D-10 Well integrity in drilling and well operations*, in *NORSOK*. 2004, Norwegian Technology Centre: Oslo. 162.[4] "Make a trip" - To hoist the drill stem out of the wellbore to perform one of a number of operations such as changing bits, taking a core, and so forth, and then to return the drill stem to the wellbore.[37]

The full list of technical systems on offshore installations, for which RNNP collects data, was at the end of 2009:

- Fire detection
- Gas detection
- Emergency shutdown valves on risers/flowlines (closure tests and leak tests)
- Wing and master valves (Christmas [X-mas] tree valves, closure tests and leak tests)
- Downhole Safety Valves (DHSV)
- Blowdown Valves (BDV)
- Pressure Safety Valves (PSV)
- BOP
- Deluge valves
- Fire pump start

3.4 Safety climate in RNNP

Safety climate can be described as the employees' perceptions, attitudes and beliefs about risk and safety.[22] These perceptions are often measured by questionnaires that provide a "snap shot" of the current state of safety. The RNNP seeks to measure the safety climate of individuals working offshore at a given time. The scores are aggregated to an organizational level to provide information representing the organization's current safety climate.

Several attempts have been made to analyze different data sources in order to discover relations between safety climate and major hazard risk. These attempts have been inconclusive so far, except for a recent study using linear regression to analyze safety climate and gas leaks, which concluded with significant correlation.[23] The safety climate questionnaire explains up to one fifth of the hydrocarbon leak variation. The results indicate that there is a relationship between the number of employees responding negatively to the questions with respect to safety climate and number of leaks.[23]

4.0 Indicators In RNNP Relevant For Well Integrity And The Two Barrier Principle

4.1 Relevant incident indicators in RNNP

With respect to incident indicators in RNNP, blowouts and precursor incidents to blowouts are related to well integrity. There were 15 blowouts in the Norwegian sector in the period 1999–2009. Fourteen of them were gas blowouts, and one was a shallow gas blowout. Major oil spills at sea are even rarer. Such infrequent occurrence data are therefore not ideal for providing meaningful indicators for RNNP. The same applies for data related to major accidents with personnel safety implications.

The main precursor incidents to blowouts are:

- Loss of well control, including kicks, may lead to blowouts that cause acute spills, irrespective of whether ignition occurs or not (ignition may reduce the amount spilled, but this is disregarded). Ignited blowouts may lead to "secondary spill" if the wellheads and/or X-mas tree fail, in addition to failure of downhole safety valve (DHSV).
- Hydrocarbon leaks (from process systems or risers/pipelines) may cause fire and explosion that escalate to wells, risers or storage if several barriers fail, thereby causing "secondary" spills.
- Damage to subsea production systems/pipelines/risers/flowlines/loading buoys/-loading hoses may lead to hydrocarbon leakages.
- Construction failures, either due to impact (such as from collision) or internal failure, may cause blowout and "secondary" spills if several barriers fail.

Kicks are precursor incidents that can cause a major accident. Information on wells kicks and loss of well control is collected in RNNP. Table 4.1 shows that there were 16,2 precursor incidents that involved well kicks. This is close to the number of non-ignited hydrocarbon leaks.

Hinton[24] reported that 11 % of all wells drilled on the U.K. continental shelf from 1988 to 1998 have experienced reportable kicks during well construction operations. Of these, 22 % were in HPHT wells (>10,000 psi and 149 °C). Other U.K. sources cited by Gao et al.[25] claim that HPHT wells have much higher reportable kick incident rates (1 to 2 kicks per well) compared to non-HPHT wells (1 kick per 20 to 25 wells). Some of the most frequent causes to kicks in U.K. drilling wells were also found in U.S. wells, such as lost circulation in the same hole section with potential flow zones, too low mud weight, and uncertainty in flow zone existence, flow potential, location, or other important characteristics.[11]

In the time period from April 1998 to March 1999, the Alberta Energy and Utilities Board (EUB) reported that 7094 new wells were drilled onshore in Canada, with a total of over 129,000 active onshore wells. Of the 7094 wells drilled, nine blowouts were recorded during the time period. Five were freshwater flows that occurred while drilling surface holes, meaning that there was no surface pipe or BOPs in place. The four other blowouts occurred at depths shallower than 350 m, resulting in sweet gas releases with no significant environmental impact. In the same period 101 kicks were recorded.[26] Even with the differences between offshore and onshore, the EUB regards the number of blowouts and kicks as a primary indicator of industry's drilling and servicing performance and pays particularly close attention to industry's response to these incidents.

In the GoM, there were 20 incidents from 1973 to 1995 related to well kicks after cementing surface casing. Another 13 similar incidents have occurred since 1995, with the most serious consequences being gas broaching to the surface, cratering, well loss, and rig and platform destruction by fire. Annular flow related to cementing surface casing has been identified as one of the most frequent causes of loss of control incidents in the GoM.[11]

The GoM frequency of deepwater kicks is high. The overall frequency of kicks is approximately 2.7 times higher in the US GoM deepwater wells than the overall Norwegian Continental Shelf

(NCS) experience. That said, the NCS kicks in deep wells, and especially HPHT wells, have occurred frequently.[27]

The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling describes the failure to adequately consider published data on recurring problems in offshore drilling. These included powerful "kicks" of unexpected pressures that sometimes led to a loss of well control, failing BOP systems, and the drilling of relief wells; the last lines of defense for a troublesome well. These problems have been relatively few considering the large number of wells around the world. However, that these problems occurred and have been known to petroleum engineers, demonstrates that wells do not perform in normal or regular ways.[28]

There is a common understanding among the regulatory authorities in Norway, UK, Canada and the U.S. that "kicks" are precursor incidents and should be avoided. The probability of kicks depends on geological conditions, but kicks can be prevented by proper well planning, design, and performance monitoring.[12, 29, 30] A safety factor or "kick tolerance" to help ensure safe well control conditions during drilling cementing operations typically is used to determine maximum operating pressures (equivalent circulating density (ECD), surge, etc.) based on leak-off test results and other measurements or calculations. In some higher pressure wells with a small margin between the mud weight and the fracture pressure, the recommended kick tolerance is nearly impossible to achieve. This is said to be particularly true for many wells drilled in the GoM.[11]

4.2 Relevant barrier indicators in RNNP

Some barrier indicators in RNNP are applicable with respect to drilling operations, well interventions, and production from wells, for example, the periodic testing of the following barrier elements:

- Wing and master valves (X-mas tree valves, closure tests and leak tests)
- Downhole Safety Valves (DHSV)
- BOP

The requirement in the Norwegian regulations to systematic application of two independent and tested well barriers in all operations enables data collection related to incidents where the principle is broken.

Usually, fluid column is the primary barrier. The secondary well barriers consist of one or more of the following[29]:

- Casing cement
- Casing
- Well head
- High pressure riser
- Drilling BOP
- Drill String
- Stab-in safety valve

- Casing float valves
- Annulus access line and valve

In RNNP, there is a classification system for all producing wells on surface installations and subsea wells, whereby each well is classified into one of the following categories:

- Green: Healthy well, no or minor integrity issue.
- Yellow: One barrier leaks within the acceptance criteria of barrier degradation, the other is intact.
- Orange: One barrier failure and the other is intact, or a single failure may lead to leak to surroundings.
- Red: One barrier failure and the other is degraded/not verified or external leak.

The RNNP survey for 2009 covers a total of 1712 producing wells on the NCS and eight operator companies; BP, ConocoPhillips, Exxon Mobil, Norske Shell, Statoil, Marathon, Talisman and Total (in random order). Figure 4.1 shows well categories by percentage of the total number of wells, 1712.

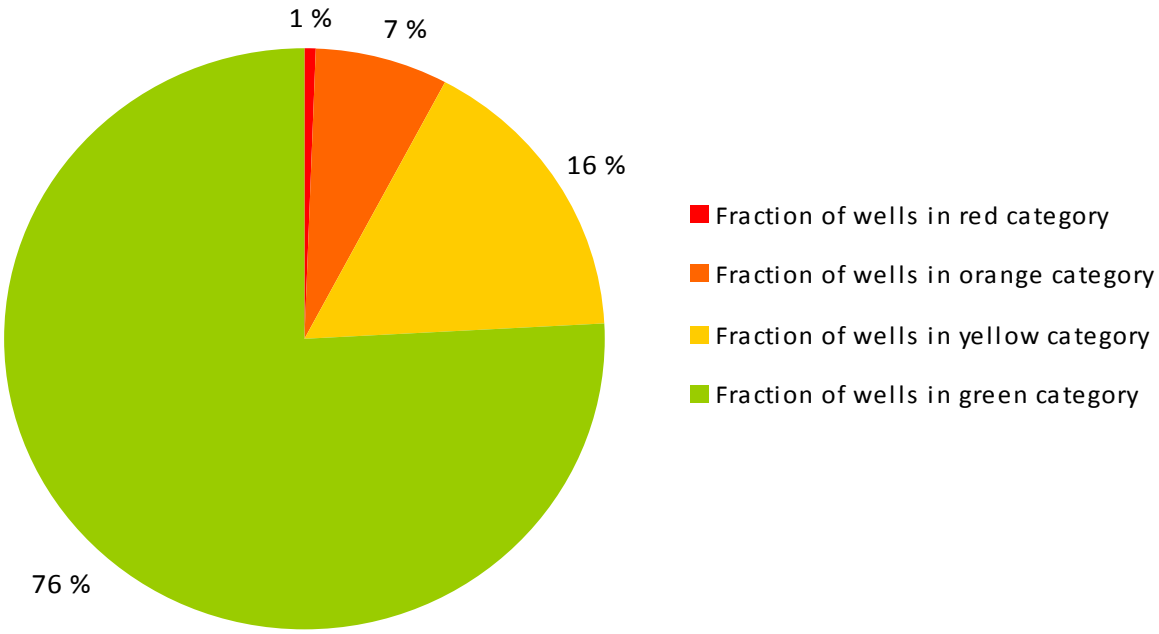


Figure 4.1 – Well classification –category red, orange, yellow and green, 2009.

The results show that 8 % (11 % in 2008) of the wells have reduced quality in relation to the requirements for two barriers (red + orange category). Sixteen percent (13 % in 2008) of the wells are in the yellow category, including wells with reduced quality in relation to the requirement for two barriers, but the companies have implemented various compensatory measures to meet the two-barrier requirement. The remaining wells, i.e., 76 % (as in 2008), fall into the green category meeting the requirement for two barriers in full.

4.3 Relevant human and organizational aspects

PSA has together with the petroleum industry worked to reduce the number of non-ignited hydrocarbon leaks, which is considered as a valid and reliable indicator reflecting the risk of major accidents caused by ignited hydrocarbon leaks. Release statistics show that half of the leaks from hydrocarbon systems on the NCS are caused by manual interventions in the process system. Engineered safety barriers are often partially deactivated during these operations in order not to cause disruption of production. The occurrences indicate that operational barriers related to containment of leaks are not functioning sufficiently during these intervention operations.[31]

A reasonable question is: Do kicks demonstrate similar organizational features as found between hydrocarbon leaks and safety climate? A study performed by Dobson[32] showed that most kicks experienced on the UK Continental Shelf are directly linked to geological conditions at the well location, and most involve conditions difficult to detect before the well is drilled. Other incidents are indirectly linked to the geological conditions, such as the challenges related to cementing casing in halite formations or in keeping the mud weight sufficient to prevent the well from flowing, but not so heavy that losses are induced. The latter challenge is not limited to HPHT wells in the GoM but is also encountered in the complex reservoirs of the Northern North Sea and the Lower Permian sands in the Southern North Sea.[32]

A significant, though small, proportion of kicks are due to human error, according to Dobson.[32] Examples are failure to shut down water injection, using an un-weighed wash during cementing operations or allowing excessively large influxes. There are two areas of concern to UK HSE as the safety regulator for the UK Continental Shelf: The most pressing issue is human error as a continuing factor in well incidents. If drilling activity levels continue as in recent years, appropriate well-control training of personnel engaged in both rig site operations and in operational planning needs to be accorded the highest priority.[32]

5.0 Extending The Indicators In RNNP For Deepwater Drilling And Well Integrity

The main focus with respect to major hazard indicators in RNNP is on production installations. There are only a very limited number of precursor incident indicators and barrier indicators for mobile drilling units. This is one of the reasons why RNNP indicators would not be suitable as early warnings for accidents like the Deepwater Horizon. Well control procedures are established to safely prevent or handle kicks and reestablish primary well control. The number of kicks and blowouts are relevant indicators, but there is a need for developing a set of deepwater drilling indicators for precursor incidents leading up to those kicks and blowouts. In this section areas for extending the safety indicators with respect to well integrity, to be used in RNNP, similar projects, or in companies, are investigated. Central issues regarding the Macondo well illustrate how the extensions or supplements are related to well integrity.

Safety indicators are not straightforward and simple. The success of indicators is related to the extent to which they are[33]:

- Able to drive process safety performance improvement and learning.
- Easy to implement and understand by all stakeholders (e.g., workers and the public).

- Statistically valid at one or more of the following levels: industry, company, and site. Statistical validity requires a consistent definition, a minimum data set size, a normalization factor, and a relatively consistent reporting pool.
- Appropriate for industry, company, or site level benchmarking.

In addition to the above factors, major indicators must reflect hazard mechanisms, i.e., be valid for major hazards, be sensitive to change, show trends, be robust to manipulation and influence from campaigns giving conflicting signals, and not require complex calculations.[7]

Often, a major challenge is that there is not enough data to support a basic set of reliable and valid safety indicators. Therefore, a broad perspective is needed when developing and analyzing indicators. In addition, the safety indicators should reflect the phases of deepwater drilling (and drilling in general). These phases are the well planning phase and the drilling phase, consisting of drilling, running casing, cementing, circulation, fluid displacement and clean-up, and completion.

Figure 5.1 gives an overview of the main lifecycle phases of the well and aspects related to undesired incidents and relevant barriers of deepwater drilling. The different areas relevant for extending or supplementing safety indicators from RNNP with respect to well integrity are discussed thereafter.

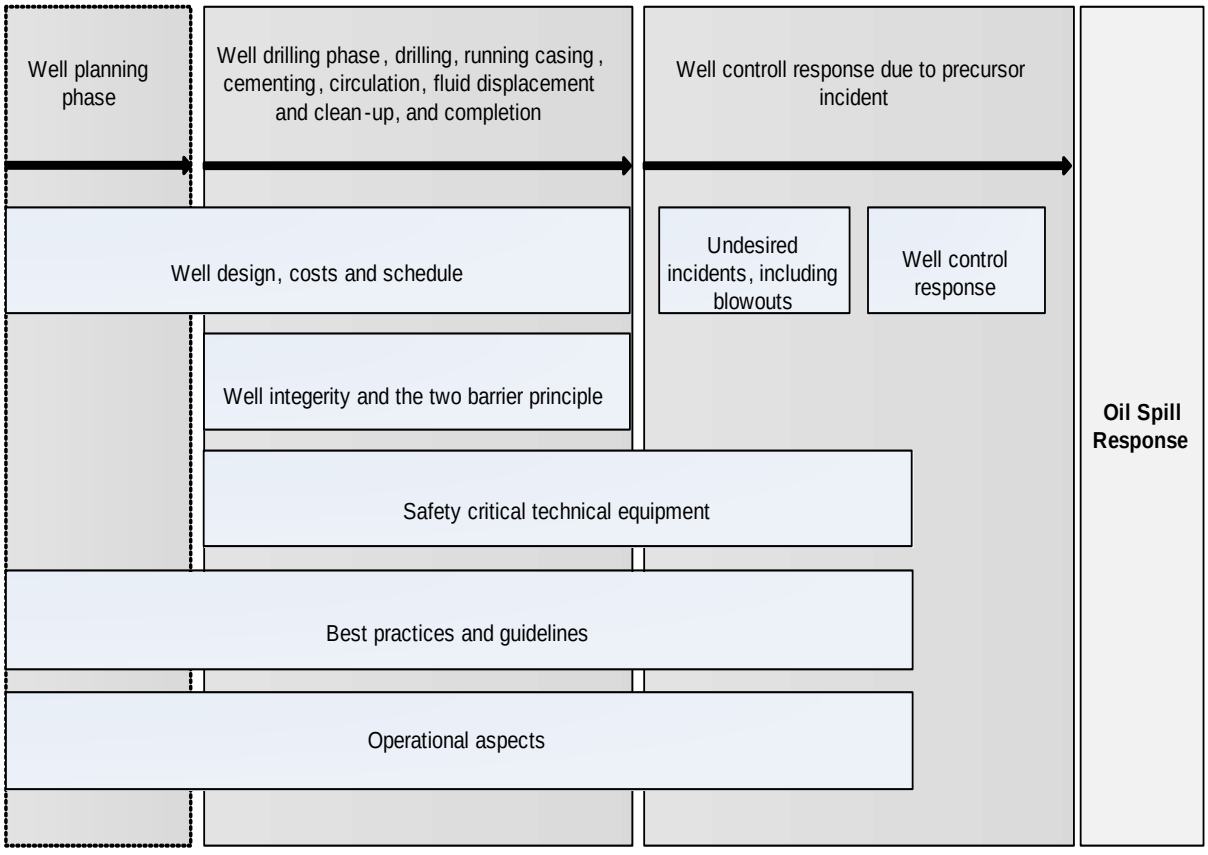


Figure 5.1 – The life cycle phases of a well (excluding production).

5.1 Well design, costs, and schedule

Deepwater wells in the GoM require a great degree of investigation, including conceptualizing during the planning and design and intense communication with a larger team for longer periods of time. Much time in the design process is devoted to the pressure and temperature profiles, mechanics (burst, collapse, axial loads, etc), data acquisition from previous wells, and other "conventional" processes of well design. Although all processes are critical, many times it may be profitable for the team to spend as much time in "data immersion," conceptualizing how a well should be drilled. "Data immersion" is time-consuming in terms of studying all available offset data, reading every hand written note, mud recaps, bit records, etc. The following are typical problems that occur if time is not spent on well design and planning[34]:

- Lack of knowledge of overall geology and basin mechanics
- Lack of production knowledge and reservoir behavior (shallow and deep)
- Not understanding the production profile of the target zone
- Not understanding the design philosophy of previously drilled wells
- Not understanding why previous wells got in trouble
- Lack of "immersion" in data available
- Not integrating contingency planning
- Cost savings mentality

According to BOEMRE, the greatest risk factor in the deepwater GoM is the sizeable flow rates, i.e., fields with very high daily output and good overall economics.[28] The petroleum industry points at the importance of high operating performance as the key for sustained economic success. Reduced maintenance requirements and increased reliability are key elements in the design stages of deepwater developments. Shutting down a 30,000+ barrels per day well impacts the bottom line directly.[35]

The Deepwater Horizon rig was 43 days overdue on April 20th, and the total costs had reached about $139 million dollars in the middle of March. The original costs were estimated to $96 million dollars, [[1]Aug 26th] indicating more than $40 million dollars in additional costs up to that point in time.

The relationship between schedule and cost, and assessment and prioritization of risks, is an essential element of risk management. Better understanding can be achieved by collecting data related to schedule and cost and compare with supplementing safety indicators.

5.2 Undesired incidents and crew's response time

During drilling and completion of the well, two aspects are of main interest with respect to indicators; well incidents and the crew's response if incidents occur. During drilling several undesired incidents may occur, among others stuck string, lost circulation, and shallow gas influx.[29] All these incidents were experienced by the Deepwater Horizon rig in March 2010.[[1], Oct. 7th]

Ballooning formations take mud (partial losses) during drilling into a fracture and give that mud back when the imposed pressure is relieved. Ballooning is a major concern as their occurrence can often complicate identification of key kick signals.[34] Ballooning is also called wellbore breathing, and losses and gains. Ballooning is particularly common in deepwater drilling because of the

frequently encountered narrow pore pressure and fracture gradient window. The phenomenon is characterized by mud losses with mud pumps on, and mud returns with pumps off. The principal risk for deepwater drilling in overpressured environments is that any increase in mud volume may be interpreted as a kick, requiring additional time being spent to flow-checking the well. Misdiagnosis can also lead to the decision being made to increase mud weight. As the occurrence of losses and gains signifies drilling with a mud weight close to the fracture gradient, additional mud weight increases can result in breaking-down the formation and inducing more problematic large-scale losses from the wellbore. The prediction and diagnosis of instances of mud losses and gains is, therefore, of clear importance in the planning and execution of deepwater wells.[36]

Swabbing is to reduce pressure in a wellbore by moving pipe, wireline tools or rubber-cupped seals up the wellbore. If the pressure is reduced sufficiently, reservoir fluids may flow into the wellbore and towards the surface. Swabbing is generally considered harmful in drilling operations, because it can lead to kicks and wellbore stability problems. Swabbing on trips[4] is the most likely cause of well controls problem in ultra deepwater drilling. In ultra-deep wells, swabbing is often complicated when a well is ballooning or when mud and formation gradients are relatively close. Furthermore, it has been shown that computation of swab pressures on the basis of steady-state flow is often incorrect.[34]

SINTEF performed in 2001 a study of deepwater kicks in the GoM for MMS.[27] In ranked order, the most significant contributors to the kick occurrences were:

- Too low mud weight (23)
- Gas cut mud (17)
- Annular losses (9)
- Drilling break (9)
- Ballooning (7)
- Swabbing (5)
- Poor cement (2)
- Formation breakdown (1)
- Improper fill up (1)

The contributors in the list do not necessarily lead to a kick.

In addition to recording the number of undesired incidents, the time between the first "signals" of an undesired incident and subsequent well control actions indicates the crew's situation awareness, training, competence, and management. Data are recorded real-time during drilling and it is therefore possible to analyze the time from the incident occurred until actions were taken and control of well achieved.

The Deepwater Horizon rig workers tested the integrity of well on April 20th. The crew conducted a positive-pressure test on the production casing, and a negative-pressure test to assess whether the cement barrier and the mechanical barriers could withstand an underbalanced situation. After having tested and (incorrectly) interpreted the results to be successful, they continued replacement of the mud with seawater.[17]

According to BP,[17] flow indications started approximately 51 minutes before the blowout. The influx was not detected until the hydrocarbons had entered the riser, 40 minutes after the first influx. Real time data were available to the drilling crew,[17] who should monitor changes to pit volume, flow rate and pressures in order to identify potential flows and losses.[11]

During the afternoon on April 20th, well monitoring might have been complicated. From 13:28 to 17:17, mud was offloaded to the nearby supply vessel, and some pits were being cleaned and emptied. These operations reduced the ability to monitor changes to the pits' levels. In addition, preparations for the next completion operations were carried out, such as preparing for setting the plug in the casing after replacing with seawater. The BP investigation report[17] states that it does not seem that pit volumes were effectively monitored the rest of the evening. Comments from Halliburton support this statement.[1]Oct 8th

Even if the crew at the Deepwater Horizon rig had been able to gain control of the well, it would be useful to know why the response time was that long. Response time is an aspect to consider in an extension of the safety indicators in RNNP, in order to enable learning by experience and accident prevention.

5.3 Well integrity during drilling and the two barrier principle

According to the barrier principle in the Norwegian regulations, the following situations are reported to the authorities[29]:

- Positive indication of flow from wellbore.
- The wellbore is closed by shutting in the BOP
- Pressure or pressure build up is registered in the closed-in wellbore.
- Kill operation is initiated.

In the US, BOEMRE requires that loss of well control (LWC) is reported.[38] This includes:

- Uncontrolled flow of formation or other fluids; the flow may be to an exposed formation (an underground blowout) or at the surface (a surface blowout).
- Flow through a diverter.
- Uncontrolled flow resulting from a failure of surface equipment or procedures.

On April 14th 2010 the final decision was made to use the production long string for the Macondo well instead of a liner tieback.[1] Aug 26th During discussions in BP it was noted that under certain circumstances the long string option would only provide one barrier; the seal assembly in the well head. With a requirement for two barriers, this would not have been an acceptable design. However, in some cases the well integrity may be reduced, as discussed regarding the classification of production wells in RNNP (Section 4.2).

5.4 Best practices and guidelines

There are numerous guidelines related to drilling.[11, 12, 16, 29, 39-43] They describe best practices and recommendations in detail. The compliance with guidelines should be a part of precursor investigations and used as basis for developing indicators. The compliance with standards/guidelines

has become even more relevant recently when BOEMRE made mandatory the practices in the American Petroleum Institute's (API) Recommended Practice 75 (RP 75).[44]

Regarding the Macondo well, it may be questioned if best practices were followed. In the letter to BP CEO Tony Hayward, the US Committee on Energy and Commerce[45] raised questions about five decisions which they believed "posed a trade-off between cost and well safety":

- The choice of well design
- The number of "centralizers" to prevent channeling during cementing
- No cement bond log to evaluate the quality of the cement job
- Failure to circulate potentially gas-bearing drilling muds out of the well
- Not securing the wellhead with a lockdown sleeve before allowing pressure on the seal from below

BP chose to use a single production casing instead of the liner tieback, a design that would save $7 million to $10 millions.[1] Oct. 7th The choice of well design increased the need for running a cement bond log.[1] Oct 7th Because of the importance of getting a good cement job, one that is bonded both to the casing and to the geological formation in which the well is dug, a series of measurements called a "cement bond log" is often run. A sonic scanning device is lowered through the well on a wireline. It checks whether there are imperfections in bonding or other problems in the cement. If there are, more cement can be squeezed into affected sections. Schlumberger personnel were called to the rig to be ready to do such work, but departed in the morning of April 20th having been told their services were not required. Documents suggest the cost saving in not having a "cement bond log" to about $118,000.[46]

Centralizers ensure that the casing is centralized during cementing to prevent channeling and a low quality cementing job. Halliburton recommended 21 centralizers to be used, but BP had six available, due to a misunderstanding that 15 of them were of the wrong kind on the rig. In hearings[[1] Oct 7th] it was stated that Halliburton and BP disagreed on the number of centralizers, and that the risk of getting a gas flow problem increased if they used ten or less centralizers.

5.5 Technical condition of safety critical systems

In 2000, Statoil developed a system for assessment of Technical Safety Condition (TTS).[47] This system assesses the conditions of technical barriers where considerable prior knowledge was available about how accidents could be caused through failures. TTS evaluates a wide set of safety functions against defined performance standards. There are 22 different Performance Standards (PS) for example regarding the gas detection system, alarm management, and well barriers. Each performance standard consists of performance requirements. The assessment is carried out at a detailed level by using checklists. The ratings in TTS are classified according to a scale with grades A (Condition significantly above reference level) through F (Unacceptable condition). The results are aggregated to illustrate the performance of an installation.[48] There exists a large amount of data collected and several oil companies have adopted the method. An important part of the Performance Standard related to well integrity is the maintenance and inspection of the BOP.

At the Deepwater Horizon rig, the BOP did not isolate the well before and after the explosions. The BOP may have been faulty before the blowout or it may have been damaged due to the

accident. According to BP, several maintenance jobs of the BOP were overdue, and leaks from the hydraulic control system had been discovered at the time of the accident.[17] The BOP on the Deepwater Horizon was not recertified in accordance with federal regulations because the certification process would require full disassembly and more than 90 days of downtime.[1] Aug 25th

The Transocean subsea superintendent said he didn't hear about the leaks before the incident and left it up to rig workers to determine if they were significant enough to report. The Transocean subsea superintendent and the subsea supervisor on the Deepwater Horizon acknowledged that the blowout preventer had not gone through a recertification every three to five years, as set by federal regulations. The subsea superintendent brushed that aside, however, saying Transocean considered it sufficient to simply monitor the device's condition while it was in use, rather than having to bring it to dry dock to get a full certification. Because the government regulation references an industry standard, the subsea superintendent said he took it to be a recommendation, not a requirement. Co-chairman of the investigative panel criticized Transocean for ignoring the government's minimum standard and choosing to follow its own monitoring program instead.[1] Aug. 25th

The chief electronics technician at the Deepwater Horizon stated in a hearing that some of the rig's alarm systems, such as the rig's general alarm, had been inhibited. This means that the sensory is still active and would register high gas levels, toxic gas or fire to a computer, but any warning signals would not be triggered.[1] July 23rd

Another issue they were struggling with onboard the rig was the chairs used for controlling the drilling functions. There were three chairs: A, B, and C. These chairs control everything, such as top drive, mud pumps, and hydraulics. The last three to four months these computers had locked up so no data could go through the system. A new system was ordered, but there were bugs with new operating system as well because they could not make the old software run correctly on the new operating system. This means at times they would lose track of what was going in the well.[1] July 23rd

The technical barriers related to reducing the consequences of a blow-out should be monitored to reveal the changes in the level of safety over time. The technical barriers are very much the same as those related to gas leaks, and is an area to consider when extending or supplementing existing safety indicators. In 2006 and 2007 there were two very serious precursor incidents – one on the Visund Platform in the Norwegian sector and one on the Rough Platform in the UK sector.[49] The former incident released over 900 kg/s into the platform – but all, the safeguards worked – ignition controls, gas detection, ESD systems, blowdown, and no ignition occurred. On the Rough platform the release was 400 kg/s and ignition did occur, but again the barriers worked and the incident was limited.[50] Both of these had the potential to be total losses, as with Deepwater Horizon, if the barriers had failed.

5.6 Operational aspects

In 2006, Statoil initiated a project to extend the TTS system into an OTS (Operational Condition Safety) system. The objective of OTS is to develop a system for assessment of the operational safety condition on an offshore installation/onshore plant, with particular emphasis on how operational barriers contribute to prevention of major hazard risk, and the effect of human and organizational factors (HOFs) on barrier performance. OTS is a means for measuring the changes over time in the level of operational safety as the result of actions taken.

The following operational performance standards have been defined in OTS[51]:

- Work performance
- Competence
- Procedures and documentation
- Communication
- Workload and physical working environment
- Management
- Management of change (MOC)

The OTS concept resembles the TTS system. The main principle of the OTS development is that the assessment of operational safety conditions shall be risk based, i.e., that the selection of influencing factors and checklist questions shall be based on the highest impact on major hazard risk.[48]

In the training area, MMS did in 1998 move away from requiring workers who were engaged in well control and production safety system operations to attend MMS-accredited schools. The responsibility for ensuring workers were properly trained was shifted to the operator.[52]

The MOC process was generated on the Deepwater Horizon rig. Several questions had to be answered, such as about the reason for change. The MOC process was required when there were temporary and permanent changes to organization, personnel, systems, process, procedures, equipment, products, materials or substances, and laws and regulations.[1]Aug 25th The MOC documents were reviewed and approved.[1] July 22nd However, it may be questioned whether the BP MOC process sufficiently reduced risks related to the changes that occurred. According to BPs own investigation report,[17] the BP Macondo team did not follow a documented MOC process. Therefore, they did not discover that the additional centralizers delivered to the rig were correct. Instead, they thought they had gotten a wrong kind of centralizers and decided to use the remaining six for the cementing.

In the chain of command in the BP engineering and operations, five individuals had been less than 5 months in their positions at the time of the accident.[1] Aug 26th Management of change documents were worked out on paper, but there was an ongoing transition to an electronic system.

Developing relevant indicators for human and organizational issues with respect to drilling is complicated. In RNNP safety culture is assessed by using interviews and questionnaires, and the same may be applied to drilling rigs. Another important aspect is to ensure a good quality MOC process for drilling. The performance standards in OTS are very much the same factors described as key capabilities for success for drilling professionals by Boykin.[53] The performance standards do also cover most of the weaknesses of current work processes in drilling pointed out by a large research and development program on drilling and wells within Integrated Operations (IO) in the Norwegian petroleum industry.[54]

6.0 Discussion and Conclusions

The indicators in RNNP are intended to be early warnings of possible increases in major hazard risk on a national industry level. Annually, there are about 80 to 100 precursor incidents for the NCS

as a whole, corresponding to slightly less than one precursor incident per installation per year. In addition, there are tens of thousands of data reported from the periodic testing of safety barrier elements for major hazards. The purpose of these indicators is to provide early warnings with respect major hazard risk at a global level, i.e., for the petroleum industry as a whole, and not for individual installations or companies, due to the low number of occurrences. On the other hand, the barrier indicators may be used for individual installations, due to a much higher number. The use of barrier indicators for individual installations and companies is discussed in detail.[7]

It should be noted that the main focus with respect to major hazard indicators in RNNP is on production installations. There are only a very limited number of precursor incident indicators and barrier indicators for mobile drilling units. This is one of the reasons why RNNP indicators "as is" would not be suitable for early warnings for accidents like the Deepwater Horizon.

The second objective of this paper is to discuss possible extensions of the safety indicators in RNNP with respect to offshore deepwater drilling. To obtain valid and reliable indicators is a major challenge. Underlying causes and contributing factors may be of such a nature that it is difficult to obtain quantitative measures that are valid individually, and have adequate coverage collectively, meaning that all aspects of a given contributing risk influencing factor are covered by a set of indicators.

The number of kicks is an important indicator for the whole industry when it comes to deepwater drilling, because it is a precursor incident with the potential to cause a blowout. However, there is a need for a broad perspective when collecting and analyzing indicators. In this paper, we have suggested aspects to consider for extending the safety indicators related to well integrity and the two barrier principle, well planning, schedule and cost, undesired incidents, and well monitoring/intervention. In addition, best practices/guidelines, status/failure in safety critical technical equipment, and operational conditions have been discussed. Within these areas, data is available, and in several cases the data is recorded, and have been recorded for years by the regulatory authorities, research communities, companies, and rigs. Still, the data is not used as basis for indicators. In a company, the Reliability, Availability and Maintainability environment collects data related to the technical condition of an installation. The Occupational Environment Committee studies the data related to safety climate and culture. Safety climate, the technical condition, and the number of precursor incidents are influencing each other and should be considered together.

According to the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, the Deepwater Horizon accident raises an important question to which extent the accident is a symptom of systemic safety problems in the whole deepwater drilling industry. To find the answer to such a question is very difficult without knowing the risk level related to major accident prevention, preparedness, and responses of the oil and gas industry, measured and evaluated over time. Therefore, we recommend the US authorities to initiate a similar project to RNNP. Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate incidents.[55] We have in this paper suggested a wide approach to areas for supplementing existing safety indicators and thereby for identifying risks. Safety indicators can also support the assessment and prioritization of risks.

In the Deepwater Horizon Incident Joint Investigation,[1] the Chief electronics technician Transocean testified that Deepwater Horizon had earlier experienced a kick due to software failure

in the drilling systems. A single kick does not show a trend, but it can function as an early warning signal, and proper actions can be taken based on precursor incident investigation. It is the authors' view that there is a need for more extensive investigations of precursor incidents like "kicks" to ensure improved learning. The broad approach to collecting and analyzing indicators in this paper would possibly have pre-warned several of the contributing factors in the Deepwater Horizon accident:

- The status of the BOP and fire and gas system could possibly been have revealed by indicators related to status/failure in safety critical technical equipment.
- The insufficient negative-pressure test and well control response could possibly been revealed by indicators related to well control response and operational conditions (competence, procedures and documentation, communication, management).

The Deepwater Horizon accident was a result of failures in multiple barriers related to human, organizational and technical barrier elements. Barriers planned and included in design do often degrade over time. Root causes are complex and rarely due to deliberate intent or risk taking. Serious blowouts are rare and the rationale for many safeguards may be lost over time and the continuous activities to keep them functional may not occur. Normalization of deviance, and even not having defined what a deviance is, is an important issue to investigate further.

The approach discussed in this paper demands cooperation across national borders, operators, vendors, specialist environments, as well as between industry and regulatory authorities. The need for cooperation was also pointed out by BP-employees Addison et al.[56] in advance of the Deepwater Horizon accident:

"The trend of deepwater discoveries in the GoM is shifting towards one with greater challenges across many disciplines represented by the conditions in the lower tertiary discoveries. The solutions to these challenges will require cooperation among the operators, the engineering contractors and the equipment suppliers working with the regulatory authorities to pave the way for the safe and reliable development of these future fields. Over the next decade the rate of advancement in deepwater technology development will need to accelerate to enable offshore operators to move forward in developing the most recent exploration successes in the GoM".

7.0 Acknowledgements

The authors are grateful to comments and reviews by members of the Deepwater Horizon Study Group. Special thanks to Senior Researcher Emery Roe (UC Berkeley) and Professor Paul Schulman (Mills College in Oakland, California) for discussions, inputs and review. Skogdalen and Vinnem also acknowledge the financial support from the Norwegian Research Council and Statoil. Skogdalen does also acknowledge the financial support by Fulbright.

8.0 Abbreviations

Table 8.1 – Abbreviations

Term	Definition
API	Application Interface
BDV	Blowdown Valve
BOP	Blowout Preventer
BOEMRE	Bureau of Ocean Energy Management, Regulation and Enforcement
DHSV	Downhole Safety Valve
DFU	RNNP – 'hazard precursor event'
ECD	Equivalent Circulating Density
EUB	Energy Utilities Board (Alberta, Canada)
HSE	Health, Safety, and Environment
HES	Health, Environment, and Safety
HOF	Human and Organizational Factors
HPHT	High Pressure, High Temperature
ICT	Information and Communications Technology
IO	Integrated Operations
I/O	Input / Output
LWC	Loss of Well Control
mD	Micro-Darcies, a measure of gas permeability
MOC	Management of Change
MMS	Minerals Management Service
NCS	Norwegian Continental Shelf
NPD	Norwegian Petroleum Directorate
PS	Performance Standard
OTS	Operational Condition Safety
QRA	Quantitative Risk Assessment
RNNP	Norwegian Risk Level Project – trends in risk levels on NCS
TTS	Technical Safety Condition

9.0 References

1. Deepwater Horizon Incident Joint Investigation, The U.S. Coast Guard (USCG) / Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) Joint Investigation Team (JIT). Board members: Hung Nguyen, David Dykes, Ross Wheatley, Jason Mathews, John McCarroll, Mark Higgins, Wayne Andersen, Robert Butts, 2010.
2. DHSG, Progress Report 2 - Deepwater Horizon Study Group, 2010, 42.
3. Salazar, Increased Safety Measures for Energy Development on the Outer Continental Shelf, in Department of the Interior, 2010.
4. Kjellén, U., Prevention of accidents through experience feedback. 2000, London: Taylor & Francis. XXVI, 424 s.
5. Øien, K., I.B. Utne, and I.A. Herrera, Building Safety indicators: Part 1 - Theoretical foundation. Safety Science, 2011. **49**(2): 148-161.
6. OECD, Guidance on safety performance indicators. Guidance for industry, public authorities and communities for developing SPI programmes related to chemical accident prevention, preparedness and response, 2003.

7. Vinnem, J., Risk indicators for major hazards on offshore installations. Safety Science, 2010. **48**(6): 770-787.
8. PSA. Integrated operation, 2010 [cited 2010 26 August 2010]; Available from: http://www.ptil.no/integrated-operation/category143.html.
9. Close, F., R.D. McCavitt, and B. Smith, Deepwater Gulf of Mexico Development Challenges Overview, in SPE North Africa Technical Conference & Exhibition. 2008, Society of Petroleum Engineers: Marrakech, Morocco.
10. Standards_Norway, NORSOK STANDARD D-10 Well integrity in drilling and well operations, in NORSOK. 2004, Norwegian Technology Centre: Oslo, 162.
11. API, Isolating Potential Flow Zones During Well Construction, in API Recommended practice 65 - Part 2. 2010, American Petroleum Institute.
12. API, Recommended Practice for Well Control Operations - API Recommended Practise 59. 2010, American Petroleum Institute.
13. PSA. Well control and well integrity. 2010 29.01.2008 [cited 2010 26 August 2010]; Available from: http://www.ptil.no/well-integrity/well-control-and-well-integrity-article4156-145.html.
14. Sklet, S., Safety Barriers on Oil and Gas Platforms, in NTNU. 2005, NTNU: Trondheim, 182.
15. Sklet, S., Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries, 2006. **19**(5): 494-506.
16. API, Isolating Potential Flow Zones During Well Construction, in API RECOMMENDED PRACTICE 65—PART 2. 2010, American Petroleum Institute.
17. BP, Deepwater Horizon Accident Investigation Report. 2010, 192.
18. BOEMRE, Fact Sheet - The Drilling Safety Rule - An Interim Final Rule to Enhance Safety Measures for Energy Development on the Outer Continental Shelf, 2010, 2.
19. DNV, Report OLF/NOFO - Summary of differences between offshore drilling regulations in Norway and U.S. Gulf of Mexico, 2010, 100.
20. Vinnem, J.E., et al., Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. Reliability Engineering & Systems Safety, 2006(7): 778-791.
21. PSA. Technical and operational barriers, 2010 [cited 2010 26 August 2010]; Available from: http://www.ptil.no/technical-and-operational-barriers/category616.html.
22. Skogdalen, J.E. and C. Tveiten, Safety perception and comprehension among offshore installation managers on Norwegian offshore petroleum production installations, in The 5th International Conference Workingonsafety.net, 2010: Røros, Norway.
23. Vinnem, J.E., et al., Analysis of root causes of major hazard precursors (hydrocarbon leaks) in the Norwegian offshore petroleum industry. Reliability Engineering & System Safety, 2010, **95**(11): 1142-1153.
24. Hinton, A., An Analysis of OSD's Well Incident Database; Results can Improve Well Design and Target Well Control Training, in Offshore Europe Oil and Gas Exhibition and Conference. 1999, Society of Petroleum Engineers: Aberdeen, United Kingdom.
25. Gao, E., et al., Critical Requirements for Successful Fluid Engineering in HPHT Wells: Modeling Tools, Design Procedures & Bottom Hole Pressure Management in the Field, in European Petroleum Conference. 1998, Society of Petroleum Engineers Inc.: The Hague, Netherlands.
26. AEUB, Field Surveillance April 1998/March 1999 Provincial Summaries, in EUB Statistical Series 57, 2004, 42.
27. Holand, P., Deepwater Kicks and BOP Performance, Unrestricted version. 2001, SINTEF Industrial Management, Safety and Reliability: Trondheim.

28. Nat.Com., A Brief History of Offshore Oil Drilling, N.C.o.t.B.D.H.O.S.a.O. Drilling, Editor. 2010.
29. Standards_Norway, Well integrity in drilling and well operations D-10. 2010, Norwegian Technology Centre: Oslo.
30. Ale, B.J.M., et al., Towards a causal model for air transport safety--an ongoing research project. Safety Science, 2006, **44**(8): 657-673.
31. Vinnem, J.E., Seljelid, J., Haugen, S., Aven, T. , Generalized methodology for operational risk analysis of offshore installations. Journal of Risk and Reliability, 2008, **223**: 11.
32. Dobson, J.D., Kicks in Offshore UK Wells—Where Are They Happening, And Why?, in SPE/IADC Drilling Conference and Exhibition. 2009, British Crown Copyright: Amsterdam, The Netherlands.
33. API, Process Safety Performance Indicators for the Refining and Petrochemical Industries - ANSI/API RECOMMENDED PRACTICE 754, in Downstream Segment. 2010, American Petroleum Institute, 54.
34. Shaughnessy, J.M., L.A. Romo, and R.L. Soza, Problems of Ultra-Deep High-Temperature, High-Pressure Drilling, in SPE Annual Technical Conference and Exhibition. 2003, Society of Petroleum Engineers: Denver, Colorado.
35. Lawrence, D.T., Deepwater production development options in the Gulf of Mexico, in 16th World Petroleum Congress. 2000, World Petroleum Congress: Calgary, Canada.
36. Willson, S., et al. Wellbore Stability Challenges in the Deep Water, Gulf of Mexico: Case History Examples from the Pompano Field. 2003.
37. OilGasGlossery.com. Oil & Gas Field Technical Terms Glossary, 2010. Available from: http://oilgasglossary.com/make-a-trip.html.
38. BOEMRE. Loss of Well Control. Statistics and Summaries 2006-2010. 2010 09/28/2010 [cited 2010 14 October 2010]. Available from: http://www.boemre.gov/incidents/blowouts.htm.
39. API, Specification for Drilling and Well Servicing Structures, in API SPECIFICATION 4F, 2010, American Petroleum Institute.
40. API, Contractor Safety Management for Oil and Gas Drilling and Production Operations, in API RECOMMENDED PRACTICE 76, 2010, American Petroleum Institute.
41. API, Recommended Practices for Blowout Prevention Equipment Systems for Drilling Wells, in API RECOMMENDED PRACTICE 53, 2004, American Petroleum Institute.
42. API, Recommended Practice for Oil and Gas Producing and Gas Processing Plant Operations Involving Hydrogen Sulfide, in API RECOMMENDED PRACTICE 55, 2007, American Petroleum Institute.
43. API, Recommended Practice for Training and Qualification of Personnel in Well Control Equipment and Techniques for Wireline Operations on Offshore Locations, in API RECOMMENDED PRACTICE T-6. 2002, American Petroleum Institute.
44. BOEMRE, Fact Sheet - The Workplace Safety Rule - On Safety and Environmental Management Systems (SEMS). 2010, 2.
45. Stupak, B. and H.A. Waxman, Dear Mr. Hayward: We are looking forward to your testimony before the Subcommittee on Oversight and Investigations on Thursday, June 17,2010, about the causes of the blowout ofthe Macondo well and the ongoing oil spill disaster in the Gulf of Mexico., M.T. Hayward, Editor. 2010, Congress of the United States, House of Representatives, Committee on Energy and Commerce: London, 4.
46. Schlumberger. Cost cement bond-log. 2010 21 October 2010]; Available from: http://energycommerce.house.gov/documents/20100614/Schlumberger-Cost.of.Completing.Cement.Bond.Log.v.Canceled.Contingency.pdf.

47. Thomassen, O. and M. Sørum. Mapping and monitoring the safety level. in Sixth International Conference on Health, Safety and Environment. 2002. Kuala Lumpur: Society of Petroleum Engineers.
48. Vinnem, J.E., et al. Operational Safety Condition - Concept Development. in Esrel, 2007, Stavanger.
49. PSA, PSA Investigation report gas leak 19 January 2006 Visund 2006, Petroleum Safety Authority Norway: Stavanger, 29.
50. Pitblado, R. and R. Tahilramani, Barrier Diagrams the Next Stage for Enhancing Offshore Operations Safety, 2010.
51. Sklet, S., et al., Monitoring of Human and Organizational Factors Influencing the Risk of Major Accidents, in SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production S.o.P. Engineers, Editor. 2010, Society of Petroleum Engineers: Rio de Janeiro, Brazil.
52. Kallaur, C.U., A Performance-Based Approach to Offshore Regulation, in SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production. 1998, Society of Petroleum Engineers Inc.: Caracas, Venezuela.
53. Boykin, G.F., A Global Drilling Organization: The Role of the Drilling Professional, in IADC/SPE Drilling Conference. 1998, IADC/SPE Drilling Conference: Dallas, Texas.
54. Korsvold, T., et al., Creating Resilient Drilling Operations through Collective Learning, in Asia Pacific Health, Safety, Security and Environment Conference, 2009, Society of Petroleum Engineers: Jakarta, Indonesia.
55. Hubbard, D., The failure of risk management: why it's broken and how to fix it, 2009: Wiley.
56. Addison, F., K. Kennelley, and F. Botros, Future Challenges for Deepwater Developments. 2010: Offshore Technology Conference held in Houston, Texas, USA, May 3–6, 2010.

Appendix I

Highly Reliable Governance Of Complex Socio-Technical Systems

W.E. Carnes

The Deepwater Horizon catastrophe is but the most recent and strident note in an oft repeated clarion call for new forms of governance. While a coherent story of what happened and why it happened is at least months, and perhaps years, from now, there are clear signals all too reminiscent of previous disasters warning us that mere band-aids and promises will not be sufficient to avoid future techno-centered horrors.

From what has been reported, there will be a wealth of technical lessons to be learned from this accident—what may be referred to as first order learning. As the Deepwater Horizon history unfolds, it seems that there are ample examples of second-order learning of human and organizational error and more trenchant examples of unprofessional conduct and malfeasance. But the larger story, the more insidious and intractable story, is that of a model of governance that is more suited to the industrial revolution than the long-forecasted and quickly emerging knowledge age.

The purpose of this paper is not to cast blame; rather to offer a perspective on the governance approach that allows Deepwater and kindred accidents such as Three Mile Island, Columbia, and Texas City to pose as singular examples of technical and corporate failure rather than as dying gasps of a governance model no longer suited for the techno-centric world we have created.

This paper is a pastiche informed by scientific research and centered in practice. Its purpose is not to define, but rather to provoke reflection and discussion. Its intended central argument is that theory-driven models, risk informed and performance based, are needed to explicate a new paradigm of highly reliable governance for complex, hazardous socio-technical systems.

The paper is presented around four thematic areas, the goals of which are to:

- Discuss the growing emphasis on the need for new models of governance for techno-centric societies where technical hazards have potential for major social harm;
- Place government regulation in the context of broader multi-agent governance models;
- Use U.S. commercial nuclear power as an example of such a multiagency socio-technical system model; and
- Identify steps forward for establishing such a model for the United States that can address the petrochemical industry and also serve as an impetus for cross-cutting efforts for emerging high-hazard technologies such as nano-technology and bio-engineering.

Acronyms

Acronym	Definition
CSB	Chemical Safety Board
EPIX	Equipment Performance and Information Exchange
EPRI	Electrical Power Research Institute
HPI	Human Performance Improvement
HRO	High Reliability Organization
INPO	Institute of Nuclear Power Operations
INSAG	International Nuclear Safety Group
NEI	Nuclear Energy Institute
NEIL	Nuclear Electric Insurance Limited
NRC	Nuclear Regulatory Commission
OSHA	Occupational Safety and Health Act
PPA	Procedures Professional Association
PRA	Probabilistic Risk Assessment

1.0 Introduction

The history of safety science is a story of searching for risk mitigation and prevention of harm. Some trace the beginning of safety regulatory attempts to the Code of Hammurabi circa mid-1700s B.C. The start of safety regulation attempts in the United States is attributed by some to the Massachusetts Factory Act of 1877. However, the New York City Triangle Shirtwaist Factory Fire of March 21, 1911, in which nearly 150 women and young girls died because of locked fire exits and inadequate fire extinguishing systems, was a turning point. This fire prompted enactment of laws and regulations instituted by the government to protect workers. Even then, it was not until 1970 that then-President Richard Nixon signed into law the Occupational Safety and Health Act (OSHA), which gave the Federal Government the authority to set and enforce safety and health standards for most of the country's workers. It was also in 1970 that the Environmental Protection Agency was established as the first independent agency to protect human health and safeguard the natural environment. History will also record that as momentous as the year 1970 was in protecting the safety of workers, the public, and the environment, the prescriptive safety science theories of prevention—the intellectual underpinnings of the new safety regimes—were already being eroded by our successes in science and technology. For in the preceding year, 1969, construction began on the Three Mile Island Nuclear Generating Station, Unit 2.

Technology has been a primary driver for the improvement of social conditions since the beginning of the industrial revolution. Modern technologies represent the intersection of science, industry, finance, government, and global politics engaged in a delicate dance to serve social needs, corporate interests, and national interests. Technology is not static; its dynamic nature is the result of instantaneous communication, unceasing research and development, and the promise of technological solutions to address social inequities. Regrettably progress in safety practice has, in the main, lagged behind progress in technology and safety science.

Reiman and Oedewald summarize the history of safety science this way:

> …organizational theory and safety science have progressed in their over-one-hundred year's history. The knowledge of what is safety and how it is achieved has also developed. The safety measures taken in high-hazard organizations a couple of decades ago are not sufficient today. The focus of the safety work has changed from component-based risk control to organizational resilience and safety. Today's organizations need to systematically ensure the reliability of the components on the one hand, and, on the other hand, understand the emergent nature of safety. Designing both safety perspectives in organizational structures and processes is demanding. Usually, outside influences are needed in order to get the new views into organizations.[1]

Complexity and dynamism of technology-involved issues have stimulated global research efforts on what is termed "risk governance." As discussed by the International Risk Governance Council, the notion of risk governance "builds on the observation that collective decisions about risks are the outcome of a 'mosaic' of interactions between governmental or administrative actors, science communities, corporate actors and actors from civil society at large, many of the interactions taking place and relevant to only individual parts of the overall process. The interplay of these actors has various dimensions, including public participation, stakeholder involvement, and the formal (horizontal and vertical) structures within which it occurs." Risk governance "includes both intellectual and material 'assets', 'skills' and as well as the framework of relations, or 'capabilities', required to make use of the former two." [2]

In many ways in the 1960s and 1970s, nuclear power represented the shining promise of all that was good about science and technology. In a 1954 speech to National Association of Science Writers, Lewis Strauss, then Chairman of the United States Atomic Energy Commission, uttered the phrase that now exemplifies failure of utopian promises of technology:

> Our children will enjoy in their homes electrical energy *too cheap to meter*. It is not too much to expect that our children will know of great periodic regional famines in the world only as matters of history, will travel effortlessly over the seas and under them and through the air with a minimum of danger and at great speeds, and will experience a lifespan far longer than ours, as disease yields and man comes to understand what causes him to age.

The 1979 accident at Three Mile Island, Unit 2, shattered our technological naiveté. In our enthrallment with future possibilities, the future in many ways seemed to rest in the hands of the scientists and engineers. Their ability to envision, develop, and design seemed limited only by time and resources. Yet that which can be designed must be capable of being operated. For that one needs organizations and people—the human element. And humans negotiate, compromise, balance competing priorities, and make mistakes. The investigations of the Three Mile Island accident reminded us of the human element, that we were no longer dealing with simple technologies for

[1] Reiman, T. and Oedewald, P. Evaluating Safety-Critical Organizations – Emphasis on the Nuclear Industry. Finland: VTT, 2009.

[2] Ortwin, Renn. Risk Governance: Towards and Integrative Approach. Geneva: International Risk Governance Council, 2006.

which protection could be prescribed, rather we were now dealing with complex socio-technical systems that functioned in new and ill-understood ways.

As with nuclear power, petrochemicals, aviation, electrical distribution, and medicine are examples of complex techno-social systems. Each accomplishes its socially productive missions through the application of technologies that if mishandled could result in catastrophe. Because of the complexity of the technologies, each requires the skills and knowledge of many scientific, technical, and management disciplines. Each exists within a web of regulators, customers, industrial suppliers and stakeholders. Regulation is necessary to protect society from the potential harm of improper operation and management, but alone it is not sufficient. Experience and research since the 1980s have demonstrated that complex socio-technical systems require complex adaptive governance models, engaging multiple agents to promote socially beneficial use of hazardous technologies. A framework for understanding these organizations has been developed: the framework of High Reliability Organizations.

2.0 The Need For A New Model: From Human Error To Complex Adaptive Systems

The Chemical Safety Board (CSB) report on the BP Texas City accident in 2005 commented on the BP safety model, stating that it was focused on a "worker safety model" versus a "process safety model." The distinction raised by the CSB is one raised by other accident investigations and safety researchers; the historical practices and programs designed to protect worker safety are necessary but not sufficient to prevent large-scale accidents. The language used may be that of "person models versus system models" or the "old view versus the new view."

To engage in a discussion of governance of complex adaptive systems a full understanding of the difference between a person model and a systems model is essential. The exclusive focus on the person model is rooted in ideas about human error as cause of accidents relieving the need for further examination and investigation. Thus, discussion of what safety science tells us about the fallacy of human error is a necessary first step.

Error, mistake, faux pas, gaffe, blunder, lapse, slip, goof, oops, blooper. How many phrases do we have to express the idea that things don't always happen as we expect or as we would prefer? At the 2009 CEO Conference of the Institute of Nuclear Power Operations (INPO), one CEO stated that the most important change in the commercial nuclear industry in the past decade was the recognition that people do not intentionally commit errors. INPO's training reference guide that introduced the commercial nuclear power industry's Human Performance Improvement (HPI) initiative stated that HPI represented "a new way of thinking." So the question is, how might we think differently about this concept of error that seems to be an inevitable aspect of the human condition?

The "fact" that some 80 percent of accidents are "caused" by human error appears in much of the safety literature. Formal accident investigation attributions of error as cause have been used for justification of blame and punishment, ostensibly to "prevent" recurrence of similar accidents. Yet after decades of labeling human error as cause, what do we really know scientifically about error as a fundamental human concept?

Much of the scientific work on accident causation can be traced to the aftermath of the Three Mile Island accident. Woods and Cook explain the situation as: "At that time, the folk model of accident causation was firmly in place among researchers and error seemed a plausible target for work on safety. It was only after a long period of empirical research on human performance and accidents that it became apparent that answering the question of what is error was neither the first step nor a useful step, but only a dead end." [3]

As James Reason explains in his book *Human Error,*[4] error means different things to different people and depends on context. In Latin the meaning of error is "to wander." In baseball an error is the act, in the judgment of the official scorer, of a fielder misplaying a ball in a manner that allows a batter or base runner to reach one or more additional bases when such an advance should have been prevented given ordinary effort by the fielder. In computer operation, an error is when an unexpected condition occurs.

The utility of error as causation is further complicated since error cannot be isolated as a particular psychological or behavioral phenomenon. Addressing efforts by cognitive psychologists to identify error types, Reason states that "Far from being rooted in irrational or maladaptive tendencies, these … error forms have their origin in fundamentally useful psychological processes." He continues, quoting Ernest Mach (1905), "knowledge and error flow from the same mental sources, only success can tell one from the other."

So it seems that what may be called error is distinguishable only retrospectively in the presence of an undesirable outcome. Absent such an outcome, error is not observable. So, if error is not observable sans outcome, is there any utility to this concept which is so rooted in the cultural views of causality yet so lacking in scientific validity?

Returning to Woods and Cook, "Error is not a fixed category of scientific analysis. It is not an objective, stable state of the world. Instead, it arises from the interaction between the world and the people who create, run, and benefit (or suffer) from human systems for human purposes—a relationship between hazards in the world and our knowledge, our perceptions, and even our dread of the potential paths toward and forms of failure.…To use 'error' as a synonym for harm gives the appearance of progress where there is none."

If the concept of error has no particular value in analysis of failure, and indeed, that such use may be counterproductive, perhaps its value lies elsewhere. Viewing error as a fuzzy concept, rather than an absolute concept, provides a basis for proceeding. William James' philosophy of pragmatism relates meaning to a concept's purpose. Operationalization is the process of defining a fuzzy concept so as to make the concept measurable in the form of variables consisting of specific observations. W. Edwards Deming explains that "An operational definition is a procedure agreed upon for translation of a concept into measurement of some kind."

How might we understand error in a purposeful sense that promotes the human condition; that is, how might the concept be operationalized? Consider, as an example, physical pain. Pain may be

[3] Woods, D.D. and Cook, R.I. "Mistaking Error," in The Patient Safety Handbook, Youngberg, B. J. and Hatlie, M..J., Sudbury, Chapter 7. Jones and Bartlett Publishers, 2004.
[4] Reason, J.T. Human Error. Cambridge: Cambridge University Press, 1990.

understood as a negative consequence; something to be avoided or even feared. Alternatively, pain may be understood as one of the body's key defense mechanisms, the purpose of which is to alert us of a threat to the body's safety or survival. Similarly we may shift the meaning of error as harm, to error as warning of harm. Thus error becomes a signal to prompt protective actions.

Reason offers three related "working" definitions of error, each predicated on a retrospective judgment of not achieving the desired outcome from pursuing a predetermined course of action. He then suggests that error be understood in terms of intentions, actions, and consequences. He also suggests that error be extended from purely an individual phenomenon to include organizational phenomena. So, if we understand error as a signal operating with intentions, actions, and consequences, we can view this formulation equivalent to Deming's description of the Shewhart Cycle of "Plan, Do, Study, Act." In this way, errors become signals that enable individuals and organizations to monitor the relationship of the doing of the plan in relationship to anticipated outcomes and then adjusting the plan and actions based on the feedback provided by error.

Error is life providing feedback on our interactions with the environment. By shifting the paradigm of error from one of "error as cause" to "error as system feedback", we find that error is nature's way of helping us proceed incrementally toward our goals while coping with an uncertain universe. Such a shift also serves to create a culture in which blame and recrimination are no longer the reflexive reaction, in which fear is replaced by the nurturing and development of human potential, in which human collaboration is the capital for innovation, and in which adaptation and continuous improvement become intrinsic value driven core competencies of individuals and organizations.

3.0 Governance And Complex Adaptive Systems

Those born to the World War II generation have seen a transition from a predominately rural, agrarian world, have lived through the industrial era, and are now part of the rapidly emerging knowledge era. The development of systems engineering and operations research that facilitated mobilization of the U.S. industrial machine to fuel the defense demands of the 1940s heralded the blending of technical and social science knowledge, which, in turn, gave rise to multidiscipline research and development. It was also the necessities of wartime and the post-war era that gave rise to the idea of socio-technical systems and the concepts of statistical process control and quality management.

The expansion of education, capital, and industrial capacity, along with government sponsorship of public and private research, produced technologies and organizations of a complexity never before witnessed. Beginning in the 1980s there were faint signals that the forms of government and management that had accompanied advancement since the early 1900s were becoming increasingly unsuited for the challenges of how to productively and safely control the technologies of which we were capable.

The publication by Thomas Kuhn of the *Structure of Scientific Revolutions* in 1962 introduced the concepts of paradigms and paradigmatic shifts in science. In summary Kuhn argues that over time prevailing scientific theories lose predictive value as anomalies are identified for which the theories have no explanation. Certain bold researchers begin a search for alternative explanations and, after

continued research, better explanations for the hitherto unexplainable phenomena are developed, thus ushering in a new paradigm.

The 1980s marked such a period of beginning a paradigmatic shift. It was then that the previous view of a mechanistic, linear, so called deterministic universe came under challenge. The discovery of quantum mechanics in physics may be argued as the start of the unraveling of the mechanistic model. In 1984 the Santa Fe Institute was established by a group of physicists to study the concept of complexity. The goal of the Institute was to promote trans-disciplinary research on complex systems. The Institute gave focus to researchers from physics, biology, and chemistry, and their collaboration shifted the intellectual model from the idea of a universe governed by deterministic laws of linear cause and effect to a universe where multiple components (called agents) interact and connect in unplanned and unpredictable ways. From beginnings in the physical sciences, the discoveries in complexity were extended to the social sciences, and today permeate the research on human organizational systems.

As stated in the history of the Institute, "The discovery of common, fundamental principles in complex adaptive systems as varied as global climate, financial markets, ecosystems, the immune system, and human culture requires an inclusive, broad perspective, one that comprehends the components of a system but views those elements as actors in a large, interconnected, often unpredictable world."

It should be of little surprise that the ideas of governance as a multi-agent mode of promoting the social good and the idea of high reliability organizations both emerged in the 1980s. Stimulated by findings of investigations of the Three Mile Island accident and confronted by the specter of future "normal accidents," researchers began to explore how some organizations, so called High Reliability Organizations, were able to create success while operating hazardous technologies within dynamic environments. What they found resonated with earlier work by Trist and Emery that led them to speak about socio-technical systems as the interface between society and complex technology.

In a similar sense the concept of governance as a complex adaptive systems approach arose from a growing recognition that the directive command and control concept of central government had become ill-suited and realistically impractical in democratic societies. The very nature of democratic systems combined with growing population size, the democratization of education, and the diversification of society cried out for better explanations of how people could work together to promote social good.

4.0 Government And Governance

The shift from the concept of Government to Governance has been discussed in a variety of scholarly papers and publications. Kemp, Parto and Gibson[5] express the general thinking. Governance as a concept became:

[5] Kemp, R., Parto, S. and Gibson, R.B. "Governance for sustainable development: moving from theory to practice." Int. J. Sustainable Development, Vol. 8, Nos. 1/2, (2005): 12–30.

> …attractive because it encompassed a broad set of factors that were increasingly important and insufficiently recognised in conventional thinking and because it encouraged a more integrated understanding of how these factors were, or should be, linked. Governance scholars viewed the political system as a complex of formal and informal arrangements that were ill-defined and unstable. This was in direct contrast to the conventional view of governments as formal, clearly identifiable, and static entities. Whereas government conjured up an image of formal structures ruling over people, the notion of governance highlighted the increasingly important role of formal and informal arrangements in the political economy.
>
> *Governance*, understood as a mode of social coordination, is different from *governing;* which is an act, a purposeful effort to steer, guide, control and manage (sectors or facets of) society….It involves the level and scope of political allocation, the dominant orientation of state, and other institutions and their interactions. Governance structures organise negotiation processes, determine objectives, influence motivations, set standards, perform allocation functions, monitor compliance, impose penalties, initiate and/or reduce conflict, and resolve disputes among actors....The effective exercise of power is through a network of interconnected actors, in which all actors hold power through knowledge, resources, money and rights granted to them.
>
> The notion of governance fits in with complex systems approaches to understanding the workings of the political economy through the inter-relationships among identifiable parts (e.g., social, economic, and ecological), rather than just the parts themselves. A complex systems approach to governance also implies explicit appreciation of complexity and uncertainty, likelihood of surprise, and need for flexibility and adaptive capacity.

Cherry suggests that "a complexity theory perspective is instrumental for understanding that government must increase regulatory resilience…government must create regulatory structures and policies of increased adaptability to the complexity and increasing pace of technological innovation and ensuing economic and social changes...problems revealed under deregulatory policies are symptomatic of a deeper, more fundamental set of sustainability problems arising from a historical process of accelerated technological and social change." [6]

Priscilla Rabb Ayres argues that the industrial age approach to regulation is out of step in the information age and offers the following observations of the predominant historical regulatory approach:[7]

- Traditional regulatory regimes are characterized by static focus
  - Highly prescriptive and rules-based
  - Compliance is siloed and risks stand alone

[6] Cherry, B.A. "Institutional Governance for Essential Industries under Complexity: Providing Resilience within the Rule of Law." CommLaw Conspectus 17 (2008-2009).

[7] Ayres, P. "Regulation in the 21st Century: From Prescription to Collaborative Supervision" (Paper presented at the 10th XBRL International Conference, Brussels, Belgium, November 16, 2004).

    - Compliance functions typically low level and dispersed throughout organizations
- Regulation viewed as exclusively the concern of the government
- Focus on discrete violations and correction of those violations
- Shortcomings for application in the 21st century
    - Inflexible and unable to keep up with rapid change
    - May not capture risk appropriately
    - Dependencies not adequately assessed
    - Can encourage "gaming the system" (e.g., Enron)
    - Highly labor intensive and slow

The Winter 2006 Issue of *Public Affairs Review* of the University of Central Florida contained an article synthesizing the literature on government and governance. The article concluded with the following observations:

> The government concept is historical and its work is recognized as the direction and distribution of public goods and services. Government is viewed as an institution. While a wealth of service delivery models may be utilized, direct service remains as a fundamental component of government activities. The government retains its status of principal actor, either through direct service or through the indirect management of contracts that are programmatically defined. Ultimately, government is a term that is not keeping pace with the changing work, structure, and culture of today's complex governance issues in a global arena.
>
> On the other hand, governance is contemporary, it suggests an interactive approach to problem solving using a variety of tools and models within a network of partnerships and envisions the role of government as a facilitator-power broker within not only a regional, but global perspective. A new era of public problem solving has occurred in the United States as well as many other parts of the world. Rather than relying solely on the government to solve public problems, a multitude of third parties have been employed to not only participate, but to lead such activities. Governance represents a new public administration perspective, which harnesses the strengths and opportunities created by engaging stakeholders across boundaries into productive networks. Reorganizing concepts of government to governance is not enough to solve public issues, but multiple approaches involving a wide array of tools is necessary for addressing public problems.[8]

5.0 A Framework For Governance Of Hazardous Technologies

In many ways the investigations into the Three Mile Island accident and the response to that accident changed the way we think about potentially high-consequence accident causation. Likewise, the response by government and industry to this accident established a new model for governance of hazardous complex socio-technical systems. Over the past 30-some years research by scholars of governance and scholars of high reliability has begun to converge though the lens of

[8] Knepper, H., Sitren, A., and Smith, H. "An Examination and Synthesis of Two Public Administration Concepts and their Relevance for Public Administration Students." Public Affairs Review: e-Journal of the Doctoral Program in Public Affairs Winter (2006).

complex adaptive systems to suggest a framework for governance of complex hazardous technologies; that of Highly Reliable Governance.

In the late 1980s, a group of researchers at the University of California Berkeley began research on organizations that were known to perform their missions with consistently high quality while operating complex technologies and operating within dynamic environments. They were soon joined by researchers from the University of Michigan and their research on U.S. Navy Aircraft carriers, the Federal Aviation Administration Air Traffic Control System, and U.S. commercial nuclear power plants gave rise to what is now known as High Reliability Organization (HRO) theory. While the organizations differed in their technologies, organizational forms, and regulatory regimes, they shared certain characteristics that differed from other organizations the researchers had studied. Much has been written about such highly reliable organizations since the early foray of inquiries, and today the application of HRO concepts spans an increasing body of organizational types, as well as a diversity of scientific and technical disciplines. As examples Roberts' research on incident command systems, Roe and Schulman's[9] 7-year longitudinal study of a large electrical distribution system, and the implementation initiatives of the wildland fire community have illuminated the relevance of high reliability concepts to dynamic domains.

In broad strokes, these HROs begin with deep knowledge of the technologies they employ. This is coupled with flexible organizational design where roles and responsibilities are clearly established and understood, yet they are bound together with extensive social communication networks; respect for diverse expertise; a healthy skepticism for what they do not know; unending inquisitiveness; a culture which values collaborative problem-solving; and an abiding respect for the hazards they manage, being ever mindful of the potential consequences of less than excellent performance. These organizations have internalized—through systems, processes, culture, and education—the essence of complex adaptive systems. Research into these organizations has produced a body of theory, which, when converted into models, has utility for guiding organizational change.

Human beings have a desire to impose order over chaos. It has been suggested that the designation Homo Sapiens would be better described as Homo Poetica—man the meaning maker. The Public Affairs Review authors observed that "Reorganizing concepts of government to governance is not enough to solve public issues, but multiple approaches involving a wide array of tools is necessary for addressing public problems." While high reliability organizations make use of tools such as quality improvement and human performance tools, the chief value of HRO theory is not in the tools themselves but rather in the intellectual framework the theory provides.

The psychological construction a framework has been described as the identification and categorization of processes or steps that constitute a complex task or mindset in order to render explicit the tacit and implicit. The original HRO researchers observed what their focus organizations did—how they acted. This activity-focused conceptualization was expanded in the Roberts and Weick article in *Administrative Science Quarterly*, September 1993, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks." This article introduced the cognitive aspects of HROs.

[9] Roe, E., and Schulman, P. High Reliability Management: Operating on the Edge. Stanford: Stanford Business Books, 2008.

A review of HRO theory by Andrew Hopkins suggests how the original definition by the Berkeley researchers "evolved" through the Weick and Sutcliffe work to shift from a functional conceptualization of an HRO to more of a cognitive conceptualization. James Reason speaks of HROs as resilient organizations that combine performance enhancing techniques to perform technical activities with a particular type of cognition. Resilient organizations are not bound by rigid adherence to preconceived ways of working, rather they are guided by a mental framework of "what good looks like" and are thus able to recognize indications that things are not going right and adapt to the unexpected. How HROs manage the unexpected was elaborated upon by Weick and Sutcliffe in their two books that advanced that theme. Weick's explanation of the value of frameworks is that "When people put stimuli into frameworks this enables them to comprehend, understand, explain, attribute, extrapolate, and predict."

The need for a framework by which people make sense of what they do and what is going on has been long discussed. Peter Drucker consistently challenged his clients and audience to define and refine their theory of business. His four key points were as follows:

- What assumptions are we making about: (1) the environment, (2) our mission, and (3) the core competencies that we need?
- Do the assumptions in all three areas fit each other?
- Is the theory of the business known and understood by everybody?
- Is the theory tested constantly—and altered if necessary?

Deming's famous 14 points constituted a framework for thinking about quality. He spoke of his points in terms of theory. According to Deming, having a theory is essential: "Experience by itself teaches nothing....Without theory, experience has no meaning. Without theory, one has no questions to ask. Hence without theory there is no learning." His teaching about theory echoes the oft repeated quote of Kurt Lewin: "There nothing as practical as a good theory."

John Carroll poses the question, "Why should effective behaviors and activities not be explicable and perhaps not discussible?" He concludes that the difficulty lies in the available "mental models" or understandings of organizations, people, and technologies. "When those mental models legitimate only certain types of behaviors, and exclude whole classes of effective behaviors, then there is need to broaden the models. When different knowledge bases and viewpoints cannot be negotiated across levels of hierarchy and occupational specialties, then organizations cannot make sense of events in ways that support effective learning." [10]

Over the past several years High Reliability Organization theory has been examined in validity and utility in variety of hazardous domains. A prominent example is the adoption of the high reliability framework for improvement of health care quality and safety. This continuing research and application has been described by Karlene Roberts in her essay to celebrate the publication of the second version of Weick and Sutcliffe's book on Managing the Unexpected. Inherent in her essay is a subtle clue to the vitality of the theory as a framework. It is robust enough to transcend diverse technical domains, yet flexible enough to accommodate new discoveries of how organizations can adapt.

[10] Carroll, J.S. "Organizational Learning Activities in High Hazard Industries: The Logics Underlying Self-Analysis." Journal of Management Studies 35(6), November 1998: 699-717.

The HRO framework has been used for reflective learning in a wide range of technical domains, from the nuclear defense work of the Department of Energy's Pantex plant to wildland fire fighting, education, and medicine. These HRO learning applications were undertaken to enhance safety and performance in operating environments. Research on governance and the recent emphasis on risk governance are in resonance with high reliability theory. The interfaces of these research fields suggest an emerging new framework for governance of complex hazardous technological endeavors. Embarking upon a framework of Highly Reliable Governance, however, is perhaps best undertaken being mindful of the observation of Thomas Kuhn: "The success of a paradigm is at the start largely a promise of success discoverable in selected and still incomplete examples."

6.0 The U.S. Nuclear Power Industry: A Case Study In Highly Reliable Governance

As notable as HROs are as individual exemplars, they do not exist in isolation and have not been the products of forward engineered design. Rather they are the result of multiple agents interacting over time to evolve unique organizational forms. A particular type of governance has been shaped over time that allows HROs to exist and flourish through their carefully crafted capacity for resilience.

When exposed to discussions of the U.S. commercial nuclear industry as an exemplar of high reliability, an often heard retort is "We're not a nuclear reactor." This superficial judgment based on technical systems belies a lack of awareness of the deep cognitive structures of organizations. Some, however, have recognized that at these deeper levels an analogy is present. Recently the President's Commission invited testimony from the current CEO of INPO and one of INPO's earlier CEOs. Others have also noted the value of considering the nuclear experience. One is former U.S. Secretary of the Interior, Bruce Babbitt, who served on the President's Commission on the Accident at Three Mile Island in 1979.

In July of this year, Babbitt offered his perspectives on what should be learned from the nuclear power analogy:

> The NRC [Nuclear Regulatory Commission], an independent body charged with oversight of all nuclear power plants, is perhaps the best starting point. In a nuclear plant, for example, all operating personnel hold licenses issued by the Commission, all contractors and suppliers must be certified, and the Commission conducts regular and rigorous inspections, aided by NRC personnel who are permanently stationed at each plant.
>
> Many of these regulatory procedures developed from reforms implemented after the near meltdown at Three Mile Island more than 30 years ago. Since then, the industry has compiled an admirable safety record.
>
> Regulation is, of course, not cost free. But as we are learning from the current Gulf disaster, good regulation is a lot less costly than the damage caused by shoddy practices

> enabled by inadequate regulatory oversight. And there is no reason why the costs of effective regulation should be borne by taxpayers.
>
> The oil and gas industry, which continues to report record earnings, can and should bear the costs of regulation. That is how it works in the nuclear industry; Congress requires the industry to reimburse the NRC for its continuing costs.[11]

This section describes U.S. nuclear industry governance. It discusses the regulator and the regulatory approach and reviews how the nuclear industry organizes itself via three main industry groups, with particular attention on INPO. The description is necessarily broad as it is not possible to represent the depth or detail of some 30 years of learning and improving. It is, however, this learning and improving that is most notable about the nuclear industry and how it has evolved into its present form. Learning and improvement are inextricably embedded within the structures and activities of the regulator, the industry support groups, and each nuclear operating organization. So a brief overview of nuclear organizational learning approaches is offered for context.

Nuclear Organizational Learning

One hallmark of High Reliability Organizations is that they have deep understanding of the knowledge and skills necessary to perform work safely. They seek to craft the appropriate blend of skill, knowledge, and procedures in consideration of work complexity and hazards. And they seek to capture the tacit knowledge of experts by converting this tacit knowledge to explicit forms, either in equipment, training, and procedures or in other performance support tools. Also they seek to keep the requisite knowledge current by robust change control and employee reporting systems to identify changes needed and to evaluate the implication of changes in technology, plant configuration, equipment aging, and employee capabilities as the workforce ages and new workers enter the organization.

Nuclear organizational learning is complex socio-technical systems thinking in action. Training and education are the foundation upon which organizational and industry learning are constructed. Education, knowledge, and skills requirements are established for all nuclear jobs; personnel are trained and qualified before being allowed to perform at the entry supervised level; and a nuclear career is one of ongoing training and development. In the United States this is true for regulators as well as the operating organizations. For example, it is not possible to achieve operational senior management levels in a nuclear organization without qualifying as a Senior Nuclear Plant Operator.

Technical competency is only the base requirement. Beginning with front-line supervisors and continuing to the levels of CEO and Boards of Director members, nuclear professionals are groomed in leadership and management skills, with heavy emphasis on safety culture and risk-conservative decision-making as well as performance analysis and improvement theory and techniques. Knowledge and skills in performance improvement and risk-informed decision-making are embedded in the job training of all personnel.

Operating organization and industry learning are facilitated through sharing of operating experience, nested systems of performance indicators, and organizational evaluation. Operating experience is collected and analyzed by both the NRC and INPO. The NRC's Licensee Event Reporting system has threshold reporting requirements through which operating plants are required

[11] Babbit, B., "Offshore Oil Needs Greater Regulation." Politico Blog, August 2, 2010. http://www.politico.com.

to report on certain events. The INPO operating experience program uses this input, along with a number of other types of information sources of operating experience that are obtained through agreements among INPO, U.S. nuclear plants, the international nuclear industry, and regulatory organizations. INPO typically receives 2,500 to 3,500 event documents each year that are screened for analysis. Analysis programs identify and communicate lessons learned from plant events, collect and trend various industry data, and communicate analytical results.

Both the NRC and INPO maintain nuclear plant data collection systems with the objective of providing reliability data for safety-related and selected other important nuclear plant systems and components. The NRC system is the Reliability and Availability Data System, and the related INPO system is called the Equipment Performance and Information Exchange System (EPIX).

These industry-wide reporting systems support examining for trends of potential industry significance. Each U.S. nuclear plant has extensive internal issue identification and reporting systems. These are designed to capture items that fall far below the regulatory required thresholds. For a well performing plant, from 9,000 to 11,000 items may be generated by plant personnel each year. These are striving to capture events or conditions that might portend a degrading state or practice.

Performance monitoring is also a combined plant-specific and industry-wide learning approach. For an individual plant, identification of indicators and trends begins with individual workers during their daily activities. These indicators roll up to work process levels, department levels (e.g., maintenance or engineering) and overall plant levels. INPO then processes the data further to produce industry-wide trends that serve to drive multi-year improvement initiatives.

Teemu Reiman and Elina Pietikäinen have conducted research on the evolving theory and application of safety indicators in nuclear power. "The role of the safety performance indicators is to provide information on safety, motivate people to work on safety, and contribute to change towards increased safety."

> Safety indicators are tools for effective safety management process. Safety management needs a continuous focus on lagging indicators of past deficiencies, leading indicators of current technical, organizational and human conditions and leading indicators of technical, organizational and human processes that drive safety forward. Drive indicators are chosen priority areas of organizational safety activity. hey are based on the underlying safety model and potential safety activities and safety policy derived from it. Drive indicators influence control measures that manage the socio-technical system; change, maintain, reinforce, or reduce something. Monitor indicators provide a view on the dynamics of the system in question; the activities taking place, abilities, skills and motivation of the personnel, routines and practices—the organizational potential for safety. They also monitor the efficacy of the control measures that are used to manage the socio-technical system. Typically the safety performance indicators that are used are lagging (feedback) indicators. Besides feedback indicators, organizations should also acknowledge the important role of monitor and drive indicators in managing safety.

> When selecting the indicators it is important first to consider what needs to be monitored, what are the critical goals of the organization (i.e., the core task that needs to be taken care of). PRA should also be utilised in identifying the most safety significant issues to monitor. The selection and use of safety performance indicators is always based on an understanding (a model) of the socio-technical system and safety. The safety model defines what risks are perceived. It is important that the safety performance indicators can help in reflecting on this model.[12]

Safety evaluation is the final nuclear learning approach for discussion. It is this element that is INPO's particular "stock-in-trade." Research on nuclear industry organizational evaluation by Reiman and Oedewald summarizes key aspects.

> A safety-critical organization can be defined as any organization that has to deal with or control such hazards that can cause significant harm to the environment, public or personnel...Control of risk and management of safety is one of their primary goals. They are expected to function reliably and to anticipate the operating risks caused by either the technology itself or the organizational structures and practices. The ability of the organization to monitor its current state, anticipate possible deviations, react to expected or unexpected perturbations, and learn from weak signals and past incidents is critical for success. Organizational evaluation is one way of reflecting on this ability.
>
> …the aim of organizational evaluation should be to promote increased understanding of the socio-technical system. This means a better understanding of the vulnerabilities of the organization and the ways it can fail, as well as ways by which the organization is creating safety. Organizational evaluation contributes to organizational development and management.
>
> …the term organizational evaluation denote(s) the use of conceptual models and applied research methods to assess an organization's current state and discover ways to solve problems, meet challenges, or enhance performance.
>
> These approaches all share an idea of organization as a system, the functioning of which can be evaluated against some criteria. Organizational diagnosis emphasizes the idea of problem identification and solving, whereas organizational evaluation as we define it does not need to start with a problem, or end in concrete solutions. The production of information on the functioning and the current vulnerabilities of the organization is the primary goal of organizational evaluation.[13]

[12] Reiman, T. and Pietikäinen, E. Indicators of Safety Culture – Selection and Utilization of Leading Safety Performance Indicators. Finland: VTT, 2010.

[13] Reiman, T. and Oedewald, P. Evaluating Safety-Critical Organizations – Emphasis on the Nuclear Industry. Finland: VTT, 2009.

Note the recurring references to models. The regulator and the industry use a variety of models to understand, guide, and inform. INPO's guidance document "Leadership in Performance Improvement" defines the goal state of performance improvement as:

- The picture of excellence is well known.
- Problems are prevented and mistakes are avoided.
- Performance gaps are thoroughly analyzed and efficiently solved.
- Performance improvement is ingrained as a core business practice.

Models help define the picture of what "good looks like." For analysis as an example, INPO developed an Anatomy of Event model. The model, influenced by the Human Performance model of Gerry Rummler, is used throughout the industry to promote common terminology and a systems approach to help understand and diagnose events.

The Nuclear Energy Institute (NEI) coordinated the industry effort to develop a Standard Nuclear Process Model that defines processes, high level functions and common terminology for all aspects of operating a nuclear plant. This performance model has eight primary processes supported by 44 sub-processes. Communities of Practice were established for each process area and standards were identified or developed for each process area. This Standard Model was commissioned by the CEO's of the major nuclear utilities and is used to guide plant operations and for benchmarking of innovations in plant processes and performance.

The NRC's regulatory approach is also defined by a model, the Reactor Oversight Model. The regulatory framework for reactor oversight is a risk-informed, tiered approach to ensuring plant safety. There are three key strategic performance areas: reactor safety, radiation safety, and safeguards. Within each strategic performance area are cornerstones that reflect the essential safety aspects of facility operation. Satisfactory licensee performance in the cornerstones provides reasonable assurance of safe facility operation and that the NRC's safety mission is being accomplished.

Within this framework, the NRC's operating reactor oversight process provides a means to collect information about licensee performance, assess the information for its safety significance, and provide for appropriate licensee and NRC response. Because there are many aspects of facility operation and maintenance, the NRC inspects utility programs and processes on a risk-informed sampling basis to obtain representative information.

The Regulator

Without an independent, technically competent, research-informed and systems-thinking regulator highly reliable governance is not possible. The NRC represents one of the most advanced risk-informed regulatory approaches. Ensuring plant safety begins by requiring a design philosophy that includes:

- Multiple, redundant, and independent safety systems;
- Multiple physical barriers, including robust reactor containment to prevent radioactive release; and

- Testing of emergency plans.

This design philosophy is supported by a strong analytical effort that goes beyond technical specifications to include operating experience along with organizational and human factors. The necessary start point for a shift from government to governance is a shift from deterministic to risk-informed regulation. This risk-informed approach combined with a performance-based regulatory regime, versus a prescriptive regulatory regime establishes a basis for a highly reliable governance approach. How these concepts are defined and combined has been described by the NRC as follows: [14]

> The risk definition takes the view that when one asks, "What is the risk?" one is really asking three questions: "What can go wrong?" "How likely is it?" "What are the consequences?" These three questions can be referred to as the "risk triplet." The traditional definition of risk, that is, probability times consequences, is fully embraced by the "triplet" definition of risk.
>
> **Deterministic and Probabilistic Analyses:** The deterministic approach to regulation establishes requirements for engineering margin and for quality assurance in design, manufacture, and construction. In addition, it assumes that adverse conditions can exist and establishes a specific set of design basis events (i.e., What can go wrong?). The deterministic approach involves implied, but unquantified, elements of probability in the selection of the specific accidents to be analyzed as design basis events. It then requires that the design include safety systems capable of preventing and/or mitigating the consequences (i.e., What are the consequences?) of those design basis events in order to protect public health and safety. Thus, a deterministic analysis explicitly addresses only two questions of the risk triplet. In addition, traditional regulatory analyses do not integrate results in a comprehensive manner to assess the overall safety impact of postulated initiating events.
>
> **Risk-Informed Approach:** A "risk-informed" approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety. A "risk-informed" approach enhances the deterministic approach by: (a) allowing explicit consideration of a broader set of potential challenges to safety; (b) providing a logical means for prioritizing these challenges based on risk significance; operating experience, and/or engineering judgment; (c) facilitating consideration of a broader set of resources to defend against these challenges; (d) explicitly identifying and quantifying sources of uncertainty in the analysis (although such analyses do not necessarily reflect all important sources of uncertainty); and (e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions. Where appropriate, a risk-informed regulatory approach can also be used to reduce

[14] Travers, William D. "White Paper on Risk-Informed and Performance-Based Regulation," NRC, March 1, 1999. http://www.nrc.gov/reading-rm/doc-collections/commission/srm/1998/1998-144srm.html.

unnecessary conservatism in purely deterministic approaches, or can be used to identify areas with insufficient conservatism in deterministic analyses and provide the bases for additional requirements or regulatory actions. "Risk-informed" approaches lie between the "risk-based" and purely deterministic approaches. The details of the regulatory issue under consideration will determine where the risk-informed decision falls within the spectrum.

Performance-Based Approach: A regulation can be either prescriptive or performance-based. A prescriptive requirement specifies particular features, actions, or programmatic elements to be included in the design or process, as the means for achieving a desired objective. A performance-based requirement relies upon measurable (or calculable) outcomes (i.e., performance results) to be met, but provides more flexibility to the licensee as to the means of meeting those outcomes. A performance-based regulatory approach is one that establishes performance and results as the primary basis for regulatory decision-making, and incorporates the following attributes: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee performance; (2) objective criteria to assess performance are established based on risk insights, deterministic analyses and/or performance history; (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern. The measurable (or calculable) parameters may be included in the regulation itself or in formal license conditions, including reference to regulatory guidance adopted by the licensee."

Risk-Informed, Performance-Based Approach: A risk-informed, performance-based approach to regulatory decision-making combines the "risk-informed" and "performance-based" elements discussed above, and applies these concepts to NRC rulemaking, licensing, inspection, assessment, enforcement, and other decision-making. Stated succinctly, a risk-informed, performance-based regulation is an approach in which risk insights, engineering analysis and judgment, including the principle of defense-in-depth and the incorporation of safety margins and performance history are used, to (1) focus attention on the most important activities, (2) establish objective criteria for evaluating performance, (3) develop measurable or calculable parameters for monitoring system and licensee performance, (4) provide flexibility to determine how to meet the established performance criteria in a way that will encourage and reward improved outcomes, and (5) focus on the results as the primary basis for regulatory decision-making.

As former Secretary Babbitt said, this regulation does not come without a cost. Currently the NRC employs about 4,000 employees to regulate U.S. nuclear reactors, materials (e.g., medical x-ray equipment), and nuclear waste management. The NRC budget is about $1.04 billion. About 75 percent of the NRC staff and budget are applied to regulating the 104 licensed nuclear power reactors in the United States. In 2009, each U.S. nuclear plant received 6,000 hours of regulatory

inspection. The licensed nuclear operating organizations pay the costs of regulation by congressionally approved approaches.

The Industry

Babbitt's comments on regulation have been augmented by calling for an oil and gas industry organization to promote safe practices; he has said a model is INPO. Similarly William Reilly, Co-Chair of the President's Commission has said that the oil industry needs to create a safety organization modeled on one that has improved operations at nuclear-power plants. An organization modeled on INPO would not be a substitute for stronger Federal oversight but could "create the safety culture that's needed" in offshore drilling, according to Reilly.

Building upon a sound, forward-looking regulatory approach, progress toward high reliability governance requires industry-wide, collaborative self-governance. The U.S. commercial nuclear industry funds three main organizations that perform an array of technical and management functions: the NEI, the Electric Power Research Institute (EPRI), and INPO.

The NEI role is to support the industry in developing policy on key legislative and regulatory issues affecting the industry. It serves as a unified industry voice before the U.S. Congress, executive branch agencies, and Federal regulators, as well as international organizations and venues. NEI also provides a forum to resolve technical and business issues for the industry. Finally, NEI provides information on the nuclear industry to members, policymakers, the news media, and the public.

EPRI conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers, as well as experts from academia and industry, to help address challenges in electricity, including reliability, efficiency, health, safety, and the environment. EPRI also provides technology, policy, and economic analyses to drive long-range research and development planning and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries.

INPO represents a "defining" new approach to independent evaluation of industry performance. INPO does not develop industry standards adopted by the regulator, nor does it conduct advocacy on behalf of the industry. Its charter and operations have been carefully crafted to draw a clear distinction between the NRC as the regulator and INPO as an independent organization that promotes excellence though four keystone programs of evaluation, training, analysis, and assistance.

INPO collects and analyzes equipment performance data, but does not engage in technical standards development. INPO also manages the National Academy for Nuclear Training. The Academy accredits the training programs run by nuclear power utilities similar to how academic programs of universities are accredited. INPO also conducts professional development seminars for nuclear power management ranging from supervisors to corporate Boards of Directors. Once every 2 years INPO evaluates each U.S. nuclear plant using the Objectives and Criteria. Plants are ranked annually based on INPO evaluation results, and the lower performing plants are held to account by

the rest of the industry for upgrading their performance. The insurance providers use INPO plant ratings as a component of setting fees paid by utilities for nuclear plant insurance.

INPO standards of excellence, referred to as Performance Objectives and Criteria, are derived from best performers in the nuclear industry, other high hazards industries such as aviation, and insights from the academic community. The standards are not static; they are continually scrutinized, informed by research, benchmarking, and operating experience; and upgraded as issues emerge and better practices are validated. The basic premise is if you keep doing what you have been doing, in a dynamic environment you are falling behind, not improving. Constant improvement is more than a mantra, it's a fact of survival. INPO standards are performance-focused, not prescriptive and address the following management and operational topics.

FUNCTIONAL AREAS

- Operations
- Maintenance
- Engineering
- Chemistry
- Radiological Protection
- Training

CORPORATE AREAS

- Corporate Leadership & Management
- Corporate Oversight & Monitoring
- Corporate Support
- Human Resources
- Communications

CROSS-FUNCTIONAL AREAS

- Organizational Effectiveness
- Foundation for Nuclear Safety
- Leadership and Management
- Human Performance
- Management & Leadership Development
- Independent Monitoring & Assessment
- Industrial Safety
- Operational Focus
  - Operational Safety
  - Operational Decision-Making
  - Operational Alignment
- Equipment Reliability
  - Equipment Performance
  - Prevention of Equipment Failures
  - Long-Term Equipment Reliability
- Work Management
- Configuration Management
- Maintaining Margins Consistent with Design Requirements
- Operational Configuration Control
- Design Change Processes
- Reactor Engineering and Fuel Management
- Performance Improvement
- Self-Assessment and Benchmarking
- Corrective Action
- Operating Experience
- Emergency Preparedness
- Fire Protection

The guiding principle behind INPO is that all U.S. nuclear plants are "Hostages of Each Other"—that an accident at one plant can cause serious damage to the entire industry.[15] While the NRC is responsible for regulating the safety of U.S. nuclear plants, the industry uses INPO to promote excellence, thus improving performance industry-wide, and to protect the industry as a whole from bad management and declining performance of the few poor performers. It should be noted that the INPO influence is now world-wide; after the Chernobyl accident in the Ukraine in 1986, the international commercial nuclear industry formed the World Association of Nuclear Operators to transfer the INPO excellence approach to all commercial nuclear plants in the world, and the INPO Performance Objectives and Criteria are now becoming the world "standards" for nuclear plant management and operations.

Collectively these three organizations provide the essential industry component of the nuclear governance model. However the industry augments with working groups and communities of practice as deemed necessary. One example of a formalized community of practice is the Procedures Professional Association (PPA).

PPA is the nuclear industry's collective voice and leader in procedure writing and processing. The association provides consistent and benchmarked guidance to commercial nuclear facilities. The mission of PPA is to function as a non-profit organization, developing and exchanging technical information on the design, development, implementation, and use of procedures to increase reliability improve performance, and ensure safe and efficient facility operation. PPA promotes excellence in procedure writing and processing through education and information sharing.

PPA was founded in August of 2005 after functioning in a working group fashion for the prior 17 years. It was determined that an industry association would give stakeholders a strong platform from which to provide input to industry oversight groups such as INPO and NEI. In 2006, members of PPA were integrally involved in the development of the AP-907-001, "Procedure Process," and AP-907-005, "Procedure Writer's Guide," both elements of the Standard Nuclear Performance Model. The Standard Nuclear Performance Model is a comprehensive model that includes INPO, NEI and EPRI process descriptions and provides a consistent basis for describing how work is done at nuclear power plants for process areas.

Insurance

Insurance is both a forcing and reward feature of the nuclear governance approach. The Price-Anderson Act, which became law on September 2, 1957, was designed to ensure that adequate funds would be available to satisfy liability claims of members of the public for personal injury and property damage in the event of a nuclear accident involving a commercial nuclear power plant. The legislation helped encourage private investment in commercial nuclear power by placing a cap, or ceiling on the total amount of liability each holder of a nuclear power plant licensee faced in the event of an accident. Over the years, the "limit of liability" for a nuclear accident has increased the insurance pool to more than $12 billion. Under existing policy, owners of nuclear power plants pay a premium each year of $375 million in private insurance for offsite liability coverage for each reactor unit. The average annual premium for a single-unit reactor site is $400,000. Insurance under Price-

[15] A book by this name by Victor Rees chronicled the development and significance of INPO in the nuclear industry.

Anderson covers bodily injury, sickness, disease or resulting death, property damage, and loss, as well as reasonable living expenses for individuals evacuated.

Separately from the Price-Anderson required insurance, utilities acquire property casualty accident coverage through Nuclear Electric Insurance Limited (NEIL). NEIL insures nuclear plants and their generating units, owned by electric utilities (the "Members"), primarily in the United States. It provides property insurance coverage to all of the commercial nuclear power generating facilities in the United States for: (1) the costs associated with certain long-term interruptions of electric generation, under the primary and accidental outage programs due to accidental physical damage to insured sites; (2) decontamination expenses incurred at such sites arising from accidental nuclear contamination; and (3) other risks of direct physical loss at such sites, including certain premature decommissioning costs under the primary and excess programs.

Research

Research on new technologies is supported by many industries. For High Reliability Organizations, a corresponding emphasis is placed on the socio aspects of socio-technical systems. The need for such research was elaborated by the National Science Foundation.

> Over the last decade, the thesis that scientific and technological research can contribute to overcoming sustainability challenges has become conventional wisdom among policy, business, and research leaders. By contrast, relatively little attention has been given to the question of how a better understanding of the human and social dimensions of science and technology could also contribute to improving both the understanding of sustainability challenges and efforts to solve them. Yet, such analyses would seem central to sustainability research. After all, human applications of science and technology pose arguably the single greatest source of threats to global sustainability, whether we are talking about the energy and transportation systems that underpin global industrial activities or the worldwide expansion of agriculture into forest and savannah ecosystems. These applications arise out of complex social, political, and economic contexts—and they intertwine science, technology, and society in their implementation—making knowledge of both the human and social contexts and elements of science and technology essential to understanding and responding to sustainability challenges. Thus, while science and technology are central to efforts to improve human health and well being, the application of science and technology has not always contributed as anticipated in past efforts to improve the human condition. It is essential, therefore, that research on the relationships between science, technology, and society be integrated into the broader sustainability research agenda. [16]

The NRC has for years invested in risk and social systems research. The NRC's Human Performance Research program focuses on the interaction of people with the systems and the environments in which they work. It establishes the technical basis for NRC initiatives in areas such

[16] Miller, Clark, et al. "Science, Technology, and Sustainability: Building a Research Agenda," National Science Foundation Supported Workshop, September 8-9, 2008.

as inspection guidance for evaluating emergency operating procedures, a systems approach to training, human system interface design for current and advanced control station design, human performance contributors in events, communications-related corrective action plans, shift working hours, and fatigue management programs.

As an example, NUREG/CR-6753 "Review of Findings for Human Performance Contribution to Risk in Operating Events," [17] was performed for the NRC by researchers at the Department of Energy's Idaho National Laboratory. The results showed that human performance contributed significantly to analyzed events. In the events reviewed, 270 human errors were identified and multiple human errors were involved in every event. Latent errors (i.e., errors committed prior to the event whose effects are not discovered until an event occurs) were present four times more often than were active errors (i.e., those occurring during event response). The latent errors included failures to correct known problems and errors committed during design, maintenance, and operations activities. This study was instrumental in helping to shift the emphasis from discipline, training, and procedure fixes to a systems view of the technical, management, workplace, and cultural factors that influence individual and collective human behaviors.

INPO also invests significant attention to research. From an operational perspective, analysis of operating experience to identify industry-wide issues is an INPO cornerstone. This analysis is often an impetus for industry-wide performance improvement initiatives. For instance, even before the NRC's NUREG/CR-6753, INPO began research on human performance contribution to events though the Human Performance Evaluation System. That effort reached similar conclusions—that latent errors were primary drivers of performance. To change the "blame, shame, retrain, and fix procedure" paradigm, INPO developed the Human Performance Improvement (HPI) initiative. INPO did an extensive review of human performance literature and engaged the nuclear industry in developing practices and techniques to reduce and mitigate adverse consequences of human error while concentrating organizational attention on remedying the underlying factors that influenced risk-provoking behavior.

For nuclear plants in Sweden and Finland, the VTT Technical Research Centre of Finland has conducted a series of studies that examine human, organizational, and cultural factors that affect nuclear operations. Currently VTT is engaged in research on the implications of these factors for construction of new plants.

Multi-agent Collaboration

Collaboration on issues of industry-wide concern is another distinguishing characteristic of commercial nuclear power. The currently ongoing collaboration on safety culture serves as an illustration.

Safety culture was established as an important to safety concept by the International Atomic Energy Agency's International Nuclear Safety Group (INSAG) in the 1988 "Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident." [18] INSAG described safety culture

[17] http://adamswebsearch2.nrc.gov/idmws/DocContent.dll?library=PU_ADAMS^pbntad01&LogonID=2e49dde151434488745b3edc36b15e6f&id=004065859.

[18] "Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident: A Report by the International Nuclear Safety Advisory Group Safety." INSAG, 1986.

as: "That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance." In 1989 the NRC expressed its expectations for a positive safety culture.

Problems at the Millstone plant in 1996 led the NRC to raise concerns about the plant's safety culture, primarily related to the handling of employee safety concerns. In 2002, a major corrosion of the nuclear reactor head was discovered at the Davis Besse nuclear plant. Investigations led to a concern about safety culture that expanded beyond earlier attention to employee safety concerns to generalized concern about the utility's risk management philosophy and behaviors. In 2004, the NRC communicated new directions for evaluating safety culture and made subsequent revisions to the Reactor Oversight Process to specifically address safety culture.

The U.S. nuclear industry took note of the importance of safety culture soon after the Davis Besse event. INPO issued number of prompt recommendations to which utilities were committed to respond. Then INPO assembled a group of industry representatives to develop guidance. This guidance, published in final form in 2004, took the form of a statement of safety culture principles and supporting attributes. This document became the basis for INPO review of safety culture during the formal INPO evaluations. The nuclear industry also engaged the assistance of Dr. Edgar Schein of MIT as an advisory member of one of INPO's senior advisory groups; Dr. Schein is well respected as a leading authority on organizational culture. Building upon the INPO efforts the industry turned to NEI to lead an effort for safety culture management and self assessment.

NRC continued work on a new policy on safety culture intended to address not only reactors, but also other licensees that use regulated nuclear material, including medical isotopes. A series of public meetings were initiated to inform stakeholders and the public of the NRC's continuing emphasis on safety culture and seek input. In February of 2010, a 3-day workshop was held at which NRC and major stakeholders presented views on safety culture improvement activities and working groups of the stakeholders' communities suggested revisions to the draft NRC policy language. Most recently NRC and INPO collaborated on an industry-wide survey of safety culture in an effort to ascertain which characteristics of the principal safety culture models might be most influential on risk. The study was conducted by INPO, with input from the NRC in study development; 100 percent of the U.S. plants participated in the study, and the results were jointly analyzed by a team of scientists from NRC and INPO.

As this example illustrates, issues of industry-wide significance warrant and require involvement of major stakeholders, the public, and the regulator. Only through such collaborative effort can the requisite knowledge, skill, experience, perspectives, and scientific rigor be assembled to produce robust improvement initiatives with the flexibility to be applied in a manner appropriate to a variety of operational contexts.

7.0 Application Of Concept

There are three prevailing perspectives on the BP Deepwater Horizon accident:

1) It's just BP—everyone else is fine; just follow procedures, trust the industry.
2) Restrict deep-water drilling, develop more prescriptive regulations, and conduct more frequent inspections.

3) Fundamental change is needed—a Highly Reliability Governance approach.

The "It's just BP" perspective is the prevailing view being heard thus far from other petroleum operators in the Gulf. The second perspective is heard from a number of environmental groups. The third, "Highly Reliable Governance," is being talked about in various terms by a number of prominent individuals, including leadership of the President's Deepwater Commission. The Highly Reliable Governance approach would involve the U.S. government, the petroleum industry, and the academic community informed by stakeholders and the public. This approach recognizes that the regulator cannot develop prescriptive regulations to foresee all possible conditions that could result in accidents. It recognizes that technology, operational, and management techniques are constantly evolving. And it recognizes that the organizational and cultural aspects of complex socio-technical systems are determining factors in safe operations. The main components of this approach that are actively being discussed include:

1) New government regulation model with
    a. Independent government regulatory agency funded by industry fees
    b. A systems safety regulatory model clearly establishing that system safety is necessary to prevent major events; that worker protection models, while essential and mandatory, alone are not sufficient
    c. Safety cases (including detailed drilling and spill response plans)
    d. Risk-informed regulation (a combination of traditional engineering requirements for technical systems and components informed by probabilistic risk assessment to focus on safety critical systems and components, combined with performance regulations for management and organizational systems and processes)
    e. Intense training and qualification programs for inspectors
    f. Onsite inspectors
    g. Industry-wide reporting system with "whistle blower" protection
2) An independent organization, established by industry, to perform evaluation of drilling and production operations
3) Independent standards and training to promote excellence
4) Industry-funded accident insurance pool
5) Research on petroleum industry management excellence
6) Research and investment in developing new safer and cheaper technologies
7) Safety equipment standardization and qualification
8) Industry-wide emergency response capability

8.0 Concluding Thoughts

Many of the items mentioned for inclusion in a Highly Reliable Governance model have already been discussed in public statements or reports on Deepwater. Applications of advanced risk analysis and risk management in the petroleum industry are not new. [19, 20, 21] Of course it is difficult to project

[19] Bea, R. G. "Performance shaping factors in reliability analysis of design of offshore structures." Journal of Offshore Mechanics and Arctic Engineering. Transactions of the ASME. Vol. 122, no. 3, (August 2000): 163-172.

[20] Bea, R.G. "Human and Organizational Factors in Reliability Assessment and Management of Offshore Structures." Society for Risk Analysis, 22 (2002): 29-45.

what will happen until after the formal inquires have been completed and the Congress and Administration take action. Many stakeholders will have input to the deliberations, and the petroleum industry inputs will be important. The industry response will directly shape public opinion—an attitude of business as usual will only heighten the public distrust of the industry.

Except for discussions about a joint spill response program, the statements from the petroleum industry in the United States have generally been that this is just a BP problem; the other companies would not have behaved as BP did. Perhaps there is yet another lesson to learn from the nuclear industry.

Immediately after the Three Mile Island accident many utilities responded similarly—the plant operator Met Ed was just a poor performer; all the others were better. Then, a few far-seeing leaders emerged. The stature of these individuals among their colleagues, and statesman-like efforts, helped catalyze other to commit to themselves and the public that another Three Mile Island would never occur in this country. Thus INPO was born with all industry CEO's agreeing to form the Institute, fund it, and adhere to an unending search for excellence. The journey continues after 30 years. Today the nuclear industry is emblematic of an industry-wide HRO effort.

There are a number of permutations of approaches that could emulate the nuclear success factors. Some combination of an NRC model and Federal Aviation Agency model is a possible regulatory approach. However independence will be essential. Regulator acceptance of API standards and multiple nation flag certification for drilling rig vessels is counterproductive to independent regulation. Industry standards may be used to share best practices in search of excellence, but they cannot be used as surrogate for government-mandated requirements based on science, engineering, and operating experience. Upon this basis, and this basis alone, can regulation then be risk informed and performance based.

Independent industry self-governance could be enabled through a single entity such as INPO, or enhanced portfolios of highly respected certifiers like Det Norske Veritas could be a possibility. However a single overseer would have to validate performance of reviews by multiple certifying agents and the inspection and certification functions would need to be separated from other consulting functions. The U.S. regulatory agency would have to figure what status might be accorded to such certifications. Whatever governance regime is established, excellence in risk management will be essential.

In a his 1991 paper, "Human Factors in Large-Scale Technological Systems' Accidents," Najmedin Meshkati[22] examined commonalities among the Three Mile Island, Bhopal, and Chernobyl accidents and offered human factors recommendations to prevent reoccurrence. The urgency of these human factors recommendations was emphasized with the admonition that these actions were "long overdue and constitute only a necessary step toward ensuring the safety of complex, large-scale technological systems." His recommendations and the urgency of improvements needed remain true today to prevent future Deepwater Horizon accidents.

[21] Thomassen, O. and Sorum, M. "Mapping and Monitoring the Technical Safety Level." Paper presented at the Society of Petroleum Engineers International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production, Kuala Lumpur, Malaysia: (March 20-22, 2002).

[22] Meshkati, N. "Human Factors in Large-Scale Technological Systems' Accidents: Three Mile Island, Bhopal, Chernobyl." Industrial Crisis Quarterly 5 (1991): 131-154.

Dr. Meshkati's paper concludes with observations foretelling the need for Highly Reliable Governance. While technical and human factors improvement are necessary:

> "To make it sufficient, in the long-run, we need much more commitment, communication and cooperation among those who could make these systems safer—the government and regulatory agencies, plant manufactures and managers, unions, and the human factors and other concerned research communities. We need an overall paradigm shift in dealing with complex technologies' safety and operation. We need more institutionalized interaction among all stakeholders in the public and private sectors. Above all, we need genuine and real dedication of all parties, not rhetoric or public relations ploys for this collective effort. As professed by the late Nobel physicist, Richard Feynman, in the context of another complex technological system's accident, the Space Shuttle Challenger explosion: "For a successful technology, reality must take precedence over public relations, for nature cannot be fooled."

9.0 References

1. Acona Ltd. "Defining Best Practice in Corporate Occupational Health and Safety Governance." Health and Safety Executive (2006).
2. American Nuclear Society. "Risk-Informed and Performance-Based Regulations for Nuclear Power Plants," Position Statement 46 (2004). http://www.ans.org/pi/ps/docs/ps46.pdf.
3. Ayres, P. "Regulation in the 21st Century: From Prescription to Collaborative Supervision" (Paper presented at the 10th XBRL International Conference, Brussels, Belgium, November 16, 2004).
4. Babbit, B., "Offshore Oil Needs Greater Regulation," Politico Blog. August 2, 2010. http://www.politico.com.
5. Bea, R. G. "Performance shaping factors in reliability analysis of design of offshore structures." Journal of Offshore Mechanics and Arctic Engineering. Transactions of the ASME. Vol. 122, no. 3, (August 2000): 163-172
6. Bea, R.G. "Human and Organizational Factors in Reliability Assessment and Management of Offshore Structures." Society for Risk Analysis, 22 (2002): 29-45.
7. Beardsley, M. "NRC Inspections: Risk-Informed and Performance-Based." Pennsylvania Journal of Nuclear Medical Technology 36 (2008): 129–131.
8. Berkes, F. "From Community-Based Resource Management to Complex Systems: The Scale Issue and Marine Commons." Paper presented at MEA Bridging Scales Conference, March 2004 and published in Ecology and Society 11:1 45. (2006).
9. Bigley, G.A. and Roberts, K.H. "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments." *The Academy of Management Journal* Vol. 44, No. 6 (December 2001): 1281-1299.
10. Boardman, J. and Lyon, A. Acona Ltd. "Defining Best Practice in Corporate Occupational Health and Safety Governance." Health and Safety Executive (2006).
11. BP U.S. Refineries Independent Safety Review Panel. The Report of the BP U.S. Refineries Independent Review Panel. London: BP (also known as the Baker Report), 2007.

12. Carroll, J.S. "Organizational Learning Activities in High Hazard Industries: The Logics Underlying Self-Analysis". Journal of Management Studies, Blackwell Publishing, vol. 35(6), November (1998): 699-717.
13. Charreaux, G. "Corporate Governance Theories: From Micro Theories to National Systems Theories." Working paper 1041202 FARGO Centre de recherche en Finance, Architecture et Gouvernance des Organisations , (2004).
14. Cherry, B.A. "Institutional Governance for Essential Industries under Complexity: Providing Resilience within the Rule of Law." CommLaw Conspectus 17 (2008-2009).
15. de Loë, R.C., Armitage, D., Plummer, R., Davidson, S. and Moraru, L. "From Government to Governance: A State-of-the-Art Review of Environmental Governance." Final Report. Prepared for Alberta Environment, Environmental Stewardship, Environmental Relations. Guelph, ON: Rob de Loë Consulting Services. (2009).
16. Deakin, Simon F. and Carvalho, Fabio. "System and Evolution in Corporate Governance." ECGI - Law Working Paper No. 150/2010 (April 2, 2010). Available at SSRN: http://ssrn.com/abstract=1581746.
17. Det Norske Veritas. "Key Aspects of an Effective U.S. Offshore Safety Regime." DET NORSKE VERITAS White Paper, (July 22, 2010).
18. Dooley, K.J., Johnson, T., and Bush, D. "TQM , Chaos, and Complexity." Human Systems Management, 14(4) (1995): 1-16.
19. Dooley, K.J. "A Complex Adaptive Systems Model of Organization Change." Nonlinear Dynamics, Psychology, and Life Sciences 1 (1997): 67-97.
20. Duit, A. and Galaz, V. "Governance and Complexity—Emerging Issues for Governance Theory." Governance: An International Journal of Policy, Administration, and Institutions 21 (2008): 311–335.
21. Eisner, M. "Corporate Environmentalism, Regulatory Reform, and Industry Self-Regulation: Toward Genuine Regulatory Reinvention in the United States." Governance: An International Journal of Policy, Administration, and Institutions 17 (2004): 145–167.
22. Gaertner, J., Canavan, K., and True, D. "Safety and Operational Benefits of Risk-Informed Initiatives." An EPRI White Paper, Electric Power Research Institute. (February 2008). http://mydocs.epri.com/docs/CorporateDocuments/SectorPages/Portfolio/Nuclear/Safety_and_Operational_Benefits_1016308.pdf.
23. Gunningham, N., Grabosky, P. and Sinclair, D. Smart Regulation: Designing Environmental Policy. Oxford: Oxford University Press, 1998.
24. Hallbert, B.P., Jeffrey, J.C., Blackwood, L.G., Dudenhoeffer, D.D. and Hansen, K.F. "Developing Human Performance Measures" (Paper presented at PSAM8, New Orleans, Louisiana , May 14-19, 2006).
25. Hartzog, P.B. "21st Century Governance as a Complex Adaptive System." http://www.panarchy.com/Members/PaulBHartzog/Papers/21st%20Century%20Governance.pdf.
26. Hartzog, P.B. "Panarchy: Governance in the Network Age." http://panarchy.com/Members/PaulBHartzog/Papers/Panarchy%20-%20Governance%20in%20the%20Network%20Age.pdf.
27. Hatfield-Dodds, S., Nelson, R. and Cook, D.C. "Adaptive Governance: An Introduction and Implications for Public Policy" (Paper presented at the ANZSEE Conference, Noosan, Australia, July 4-5, 2007).
28. Heimeriks, G. "Governing science as a complex adaptive system." Innovation Studies Utrecht (ISU) Working Paper Series ISU Working Paper #09.16 (November 2009).

29. Hillman, K., Nilsson, M., Rickne, A. and Magnusson, T. "Fostering Sustainable Technologies – A Framework for Analysing the Governance of Innovation Systems." Proceedings of the First European Conference on Sustainability Transitions, Amsterdam, June 4-6, 2009)
30. Hopkins, A. "The Problem of Defining High Reliability Organisations." Working Paper 51: National Research Centre for OHS Regulation Australian National University (2007).
31. Kadak, A.C. and Matsuo, T. "The nuclear industry's transition to risk-informed regulation and operation in the United States." Reliability Engineering and System Safety 92 (2007): 609–618.
32. Kemp, R., Parto, S. and Gibson, R.B. "Governance for sustainable development: moving from theory to practice." Int. J. Sustainable Development, Vol. 8, Nos. 1/2, (2005): 12–30.
33. Knepper, H., Sitren, A., and Smith, H. "An Examination and Synthesis of Two Public Administration Concepts and their Relevance for Public Administration Students." Public Affairs Review: e-Journal of the Doctoral Program in Public Affairs (Winter 2006).
34. La Porte, T.R. and Thomas, C.W. "Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations." Journal of Public Administration Research and Theory: J-PART 5 (1995): 109-137.
35. Leach, M., Bloom, G., Ely, A., Nightingale, P., Scoones, L., Shah, E., and Smith, A. "Understanding Governance: Pathways to Sustainability" STEPS Working Paper 2. Brighton: STEPS Centre, (2007).
36. Meserve, Richard. "NRC's Regulatory Approach: OIG's Role in a Time of Change" (Keynote Address at OIG Annual Information and Planning Conference, Rockville, MD, September 12, 2000).
37. Meshkati, N. "Human Factors in Large-Scale Technological Systems' Accidents: Three Mile Island, Bhopal, Chernobyl." Industrial Crisis Quarterly 5 (1991): 131-154.
38. Miller, C., Sarewitz, D. , Light, A. "Science, Technology, and Sustainability: Building a Research Agenda." National Science Foundation Supported Workshop, September 8-9, 2008).
39. Moss, D., and Cisternino, J. eds. New Perspectives on Regulation. Cambridge: The Tobin Project, 2009. http://www.tobinproject.org/twobooks/pdf/New_Perspectives_Full_Text.pdf.
40. Ortwin, Renn. Risk Governance: Towards and Integrative Approach. Geneva: International Risk Governance Council, 2006.
41. Reason, J.T. Human Error. Cambridge: Cambridge University Press, (1990)
42. Reiman, T. and Norros, L. "Regulatory Culture: Balancing the Different Demands of Regulatory Practice in the Nuclear Industry." In Changing Regulation – Controlling Hazards in Society, ed. A. R. Hale et al., 175 – 192. Oxford: Pergamon, 2002.
43. Reiman, T. and Oedewald, P. "Evaluating Safety-Critical Organizations – Emphasis on the Nuclear Industry." Finland: VTT, 2009. http://www.stralsakerhetsmyndigheten.se/Global/Publikationer/Rapport/Sakerhet-vid-karnkraftverken/2009/SSM-Rapport-2009-12.pdf.
44. Reiman, T. and Oedewald, P. "Safety Management and Organizational Learning and Safety Culture" and "Organizational Learning." In SAFIR2010 The Finnish Research Programme on Nuclear Power Plant Safety 2007–2010 Interim Report, ed. Eija Karita Puska, 305–322. Finland: VTT, 2009.
45. Reiman, T. and Pietikäinen, E. "Indicators of Safety Culture – Selection and Utilization of Leading Safety Performance Indicators." Finland: VTT, 2010.

46. Renn, O. ed. "Risk Governance Towards An Integrative Approach." Geneva: International Risk Governance Council, 2005 (reprinted 2006).
47. Roberts, K.H. New Challenges to Understanding Organizations. New York: Macmillan, 1993.
48. Roberts, K.H. "Managing the Unexpected: Six Years of HRO-Literature Reviewed." Journal of Contingencies and Crisis Management 17 (2009): 50-54.
49. Roe, E., and Schulman, P. High Reliability Management: Operating on the Edge. Stanford: Stanford Business Books, 2008.
50. Sabel, C.F. "Beyond Principal-Agent Governance: Experimentalist Organizations, Learning and Accountability." In De staat van de democratie, Democratie voorbij de staat, ed. E. R. Engelen and M. Sie Dhian Ho., Chapter 9. Amsterdam: Amsterdam University Press, 2004.
51. Sandom C. "Human Factors Considerations for System Safety." In Components of System Safety, ed. Redmill F and Anderson T. Proceedings of 10th Safety Critical Systems Symposium, Southampton, UK: Springer-Verlag, February 5-7, 2002.
52. Santa Fe Institute History, http://www.santafe.edu/about/history/.
53. Schneider, V. and Bauer, J.M. "Governance: Prospects of Complexity Theory in Revisiting System Theory." Paper presented at the annual meeting of the Midwest Political Science Association, Chicago, Illinois, April 14, 2007.
54. Scoones, I., Leach, M., Smith, A., Stagl, S., Stirling, A. and Thompson, J. Dynamic Systems and the Challenge of Sustainability. Brighton: STEPS Centre, 2007.
55. Smith, R. "Members of Past Disaster Panels See Recurring Pattern." Wall Street Journal, June 16, 2010.
56. Stoker, G. "Governance as Theory: Five Propositions." International Social Science Journal 50 (1998): 17–28.
57. Thomassen, O. and Sorum, M. "Mapping and Monitoring the Technical Safety Level." Paper presented at the Society of Petroleum Engineers International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production, Kuala Lumpur, Malaysia: March 20-22, 2002.
58. U.S. Chemical Safety and Hazards Investigation Board. Investigation Report: Refinery Explosion and Fire. Washington, D.C.: U.S. Chemical Safety and Hazards Board, 2005.
59. U.S. Nuclear Regulatory commission, "History of the NRC's Risk-Informed Regulatory Programs", http://www.nrc.gov/about-nrc/regulatory/risk-informed/history.html.
60. U.S. Nuclear Regulatory Commission, SECY-98-144 - WHITE PAPER ON RISK-INFORMED AND PERFORMANCE-BASED REGULATION, http://www.nrc.gov/reading-rm/doc-collections/commission/srm/1998/1998-144srm.html.
61. U.S. Nuclear Regulatory Commission. "White Paper on Risk-Informed and Performance-Based Regulation, Secy-98-144." Washington D.C.: U.S. Nuclear Regulatory Commission, (1998).
62. Vaughan, D. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago: University of Chicago Press, 1996.
63. Wahlström, B. "Risk Informed Approaches for Plant Life Management: Regulatory and Industry Perspectives." Paper presented at FISA 2003, EU research in reactor safety, Luxembourg, November 10-13, 2003.
64. Wahlström, B., Wilpert, B., Cox, S. Solá, R. Rollenhagen, C., Ibanez, M., Canaff, Y. Friberg, M., Andersson, O., Scheuring, R., Gerdes, P., Rycraft, H., Dunge, E. and Egnér, K.

"Learning organisations for nuclear safety (LearnSafe)." Paper presented at FISA 2003, Luxembourg, November 10-13, 2003.
65. Weick, K. Sensemaking in Organizations. Thousand Oaks: Sage, 1995.
66. Weick, K. and Roberts, K.H. "Collective Mind and Organizational Reliability: The Case of Flight Operations on an Aircraft Carrier Deck." Administrative Science Quarterly 38 (1993): 357-381. Also in Organizational Learning, M.D. Cohen, and L.S. Sproull (Eds.), 330-358. Thousand Oaks, CA: Sage, 1995.
67. Weick, Karl and Sutcliffe, Kathleen. Managing the Unexpected: Assuring High Performance in an Age of Complexity. San Francisco: Jossey Bass, 2001.
68. Weick, Karl and Sutcliffe, Kathleen. Managing the Unexpected: Resilient Performance in An Age of Uncertainty. 2nd Edition. San Francisco: Jossey Bass, (2007).
69. Wilkinson, P. "Safety Cases: Success or Failure?" National Research Centre for OHS Regulation, The Australian National University, Seminar Paper, May 2, 2002.
70. Woods, D.D. and Cook, R.I. "Mistaking Error" In The Patient Safety Handbook, Youngberg, B. J. and Hatlie, M..J., Sudbury, Chapter 7. Jones and Bartlett Publishers, 2004.
71. Ozoliņa, Z., Mitcham, C. Stilgoe. J., Andanda, P., Kaiser, M., Nielsen, L., Stehr, N. and Ren-Zong Qiu. EUR 23616 EN – Global Governance of Science – Report of the Expert Group on Global Governance of Science to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, 2009.
72. Wahlström, B. "Organisational learning in theory and practice – reflections from the nuclear industry." Paper presented at the NeTWork workshop Event Analysis and Learning from Events, Steinhoefel near Berlin, August 28-30, 2008.

Appendix J

A High Reliability Management Perspective On The Deepwater Horizon Spill, Including Research Implications

Emery Roe and Paul R. Schulman

1.0 Introduction

We may never know all the events that led up to the Deepwater Horizon Oil Spill, but that will not stop decisionmakers from having to explain what happened. The outlines of their storyline are already clear. The Spill was the culmination of multiple failures, human and technical.[1] What could have been prevented by way of better technology, drilling practice, industry standards, corporate responsibility and government regulation wasn't, and as a result a catastrophe like this became all but inevitable.

The problem with the storyline isn't the facts about the casing, blow-out preventer, cement, saltwater replacing the mud, and more. The real issue for us is the premature policy implications that are now being—and are going to be—drawn from this sequence of mistakes. A blame scenario built around mistake-after-mistake is one that invariably scapegoats the lack of government regulation as the ultimate culprit. For it is government regulation that ensures oversight to prevent error, and a storyline that is a catalogue of preventable error after preventable error is one that nearly always ends up at regulation's front door.

You see this kind of blame scenario everywhere today. Just as it is now argued that mortgage companies and investment firms were "acting rationally" in the face of government's failure to regulate the banking and finance sector, so too increasing numbers will be arguing that oil companies were actually under-regulated and thus "acting rationally" given the incentives and disincentives they faced for deepwater drilling. Just as we are told that the financial crisis requires international coordination and regulation—which of course won't happen any time soon—so too we will hear the argument that oil drilling really requires a powerful national if not international regulatory regime, otherwise we should expect such spills to continue. The soft underbelly of this kind of reasoning is patent: It implies that the original errors were preventable, if and only if—miracle happens here—"effective regulation" were in place at the scale needed from the outset.

More effective regulation, it seems, is required, and certainly its lack had a role in the Spill. But it is too early to claim "bad regulation" as the disease and "good regulation" as the antidote when it comes to catastrophes such as the Deepwater Horizon. The conclusion is premature for at least three sets of reasons.

First, we know that high-level executive management failures in the context of severe market pressures can induce large-company technological disasters. Charles Perrow, the sociologist and

[1] S. Kirchgaessner, "Mystery over crew's reaction times to disaster," Financial Times, May 28, 2010, 3.

complex systems analyst, reviewed the case material and concludes there is "very good evidence of what will be called 'executive failures,' where the chief executive ignores the warnings of his staff and forces them to conduct unsafe practices." [2] But large companies facing the same regulatory incentives and disincentives act in very different ways when it comes to being reliable in what they do. Such differences are not reducible to "regulation." [3]

Second, even with political will, the proffered solution—more effective regulation on a wider scale—isn't the basket in which you would want to put your most important eggs. We know that deepwater oil drilling is incredibly complex and uncertain. By differentiating regulatory responsibilities or creating new or expanded multinational or international regulatory agreements, we instantaneously increase the complexity and uncertainty of regulatory oversight and inspection. Regulatory responsibilities can be confused as well as sharpened by agency differentiation. The larger the territory to be regulated, for example, the more important site-to-site differences are when it comes to interpreting or modifying the regulations.

The remainder of this paper looks to a third set of reasons why it is premature to draw policy implications at this stage from the Spill, and suggests a line of research needed to inform discussions about future regulatory strategies.

Our specific concern centers on a different problem in the "mistake-after-mistake-inevitably-leading-to-disaster" scenario. It gives the impression that the "correct" understanding of the Spill follows this format: a set of identifiable preventable mistakes is discovered, which because they weren't prevented, meant that causally, disaster was inescapable. This conclusion may be part of a carefully researched conclusion, but that conclusion would also have to consider:

- That other mistakes may have been prevented by control operators and support staff (on the rig in the driller's chair or in Houston[4, 5]) which could have led to an earlier disaster, had they not been prevented;
- That an earlier or later disaster could have happened even if the sequence of events leading up to the Spill had not occurred; that is, the highlighted mistakes were sufficient but not necessary; and/or
- That there was a point at which the control operators and support staff, on the rig in the driller's chair or in Houston, if listened to, could have prevented the blowout from occurring—albeit they may have been unable to prevent another failure from occurring in its place.

The three possibilities can render conclusions about the preventability of the mistakes and/or the inevitability of the Spill much less clear-cut than supposed. In particular, we suspect one reason why regulators always play catch-up to changing events ("Why do we keep fighting the last war?") is that political and regulatory decisionmakers seize on one sequence of mistakes as the "cause" of the

[2] C. Perrow, The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters (Princeton, NJ: Princeton University Press, 2007), 9-10.

[3] E. Roe and P.R. Schulman, High Reliability Management (Stanford, CA: Stanford University Press, 2008).

[4] "Just like NASA, BP has a control room in Houston where engineers and managers stare at monitors showing remote craft in a distant location attempting to pull off extraordinary feats." (Gapper)

[5] J. Gapper, "BP is drilling itself into deep water," Financial Times, May 6, 2010, 11.

catastrophe without having to think through all the other possibilities that were at work at the same time.

Below we argue that you first have to understand what control room operators do and are expected to do, an approach we have examined is High Reliability Management (HRM). The rest of our paper parses the Spill through the HRM approach focused on control operators and support staff, so as to draw out the above possibilities more clearly. Once drawn, we examine their policy implications and compare them to those currently discussed.

2.0 Control Rooms And High Reliability Management

To be clear, the little we know about control operators on the Deepwater Horizon drilling rig and support staff in Houston is what we have taken from media accounts, email interchanges with DHSG members, and published documents related to the spill.

Certainly, there is no single large control room on the rig in the same way as there is in a major nuclear power plant or electricity transmission center. The rig's driller has controls and video screens and some support staff—for example, the mud engineer at another console—to help. There is a separately located control room on the rig to keep the rig afloat, on site, and undertake other operational activities, although this is the domain of the captain and not the driller.[6] As for Houston, its support operations have been much more in the form of an improvised incident command center than as a permanent control room with shift operators at formal consoles. The organizational and business tensions between Houston and the rig, and within the rig's corporate and drilling components, remain to be more fully accounted for and explained.

Our own professional knowledge about control operators comes from what we have found in our research on water and electric transmission control rooms as well as what others have written about operators in transportation (air and rail), telecommunications and other critical infrastructure control rooms.[7, 8, 9, 10, 11, 12, 13, 14] What follows is based on that knowledge and we would expect that what follows would have to be modified in some respects for drilling control operations, if only because of their off-shore/on-shore components.

---

[6] Peter Marshall, personal communication; William Gale, personal communication.

[7] The literature on operators working in control rooms or in other units operating under mandates for real-time reliability is wide but dispersed. Much has done in the field of Human Factors Analysis and Quality Control, though by no means do these literatures speak with one voice (Roe and Schulman). The reader seeking to delve more in this area by way of material that joins concepts and case material can start with the sampler of Kahneman and Klein, Klein, De Bruijne, Woods and Hollnagel, Garbis and Artman, and Roth et al.

[8] E. Roe, op. cit.

[9] D. Kahneman and G. Klein, "Conditions for intuitive expertise," American Psychologist, 64 (2009): 515-526.

[10] G. Klein, Sources of Power: How People Make Decisions (Cambridge MA: MIT Press, 1999).

[11] M. de Bruijne, Networked Reliability: Institutional Fragmentation and the Reliability of Service Provision in Critical Infrastructures (Delft, The Netherlands: Delft University of Technology, 2006).

[12] D. Woods and E. Hollnagel, Joint Cognitive Systems (Boca Raton: CRC Press, 2006).

[13] C. Garbis and H. Artman, "Team situational awareness as communication practice," In A Cognitive Approach to Situation Awareness: Theory and Application, edited by S. Banbury and S. Tremblay (Great Britain: Ashgate Publishing, 2004).

[14] E. Roth, J. Multer, and T. Raslear, "Shared situation awareness as a contributor to high reliability performance in railroad operations," Organization Studies 27(7), (2006): 967-987.

Control operators are doing their job when their unit manages the safe and continuous provision of a critical service deemed necessary in a wider organizational or social context. In the context of the oil and natural gas sector, exploration and drilling are considered essential activities. To do that job requires situational awareness of those in the drilling control units.

Why is situational awareness important? Because operators see the technical systems they manage as full of major accidents waiting to happen, which would happen if they were not prevented by the operators with the tools they have. For our purposes, this capacity for high reliability management has four components: (a) key skills of control operators, (b) their avoidance of an accident precursor zone, (c) access to multiple performance modes, and (d) bandwidth management.

The *key operator skills* are the operators' abilities, on one hand to recognize patterns (relationships and trends) at the system level, while on the other hand, formulate specific contingency scenarios for what they are doing right now, right here. Without these skills and the knowledge that comes with knowing system patterns and local contingency scenarios, the control room can't tell what's abnormal or unusual—and that is where the precursor zone comes in. "If we've learned anything so far about the deepwater Gulf of Mexico, it is that it contains surprises. And that means an operator needs depth — depth in terms of resources and expertise — to create the capability to respond to the unexpected," wrote the then BP vice-president for Gulf deepwater developments.[15]

The control operators' *precursor zone* is a set of conditions that are at the limit of the knowledge and skills the operators have with respect to the system they are operating. This edge of control operations is where the skills of operators and their support staff are significantly challenged in relation to their task requirements. Operators are no longer clear on what actions of theirs could lead to accidents and failure versus what would lead to them.

Of course, given time and support staff, operators try to figure out what is going here, but all too often that those assets aren't available. As such, operators avoid this zone as much as they can, not just because the risks are higher from being there but for the more basic reason that they can't actually calculate and compare operational risks once they're there. They end up outside their domain of competence and that is a risk all of them are trained to avoid.

This isn't to say that operators never have to operate at the limits of their knowledge or that when they operate in their own domain of competence everything is smooth and unproblematic. On the contrary: In our research, we found operators had to have access to *multiple performance modes* if they were to be reliable. They continually face situations with varying degrees of unpredictability and/or uncontrollability (they can predict the weather but can't control it when it goes bad). Furthermore, those situations are faced with varying resources and options with which to respond.

Sometimes the volatility (unpredictability and/or uncontrollability) they face is high or it is low, while the options they have with which to face that volatility can be many or few. Behavior that is "just-in-case" (having lots of options even when volatility is low) doesn't work when operators have to be creative "just-in-time" (that is, when system volatility suddenly increases because of, say, bad

[15] E. Rosenthal, "Our fix-it faith," New York Times Week in Review (2010): WK 1.

weather). To be reliable is to provide safe and continuous services even as (especially when) conditions become more unpredictable or uncontrollable, while options grow fewer.

We found that the worst situation for control operators to be in is a prolonged state of "just-for-now" performance where volatility is high and options are now very few. Here doing something to make one thing better can make another worse off. In these situations, operators are constantly resorting to quick fixes and band-aids to hold things together in contrast to those situations of "just-in-time" performance, where their multiple options and skills enable them to assemble and improvise strategies to ensure reliability when conditions temporarily turn bad.

From what we have read, the Deepwater Horizon drilling control operators (and their Houston counterparts) were having to operate increasingly outside known patterns and scenarios, well into their precursor zone (if not beyond into experimenting with unknown unknowns), and in part due to prolonged conditions of having to perform "just-for-now" with recourse to only last-ditch measures in the days and hours leading up to the Spill.

And last-ditch they were. "Jimmy Harrell, Transocean's top rig manager, [said]: 'Guess that's what we have those pinchers for' as he left the meeting, having reluctantly agreed to follow BP's instructions" on April 20th, where Harrell, Transocean's offshore installation manager, appears to have been "referring to the shear rams on the blow-out preventer, which were designed to cut off the flow of oil and gas in the case of emergency." [16] The driller on the rig's tower is said to have added, "We'll work this out later;" only by that point there was no more later to work it out and no viable shear rams able to do that work.[17]

Finally, control operators we have observed operate within formal and informal *bandwidths* for their real-time operations. These bandwidths, which have been determined or settled on beforehand, tend to be ranges, limits, or tolerances within which operators drive or navigate the system. In order to keep the system reliable, they may have to breach the bandwidth bounds if they are experiencing a situation not encountered before.

However, the longer they breach the bandwidths or the more often they have to do so or the more those "bandwidths" are not based in actual experience and practice, the more unreliable control operations become. The existence of informal bandwidths derived from control operator experience is especially important, since they supplement what exists in formal manuals and procedures[18, 19]

For example, an expedited process for the Minerals Management Service to approve permit requests looks to be an ideal formal procedure, if viewed on its own. However, when BP's rushed request of April 15th to revise its drilling plan is approved within 10 minutes of submission to MMS,

[16] Kirchgaessner, op. cit.

[17] Michael Williams Testimony, "FUSCG/BOEM Marine Board of Investigation into the Marine Casualty, Explosion, Fire, Pollution, and Sinking of Mobile Offshore Drilling Unit Deepwater Horizon, with Loss of Life in the Gulf of Mexico, 21-22 April 2010," (July 23, 2010), 5-241. See http://www.wadisasternews.com/external/content/document/3043/856507/1/7-23-10.pdf and http://www.c-spanvideo.org/program/294728-1.

[18] For the debate between Transocean and BP over who was following what with respect to the rig's formal emergency manual on April 20th, see Gold and Chazan.

[19] R. Gold and G. Chazan, "BP tries to shift blame to Transocean," Wall Street Journal, May 22-23, 2010, A4.

the request falls considerably outside the range of MMS or BP experience. What is striking to us is the degree to which the regulators involved had themselves been caught up in the "just-for-now" behavior on the rig in its last weeks.[20]

It is against this HRM backdrop and interpretation of the Spill that the following series of questions and implications take on research importance.

3.0 First-Order Questions

First, we have to understand the rate of system change and complexity in control room operations.

If the preceding section is correct, then a fuller account of the Spill requires a more detailed description of "normal control operations" on the Deepwater Horizon rig. As others in the Deepwater Horizon Study Group have pointed out,[21] the rig was operated safely for years with some level of competence. We also need to know when control operators themselves felt things were going wrong over the course of the rig's operation, i.e., "We're outside our comfort zone right now." All this would be helped by assembling existing, real-time indicators of when operators were being pushed to their performance edges and into their precursor zone.[22, 23]

To start we would need to know what were the specific real-time reliability requirements in the drilling and rig control units and how were they monitored.

Clearly one requirement was that downward pressure exerted by the mud and other means from the top of the well pipe had to balance the upward pressure exerted by gas and other elements from its bottom. "You don't want to push too hard, but you don't want to push too easy. There's—a delicate balance that has to be maintained at all times. . . . The bottom line is. . . it's all about pressure in a well. That's all it's about. You have to balance the pressures between the seabed and the bottom of the well. And it's not unusual to have problems down below with pressure. That's why have all of the sophisticated instrumentation?" reports an informed crewmember on the Deepwater Horizon.[24] But just what did that instrumentation show and in what form and for how long?

The indicators would have to be more than those events described in media reports by way of confrontations and short-cuts driving operations during the rig's last days. We are talking about a great deal more than a record of what happened in the 50 minutes prior to the blowout when there were overt signs something was wrong.

---

[20] Of course, the classic charge is that regulators and industry are always in a cozy relationship, so we should expect such "expediting" to the mutual benefit of each. That may be true, but *in this case* the charge may well miss the important point. The hurried approval of the April 15th permit scarcely did any favors for BP or for the Service when it came to ensuring drilling reliability or their own organizational survival. In HRM terms, the regulators and BP were both caught up in a string of just-for-now quick fixes, band-aids, and last-ditch interventions that took on a life of their own.

[21] e.g., Peter Marshall, personal communication.

[22] For one example of indicators focusing on reliability violations, see Roe and Schulman.

[23] E. Roe, op. cit.

[24] Michael Williams, op. cit.

We would need to know much more about the crew rotations (how long on the rig, how long off), since first days back for control operators can pose considerable skill issues. So too we would need to know more about the on-rig shifts (e.g., Did different shifts have different personalities? What was the turnover or downsizing on any given shift? What was the mood?[25, 26] etc). We would need to know more about the support staff for control operators (e.g., Were off-site Houston engineers supporting on-rig operators or directing them? Where support staff contracted in as vendors, and, if so, with what effect? Etc.). What was being monitored and what should have been monitored, but wasn't? Finally, we would have to have a much better idea of what the operators themselves saw as their major performance edges, namely, those tasks or activities which challenged them regularly or periodically.

With a more detailed control operations description in hand, we'd be positioned to illustrate the relevance, if any, of the three possibilities mentioned earlier. If the operators concerned were actually having to operate in their precursor zone or beyond for prolonged periods of time, that means that a major disaster could have happened at any time during that period. For all we know, a major failure could have happened with an earlier loss of well control and not just the one on the day of the Spill.[27, 28, 29]

Remember, the risk of operating in the precursor zone is that those managing there do not know or understand all the cause and effect that matter. What works by way of helping matters within their domain of competence could end up making matters altogether worse when undertaken in the precursor zone. That the worse didn't happen with an earlier loss of well control could scarcely have been reassuring to the operators: Failing to fail is not what control rooms mean by reliability.

Moreover—and this point is major—control and support operators on the rig and in Houston may have prevented other major accidents from happening even though the Spill did occur. Operators we observed are sometimes in the position of having to incur a formal reliability violation in order to avoid an even worse reliability lapse; they are forced to make "errors" in order to keep the system reliable. They do this because they are skilled in taking risks to reduce risks. When that works, that is great, and we would need to determine the level of operator and crew competence on the Deepwater Horizon drilling rig in the years and months prior to the Spill to see if such actions were evident.

However, when this risk-taking behavior is transferred from their domain of competence where skills work, into their precursor zone where skills are significantly challenged, it can have disastrous consequences. Operators preventing accidents waiting to happen may find that even worse accidents occur because the earlier ones were prevented in the way they were. Possibly, every day that the Transocean Offshore Installation Manager (OIM) manager and control operators managed the rig

[25] According to one crew member: "Towards the end of the well, right before the explosion, [the mood] was getting worse. We knew we had about two more of these small—supposed 21-day wells to do. And here we are on—six weeks later on a 21-day well. But the biggest—complaint was we were gonna have to go back to where we drilled that 35,000-foot well. And that was an issue, because it was such a long helicopter ride."

[26] Michael Williams, op. cit.

[27] On an earlier loss of well control see Urbina. For the loss of well control on the day of the blowout see the interview transcript with Michael Williams, chief electronics technician on the rig.

[28] I. Urbina, "Documents show earlier fears about safety of offshore well," New York Times, May 30, 2010; 1, 16.

[29] Michael Williams, op. cit.

without major incident turned out to be one more day that corporate BP representatives felt justified in undertaking even more hazardous activities.[30, 31, 32]

4.0 Second-Order Questions

Second, we have to understand the rate of system change and complexity confronting decision-makers outside the control units.

If you argue that the specific mistakes leading up to the April 20th blowout were preventable, then from a HRM perspective you have to be careful in not simply assuming that: (1) preventing those mistakes would have meant no other major incident would have occurred at the rig, or (2) very important mistakes were not being prevented even though the Spill did occur. If you too readily accept (1) and (2) then you risk the tyranny of hindsight that renders the past more linear and inevitable than it actually was. In actuality, there may have been a great deal more contingency, coincidence and luck, good and bad, at work leading up the Spill than hindsight's rapid connecting the dots suggests.

From a control room perspective, it is difficult to see how the major policy implication becomes primarily one of calling for more and better regulation. Such regulation would require not just oversight, but, if we are correct, deep hands-on, continuous site inspection, with recourse to real-time supervisory control to correct observed infractions.

In reality, the President's "we will trust but we will verify" has to be backed up the added qualifier "… and when necessary we will directly manage." But no regulatory cadre exists with such a wide purview and deep knowledge, and those who have it—control room crews and their immediate support staff—can't stop infractions from taking place when senior executives and corporate leaders are determined to trade off system reliability (which may in fact be an essential part of the corporation's own brand!) for short-term windfalls or moving onto their next senior position elsewhere.

These regulatory challenges need careful analysis. But a prior need is to at least identify empirical measures of when control operators move to their performance edges and into their precursor zones. That way, we would be able to see that those movements into the precursor zone constitute substantial proof that "threats to reliability are actually happening, right now, right here." With indicators, we'd also have a chance to see whether new regulations themselves move operators away from the precursor zone as hoped or closer to those performance edges as often inadvertently happens.

[30] According to one report, "the lack of a major catastrophe for many years, even though a rig explosion occurred as recently as a few months ago in the waters off East Timor" has led some expert to conclude that this "success of safety may have set the basis for what happened" in the Deepwater Horizon Spill (Hoyos, Samuelson).

[31] D. Hoyos, "The rig's blow-out preventer holds the key to what went wrong and why," Financial Times, May 7, 2010, 7.

[32] R. Samuelson, "Oil spill reveals dangers of success," Washington Post, June 7, 2010, A17.

5.0 Third-Order Questions

Third, it is important to understand the rates of change and growing complexity in the technical systems themselves that confront decision-makers both inside and outside the control rooms.

For it is change and complexity, we believe, that threaten to overwhelm both groups and challenge the industry safety record as never before.[33, 34] For we argue that increasingly we do not know what the "system" is we are managing until "it" actually fails. Only then do we understand in greater depth what the system is we were meant to be managing reliably but in hindsight weren't.

To see how different this challenge is contrast it with the dominant view about how reliability fails in our large critical infrastructures. In this view, reliability is eroded little by little until disaster occurs. Industry standards are breached, and lo! nothing happens, and then pressure builds to lower standards further and so on, until we find ourselves taking risks that would have been unthinkable a few years before. This is called "the normalization of deviance," [35] a term coined to describe events leading up to the 1986 Challenger Accident, where warnings and concerns about the O-rings were ignored with each successive successful flight…until that 25th flight in the program.

If the problem were movement closer and closer to a performance edge without really knowing just how close to failure you really are, then an obvious solution would be to get back to those types of error-intolerant industry standards that worked so well before standards were eroded. Again, the call for more and better regulation is heard.

But there is a less comforting way to see the Challenger Accident and other more recent large technical system failures. It may be that only after the O-rings failed—instead of all the other things "waiting" to go wrong—that NASA managers were able to really comprehend just what kind of system the Challenger shuttle actually was and the limits it had to operate under. Technical systems are so complex today that they confront their managers with the challenge of not just finding useful information in the midst of all the data available ("information overload"), but also having to know just what information they need but may not recognize when they see it ("cognitive undercomprehension").

This dual challenge is a direct function of system complexity that arises through design and redesign and through workaround on workaround to compensate for inadequate design. In this world, not only do regulators not know what it is that is failing until failure happens, they can't know what the effective resources are with which to respond until that failure makes the real system apparent. We do not know if this dual challenge is underway in the oil and natural gas industry, but we have seen it in the electricity and water infrastructures we have studied.

[33] D. Brooks, "Drilling for certainty," New York Times, May 28, 2010, A23.
[34] R. Samuelson, op. cit.
[35] D. Vaughan, The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA (Chicago: University of Chicago Press, 1996).

6.0 Conclusion And Proposed Research

If we are correct in our argument, then what decision-makers should be doing right now, right this minute, is not only seeking to contain the Deepwater Horizon Spill; they should also be giving *equal attention and care* to ensuring that all those other operating deepwater drilling rigs are being managed by control operators well within their respective domains of competence and nowhere near their precursor zones. We should be most concerned about instances where units have been and are still performing outside their comfort zones without relief in sight. We must wonder if the reorganized Minerals Management Service can meet this priority challenge.

All of above, however, is hypothesis and speculation. While based on theory and prior research findings, it is only a reasonable argument at best and requires confirmation and modification in light of the particulars of control operations behavior on the Deepwater Horizon drilling rig and its Houston counterparts over the years of the rig's operations and not just for the days and hours before the Spill.

Much of this information trail would have to be reconstructed from interviews with former control operators. Such a description need not all be based on existing operator knowledge, though that too would have to be canvassed. In addition, a database of indicators of real-time reliability, such as changes recorded by instrumentation, would be very helpful. In sum, we would propose:

- Review of the growing documentation on the Deepwater Horizon;
- Interview relevant control operators and managers from the rig and support staff in Houston;
- Identify indicators of real-time reliability from control operators and documentation (be they from the Deepwater Horizon's operation or from other deepwater drilling rigs); and
- Assembly of a multi-year database around these indicators and tracking their movements.

Such information will be difficult to retrieve, if only because of legal considerations, but it is perishable in another important sense as well. We know from research that the long- and short-memories of control operators are themselves "perishable," especially under fast-changing conditions of an industry like oil and natural gas. It is important that key informant interviews, however confidential and anonymous they may have to be, start as soon as possible with operators.

Appendix K

Institutional Governance of Offshore Oil and Gas Development

Michael Baram and Florian Buchler

1.0 Background

This paper provides preliminary recommendations regarding the legal and regulatory framework for preventing future major accidents in oil and gas developments on the Outer Continental Shelf (OCS).[1]

The management and regulation of oil and gas development on the OCS is mainly governed by the Outer Continental Shelf Lands Act (OCSLA)[2] and administrated by the Secretary of the Interior through the Bureau of Ocean Energy Management, Regulation, and Enforcement (BOEMRE).[3] In developing offshore oil and gas resources it is the declared Congressional policy that

> *"the Outer Continental Shelf is a vital national resource …which should be made available for expeditious and orderly development …"*[4] *and, in particular, shall be conducted "…subject to environmental safeguards…"*[5] *and "… in a safe manner by well-trained personnel using technology, precautions and techniques sufficient to prevent or minimize the likelihood of blowouts, loss of well control, fires, spillages, physical obstructions to other users of the waters … which may cause damage to the environment or to property, or endanger life or health."*[6]

In addition to OCSLA and its implementing regulations,[7] offshore oil and gas development is further regulated by several other federal and state laws, executive orders, and case law.

Furthermore, a multiplicity of federal and state agencies, as well as private sector classification societies, are implicated in the oversight, regulation, and quality and safety management of the subject activities.

---

[1] Issues relative to the adequacy of the legal and regulatory framework for oil spill response will be addressed in the environmental section.

[2] Outer Continental Shelf Lands Act, Pub. L. 83-212, ch. 345, 67 Stat. 462 (1953), codified at 43 U.S.C. §§ 1331 *et seq.*

[3] Prior to June 18, 2010, the federal agency charged with the administration of OCS mineral development was the U.S. Minerals Management Service (MMS) On June 18, 2010, the Secretary of the Interior issued Order No. 3302 changing the name of the MMS to (BOEMRE). Section 3(c) of the Order provides that BOEMRE shall exercise all authorities previously vested in the MMS. The Secretary of the Interior, U.S. Department of the Interior: Order No. 3302. June 18, 2010. This report will refer to MMS/BOEMRE to capture actions before and after the reorganization.

[4] 43 U.S.C. § 1332(3).

[5] 43 U.S.C. § 1332(3).

[6] 43 U.S.C. § 1332(6).

[7] 30 CFR 250 *et seq.*: Oil and Gas and Sulphur Operations in The Outer Continental Shelf.

In general terms, OCSLA establishes a four-stage process for the development of oil and gas leases:

(i) The development of a Five-Year Plan by MMS/BOEMRE which creates a schedule of proposed lease sales, providing the timing, size, and general location of the leasing activities in the plan area;[8]
(ii) The individual lease sale consultation process, which provides adjacent states and the public an opportunity to review each proposed lease sale. This stage culminates in the competitive bidding process and the sale of a leases;[9]
(iii) Submission to, and approval by MMS/BOEMRE of exploration plans (EPs) that include detailed descriptions of the exploration activities.[10] Once the EP has been approved on the regional level, a further Application for a Permit to Drill (APD) needs to be reviewed and approved on the local level.
(iv) Submission to, and approval by MMS/BOEMRE of development and production plans (DDPs) that include detailed descriptions of the development and production activities.[11] Once the DDP has been approved on the regional level, a further Application for a Permit to Drill (APD) needs to be reviewed and approved on the local level.

OCSLA, the National Environmental Policy Act (NEPA),[12] as well as several environmental statutes[13] require that MMS/BOEMRE consult at different junctions in this four-step process with outside agencies such as the Environmental Protection Agency (EPA), the National Oceanic and Atmospheric Administration (NOAA), the Fish and Wildlife Service (FWS), and the National Marine Fisheries Service (NMFS). Furthermore, consultation with, and approval of proposed actions by affected states is required under the Coastal Zone Management Act (CZMA).[14]

For a number of reasons, the process of interagency consultation has never been cohesively integrated and, as a result, it has never created a true system of checks and balances that could serve to implement the Congressional prerogative to *prevent damage to the environment or property, or endanger life or health* in the development of offshore oil and gas operations.

As such, the Deepwater Horizon accident was a symptomatic result of a governance system that is ill suited to properly consider - and inform the public about - the dynamic and hazardous nature of current and emerging offshore petroleum developments. The analytical work is still in progress, however, some of the key issues have already been identified and are being widely discussed. These include, inter alia:

[8] 43 U.S.C. § 1344.
[9] 43 U.S.C. §§ 1337, 1345.
[10] 43 U.S.C. § 1340(b),(c).
[11] 43 U.S.C. § 1351.
[12] 42 U.S.C. § 4332(2)(C).
[13] Consultations or permits are required under statutes including the Clean Air Act § 328, 42 U.S.C. § 7627 (1990), Clean Water Act § 402, 33 U.S.C. § 1342 (1987), Marine Mammals Protection Act § 104, 16 U.S.C. 1374 (2007), Endangered Species Act § 7, 16 U.S.C. § 1536 (2006), Magnuson Stevens Fishery Conservation and Management Act § 305(b), 16 U.S.C. § 1855 (1976). *See* Freeman, *Structural Options for Improving MMS/BOEM Decision Making on Offshore Drilling,* p. 2. October 13, 2010. Available at: http://www.oilspillcommission.gov/document/jody-freeman-presentation-structural-options-mmsboem.
[14] Coastal Zone Management Act § 307, 16. U.S.C. § 1456 (1988).

- Lack of adequate interagency consultation requirements, or meaningful integration with existing consultation requirements under the National Environmental Policy Act (NEPA), the Coastal Zone Management Act, and other federal laws with respect to the leasing and permitting process;
- Interagency consultation with the relevant outside agencies in most cases does not result in binding mandates for MMS/BOEMRE to implement recommendations of outside agencies in the planning of offshore oil and gas developments;
- The four-stage development process under OCSLA allows for a "tiering" of NEPA analysis that is counterintuitive: the findings in an environmental impact statement (EIS) for a five year plan that covers a large area for lease sales over an extended time period of time can be implemented by reference to subsequent planning steps, a process that has de facto resulted in the routine granting of categorical exclusions for the production of environmental impact statements or environmental assessments (EA) on the micro-level of operations, such as exploration and production plans. In other words, detailed analysis is undertaken on the macro level where specific conditions cannot be anticipated, and on the micro-level, where assessment of specific conditions is necessary, exemptions for detailed analysis are being granted;
- The combined OCSLA-NEPA review process only requires MMS/BOEMRE to fully disclose environmental impacts, but not to alter their plans in light of that disclosure. NEPA itself does not require mitigation even when environmental impacts are expected to be severe, nor does it require MMS/BOEMRE to provide a "worst case" analysis.[15] Worst case planning would have revealed that there currently exist no practical means to intervene with a deep-water well blowout other than the "static kill" option via a relief well.
- Inadequate prescriptive regulatory framework relative to the technical and safety elements for exploration and development;
- Apparent conflict of interest between operator developed (American Petroleum Institute) and regulator adopted (MMS/BOEMRE) standards and safety models;
- Application of an inspection system relying on a limited number of inspections, limited number of inspectors with questionable technical qualifications;
- A regulatory regime in which the regulator bears the burden of proof for proving operator non-compliance.

2.0 Recommendations

Research on governance of complex technical endeavors indicates that inclusion of objective- or performance-based regulations based on research, collaboration and adaptation of industry operating experience can produce superior safety and performance results as compared to an exclusively prescriptive command and control regulatory approach (Carnes DHSG Working Paper). Experience in the U.S. commercial nuclear power industry demonstrates the effectiveness of such a models. Review of regulatory and management approaches in the United Kingdom and Norway

[15] *See* Freeman, *Structural Options for Improving MMS/BOEM Decision Making on Offshore Drilling,* p. 2. October 13, 2010. Available at: http://www.oilspillcommission.gov/document/jody-freeman-presentation-structural-options-mmsboem.

offshore petroleum industries find that a number of objective- or performance-based approaches are in use, or in various stages of development in successful offshore petroleum operations.

However, very recent experience and analysis of the blowout of the Montara Wellhead Platform in Australia indicates that while objective-based regulation has been a desirable development overall, it demands that an active regulatory agency exists that is able to properly validate the elements of an objective-based regulatory approach.

a. General Elements

Recommended core elements gleaned from the nuclear industry, the commercial aviation industry, and high performing petroleum industry for error prevention and management programs designed to reduce, minimize, and ultimately eliminate human factors in accidents include the following elements:

- Progressive and adaptive key regulatory institution that is directly and adequately funded by the royalties obtained from the subject activities, *i.e.* monetary needs of the key regulatory agency need to be satisfied first from offshore oil and gas royalties; (caveat…this can lead to agency prioritization of production over safety, as has been claimed about FDA fast-track drug approval process which is paid for by the pharmaceutical industry).
- Adoption of a systems safety model clearly establishing that system safety is necessary to prevent major accidents; additionally, worker protection models are essential and should be mandatory to calibrate system safety models from a 'real life' perspective;
- Development of safety cases, including detailed drilling, containment, and spill response plans;
- Risk-informed regulation: a combination of traditional engineering requirements for technical systems and components informed by probabilistic risk assessment to focus on safety critical systems and components, combined with performance regulations for management and organizational systems and processes;
- Intense training and qualification programs for operating personnel and inspectors;
- Operating experience monitoring together with onsite inspectors and promotion of organizational learning from anomalies, near misses and accidents;
- Meaningful integration of key regulatory agency with other relevant technical, environmental, and responsive agencies;
- An independent organization, jointly established by government and industry, to perform research and evaluation relative to drilling and production operations, such as the formation of an Offshore Institute, as proposed by Secretary Salazar,
- The establishment of independent operating and training standards to promote excellence;
- An industry-funded accident insurance pool that is dedicated specifically to disaster prevention and response;
- Sufficient funding for research on petroleum industry operation and management excellence;
- Research and investment in developing new safer and cheaper technologies.
- Safety equipment standardization and qualification.

- Industry-wide emergency response capability.

- Industry-wide reporting system with "whistle blower" protection.

b. Specific Recommendations

In addition to these more generalized elements, the following more particular recommendations with respect to the development of the legal and regulatory framework are made:

- Development of an integrated regulatory system under OCSLA and relevant environmental laws that creates real leverage for outside agency recommendations, *i.e.* recommendations that need to be addressed or even implemented by BOEMRE.
- Existing consultation requirements between BOEMRE as the action agency and outside agencies need to be reviewed. Since outside agencies, much like BOEMRE itself, often lack the financial capabilities to properly comment on the environmental impacts of proposed activities, independent third party institutions can be tasked with performing analysis, and this analysis should be paid for by either the lead agency or the industry that is seeking permits. (caveat about industry paying certifiers. In the financial services debacle, the point has been made that credit-rating org's favored companies because of the prospect of service contracts & therefore were not robustly objective in their ratings)
- Compliance by BOEMRE and permit applicants pursuant to the National Environmental Policy Act must be based on context-specific and activity-specific information (not boilerplate). Ultra-Deepwater drilling activities need to be distinguished from shallow water drilling activities, other offshore development activities, and proposed development activities in the arctic, all of which pose different reasonably foreseeable impacts of routine operations, accidents and other non-routine incidents on the human and natural environments. Unless the technology differences that apply to operations in these differing environments are not clearly understood and described, meaningful environmental impact statements pursuant to NEPA cannot be formulated.
- As long as impacts of activities on the human and natural environments remain unknown, e.g. the use of dispersants, the magic 'disappearance' of large amounts of oil, or the effects of deep-water methane hydrates on aquatic life, the utilization of "Findings of no Significant Impact" (FONSI) or "Categorical Exclusions" (Cat-Ex) for activities should be minimized.
- Development and implementation of "worst case" analysis for activities that have high impact implications (human, environmental, financial). Worst-case analysis needs to reflect the latest standard of technical expertise and the plausible concerns of others whose interests may be impacted (*i.e.* 'stakeholders'). In order for not having to 're-legislate' NEPA, a process must be devised under the enabling legislations, most notably the Outer Continental Shelf Lands Act and the Oil Pollution Act, to formulate and enforce plausible worst case scenarios, and to determine whether drilling permits will be granted with special conditions for minimizing the likelihood of the worst case and for minimizing its impacts if it does occur.
- Finally, a comprehensive review of the Coastal Zone Management Act (CZMA) and its implementing regulations should be initiated to realize the Congressional intent of a

system of checks and balances between the federal government and state governments in reviewing the direct, indirect, and cumulative effects of oil and gas development activities on the Outer Continental Shelf on coastal resources, and their consistency with a state's Coastal Management Plan, as envisioned by the CZMA and the Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101-508, 104 Stat. 1388, Title VI (1990). In this context, the idea of regional planning councils should be further developed to allow the local communities to effectively participate in the development and management of coastal resources.

- Since NEPA is a 'procedural' statute only, a review of the Outer Continental Shelf Lands Act and its implementing regulations is necessary to identify the different operating scenarios (deep-water, shallow-water, and arctic), and to formulate typical technical regulations (*i.e.* standards for pipes, cementing, centralizers, blow-out preventers) for different operations. Typical technical regulations will enable the NEPA review to properly correlate activities with reasonably foreseeable impacts.
- Jurisdiction and responsibilities must be clarified to resolve current uncertainties regarding the regulatory and inspection roles of the Coast Guard, BOEMRE, OSHA and EPA for offshore operations.[16] In particular, a rule needs to be enacted to clarify and coordinate responsibilities at multi-employer work sites and ensure compliance with applicable regulations and procedures by the party holding the permit and its contractors, subcontractors and service providers.[17] Furthermore, the Crew Resource Management system employed by the commercial aviation industry might be a good example because it recognizes the fact that multiple people (teams) are working together that have NOT been trained as teams, but individually to function as teams.
- Priority should be given to resolving current uncertainties regarding regulatory and inspection roles of BOEMRE and the Coast Guard for worker safety and health,[18] and to enactment of a process safety management standard (which includes provisions for management of change), similar to OSHA's process safety management rule for onshore oil and gas operations.[19]
- In assuming responsibilities for worker safety and health, BOEMRE should enact workplace safety and health regulations that are integrated with its accident prevention requirements, and not assume that accident prevention requirements alone provide sufficient protection for worker safety.[20] In this regard, BOEMRE should require by rule that a worker safety representative be appointed at each installation to participate in operational decisions and be empowered to suspend operations when the representative believes in good faith that continuation of operations would imminently endanger

[16] Numerous Memoranda of agreement and Understanding between these agencies over the years have led to many regulatory uncertainties. M. Baram, *Preventing Accidents in Offshore Oil and Gas Operations: the US Approach and Some Contrasting Features of the Norwegian Approach* (Sept. 2010), http://ssrn.com/abstract=1705812. Also National Academy of Engineering, *Interim Rpt. on Causes of the Deepwater Horizon Oil Rig Blowout and Ways to Prevent Such Events* (Nov. 16, 2010).

[17] In this regard, OSHA Instruction CPL 02-00-124 should be considered.

[18] M. Baram, note 2 supra. Also "Coast Guard Says it Oversees Offshore Oil Rig Safety, Lawmakers Cite Regulatory Disarray", 40 OSHR 537 (June 24, 2010); and Hearings, Committee on Education and Labor.

[19] OSHA standard at 29 CFR 1910.119.

[20] Numerous studies indicate the value of worker involvement in offshore safety management, e.g. P. Bentley et al, Development and Implementation of an HSE Management System in Exploration and Production Companies, Society of Petroleum Engineers (1994).

worker safety. These are key features of proven value in the Norwegian regulatory approach to industrial safety.[21]

- BOEMRE should maintain oversight of the contracts between the permit holder and its contractors and other service providers to ensure that any fee incentives based on reduced time and costs of performance do not compromise the professional quality of the contracted work in ways that would undermine operational safety.[22]
- BOEMRE should secure the cooperation of OMB/OIRA in ensuring that enactment of new regulations it finds necessary for accident prevention are not obstructed by unduly stringent application of cost-benefit analysis.[23]
- BOEMRE should establish an advisory committee on safety culture to give meaning to this concept and provide guidance for its establishment and maintenance within offshore industries. The concept has been loosely used in a judgmental way to summarize why a company experienced an accident. But the safety culture concept has not been clearly defined, nor its ingredients identified, other than that it involves, for example, organizational learning from accidents and near miss incidents, more than regulatory compliance, internal reporting and lively discourse on safety matters, ethics in decision-making, and leadership which promotes continuous improvement. An interdisciplinary advisory committee could advance the concept and provide guidelines for its implementation and measurement, as is being done in other industrial sectors.[24]
- Repeal of the $75 million liability cap for economic damages under the Oil Pollution Act. If operations can yield $10 million per day, a maximum penalty of $75 million is negligible from an operator's perspective and, accordingly, does not provide the necessary deterrent function of a penalty, even for the "worst case."

c. Safety and Environmental Management System (SEMS)

BOEMRE's new SEMS rule marks the first time that a federal agency will directly regulate the structure and core functions of the safety management system of an offshore operator. The SEMS rule mandates operator fulfillment of eleven broadly stated safety management functions (and compliance with other requirements for self-auditing, documentation, and reporting).[25] The rule also explicitly provides that compliance with the functional requirements will involve operator implementation of standards and practices developed by the American Petroleum Institute and other industrial organizations, and for enforcement when operators do not fulfill the designated functions.

This new approach raises several issues that need to be addressed by BOEMRE (Baram DHSG Working Paper):[26]

---

[21] S. Martorell et al, Stop in the Name of Safety-The Right of the Safety Representative to Halt Dangerous Work. In *Safety, Reliability and Risk Analysis* (2009).

[22] For an approach used in the realm of federal contracts, see DFARS 216.405-270: Award fee reduction or denial for jeopardizing the health or safety of Government personnel, at http://www.acq.osd.mil/dpap/dars/dfars/html/current/216_4.htm#216.405-270

[23] A. Sinden, OMB Regulatory Hit List, Ctr. For Progressive Regulation. http://www.progressivereform.org/perspOMB.cfm

[24] M.Baram, M. Schoebel, Safety Culture and Behavioral Change at the Workplace, 45 Safety Science 631-636 (2007).

[25] Safety and Environmental Management Systems: Final Rule, 75 Fed. Reg. 199 (Oct. 15, 2010) 63610. et seq.

[26] M. Baram, Self Regulation and Safety Management, Working on Safety Conference (Sept. 7, 2010). http://www.wos2010.no/presentations.php

- Given that each company's fulfillment of the functional, performance-based requirements will be based in part on consideration of the special features of its operation and thus differ in several respects from what each other company does for compliance, BOEMRE needs to ensure that each company's compliance with SEMS affords equivalent protection for workers and the environment.
- Because the current checklist approach to inspection which involves policing companies for PINC's (potential incidents of non-compliance) by relatively inexperienced inspectors was developed for ensuring compliance with prescriptive technical standards and rules,[27] it is inadequate for evaluating compliance with the broadly-stated functional requirements of the SEMS rule. Therefore, BOEMRE needs to ensure that inspection pursuant to the SEMS rule is conducted by highly qualified personnel who are capable of fully evaluating company efforts to meet the performance-based functional requirements, and capable of offering regulatory guidance when necessary.[28]
- BOEMRE must also ensure that the American Petroleum Institute and other industrial safety standards and recommended practices relied upon by companies for compliance with the SEMS rule are qualitatively sufficient in terms of the technical state of the art, and are not compromised by the economic interests and lobbying activities of the membership of the industrial standard-setting organizations.[29] Because the procedures used by such organizations for developing industrial standards and recommended practices are not transparent nor permit access by non-industrial stakeholders, BOEMRE should also conduct transparent "regulatory forums" in which existing industrial standards and the need for additional industrial standards pertinent to the SEMS rule are discussed with participation by non-industrial stakeholders.[30]

[27] PINC's at http://www.boemre.gov/regcompliance/inspect.htm

[28] M. Baram, *Preventing Accidents in Offshore Oil and Gas Operations: the US Approach and Some Contrasting Features of the Norwegian Approach* (Sept. 2010)). http://ssrn.com/abstract=1705812

[29] M. Baram, Id. Also NAE Rpt., note 3 supra.

[30] The Norwegian model for regulatory forums is instructive. See http://www.ptil.no/regulatory-forum/category168.html