Risk Management in the Oil and Gas Industry
Testimony: Senate Committee on Energy and Natural Resources

Prof. Nancy G. Leveson
Aeronautics and Astronautics Dept.
MIT
May 17, 2011

I thank you for inviting me here today to speak on risk management in the offshore oil and gas industry. To provide some background, I have been practicing, teaching, and doing research in system safety engineering for over 30 years. Although I am a professor of aerospace engineering, I have experience in almost all industries including aerospace, defense, transportation (automobiles, trains, air traffic control), oil and gas, chemicals, nuclear power, medical devices, and healthcare. I have been involved in the investigation of many major accidents, most recently I was on the Baker Panel investigation of the BP safety culture after the 2005 Texas City Oil Refinery explosion and a consultant to both the Columbia Accident Investigation Board and the Presidential Oil Spill Commission. I am also a co-owner of a 20-year old company that provides safety engineering services.

System safety engineering (which should not be confused with occupational safety) has been in existence as a system engineering discipline for at least 50 years. In the process industry, this engineering discipline is called process safety engineering. Much is known about how to engineer and operate safer systems and to manage safety risks successfully. The low accident rates in industries that apply these principles, such as commercial aviation, nuclear power, and defense systems, is a testament to their effectiveness. The recent accidents and subsequent investigations in the offshore oil industry makes it clear that at least some players in this industry are not using basic and appropriate safety engineering technologies and practices.

Commercial aviation is an example of an industry that decided early that safety paid. After World War II, Boeing wanted to create a commercial airline industry but, because of the high accident rate (there were 18 airplane crashes in 1955 despite a relatively small number of flights), only 20 percent of the public was willing to fly. Today the commercial aircraft accident rate is astoundingly low, particularly considering that there are about 10 million commercial airplane flights per year in the U.S. and over 18 million world-wide. In 2010, for example, U.S. Air Carriers flew 17.5 million miles with only one major accident.

Another surprisingly safe industry is defense. We have never, for example, accidentally detonated a nuclear weapon in the 60 years they have been in existence. The nuclear Navy, which prior to 1963 suffered the loss of a submarine on average every two to three years, instituted a wildly successful safety program (called SUBSAFE) after the loss of the Thresher nuclear submarine in 1963. No U.S. submarine has been lost in the 48 years since that program was created. Nuclear power in the U.S., after the wakeup call of Three Mile Island, has also had an extremely successful safety record.

These success stories show that even inherently very dangerous technologies can be designed, operated, and managed in ways that result in very low accident rates. Accidents are not inevitable nor are they the price of productivity. Risk can be managed successfully without reducing profits long-term, but some effort must be expended to do so. We know how to do this and the costs are surprisingly low when done right.

Common Factors in Major Accidents

Major accidents share some common factors:

- *Flaws in the safety culture* of the organization and sometimes the whole industry: Organizational culture is the set of shared values and norms upon which decisions are based. Safety culture is simply that subset of the overall culture that reflects the general attitude and approaches to safety and risk management. Safety culture is primarily set by the leaders of the organization as they establish the basic values upon which

decisions will be based. Some common types of dysfunctional safety cultures can be identified. For example, Hopkins coined the term *Culture of Denial* to describe industries or organizations where risk assessment is unrealistic and credible warnings are dismissed without appropriate actions. In a culture of denial, accidents are assumed to be inevitable. Management only wants to hear good news and may ensure that is what they hear in subtle or not so subtle ways. Often arguments are made in these industries that the conditions are inherently more dangerous than others and therefore little can be done about improving safety or that accidents are the price of productivity and cannot be eliminated. Many of these features of a culture of denial are displayed by at least some companies engaged in off-shore oil drilling. The president of the American Petroleum Institute, for example, was quoted as saying after both the Washington State Tesoro Oil Refinery explosion and after Deepwater Horizon that the oil and gas industry is just more risky than others. Note, however, that there is nothing very safe about flying in a metal tube 30,000 feet in the air in an unsurvivable outside environment and kept aloft by two engines or being a mile below the surface of the ocean in a submarine with a nuclear power plant. Yet these very dangerous industries are able to operate with very few or no accidents.

A second type of dysfunctional safety culture might be termed a *Paperwork Culture*, where employees spend all their time writing elaborate arguments that the system is safe but little time actually doing the things necessary to make it so. After the U.K. Nimrod aircraft loss in Afghanistan in 2006, the accident report cited the use of safety cases as a major contributor to the accident and noted the use of such cases had created a "culture of paper safety" at the expense of real safety [Haddon-Cave, 2009].

- *Lack of real commitment to safety by leaders:* Management commitment to safety has been found to be the most important factor in distinguishing between organizations with high and low accident rates [Leveson, 1995].
- *Nonexistent or not followed management of change procedures*: A large percentage of major accidents occur after some change in the system or in the way it is operated. While most companies have management of change procedures on their books, these procedures are not always followed.
- *Inadequate hazard analysis and design for safety***:** Instead of putting the emphasis on designing safety into the system from the beginning, the major emphasis is instead placed on recovery from adverse events or investigating them after they occur.
- *Flawed communication and reporting systems:* In a surprisingly large number of accidents, unsafe conditions were detected prior to the actual loss events or precursor events occurred but were not adequately reported or investigated so that the loss event could be prevented.
- *Inadequate learning from prior events:* Prior incidents and accidents are very often only superficially investigated. The symptoms of the underlying systemic causes of the accident or incident are identified as the cause of the events but not the underlying flawed processes or culture that led to those symptoms. This behavior leads to a sophisticated game of "whack-a-mole" where changes are frequently made but accidents continue to occur. Such organizations are in continual fire-fighting mode after multiple accidents caused by the same underlying causes. In the "whack-a-mole" safety culture, accident investigation usually focuses on operator error or on technical failures and ignores management and systemic factors.

Human error is a symptom of a safety problem, not a cause. All behavior is influenced by the context or system in which it occurs. Reducing operator error requires looking at such things as the design of the equipment, the usefulness of the operating procedures provided, and the existence of goal conflicts and production pressures [Dekker, 2006]. Telling people not to make mistakes, firing operators who make them, or trying to train people not to make mistakes that arise from the design of the system is futile. Human error can be thought of as a symptom of a system that needs to be redesigned. In addition, technical failures also need to be investigated for the flaws in the process that allowed them to be introduced and not to be identified during reviews and testing.

A basic flaw in accident and incident investigation is the search for a *root* cause. Finding one or two so-called root causes of an accident provides management with the illusion of control, a phenomenon John Carroll labeled "root cause seduction." Accidents are complex processes and oversimplifying causation leads to future accidents caused by those problems that were never identified or fixed after the previous losses.

Sometimes important causes of accidents are identified or problems detected during performance audits, but the information is never effectively used to redesign the social and physical components of the system. Why was the safety control structure (see below) ineffective in preventing the loss events? How can it be strengthened? A program of continual safety improvement needs to be created.

Two additional common factors in accidents are primarily found only in the process (chemical, oil, and gas) industry:

- *Confusion between occupational and system safety*: Most industries separate these very different problems. Occupational safety focuses on controlling injuries to employees at work by changing individual behavior. System safety puts an emphasis on designing the system, including the engineered and operational components, to prevent hazardous system states and thus losses. Confusion between these two very different problems and solutions can lead to overemphasis on only one type of safety, usually occupational or personal safety, while thinking that the other types of accidents or losses will also be prevented—which they will not. Because personal safety metrics (such as days away from work) can more easily be defined and collected than process or system safety metrics, management is fooled into thinking system safety is improving when it is not and may even be deteriorating.
- *Belief that process accidents are low probability*: Referring to accidents as "low-probability, high consequence" events is rampant and unique to this industry. The implication is that accidents are low probability no matter how the system is designed or operated. Labeling is used to prove that accidents are rare. While process accidents may be low frequency, they are not necessarily low probability. The number of reported oil spills in the Gulf of Mexico alone cited in the Presidential Oil Spill Commission report between 2006 and 2009 was 79, not a low number considering that translates to 6 oil spills a year or one every two months in a relatively small part of the industry and other unreported smaller spills may have also occurred. The fact that the consequences of the events may differ often depends on factors in the environment over which the engineers and operators have no control and are often a matter of luck. The way that the Macondo well was designed and operated made an accident quite high probability. It was not a low probability event. This mislabeling leads to the belief that nothing can be done about such events nor does anything in particular need to be done to reduce their probability—they are by definition already low probability.

Safety as a Control Problem

Traditionally, safety has been considered to be a system component failure problem. Preventing accidents then simply requires making each individual component very reliable. This approach, however, oversimplifies the accident process and cannot prevent accidents created by interactions among components that have not failed. A new, systems approach to accidents instead considers safety to be a control problem [Leveson, 2011]. In this conception, accidents result from a lack of enforcement of constraints on safe behavior. For example, the O-ring did not control the release of propellant gas by sealing the gap in the field joint of the *Challenger* Space Shuttle. The design and operation of Deepwater Horizon did not adequately control the release of hydrocarbons (high-pressure gas) from the Macondo well. The financial system did not adequately control the use of dangerous financial instruments in our recent financial crisis.

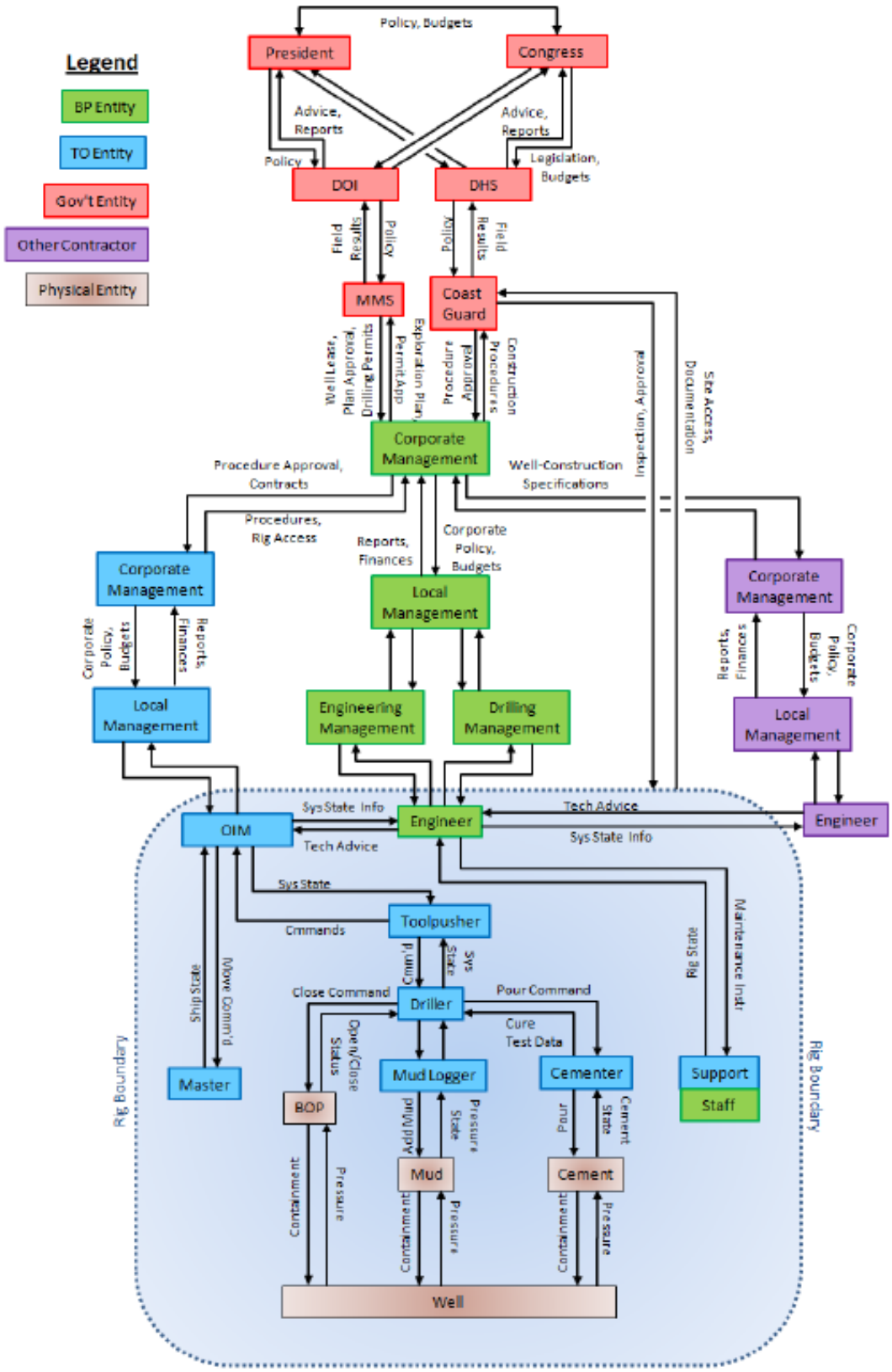

Figure 1: The Operational Safety Control Structure for the Macondo Well

Behavioral safety constraints are enforced by the safety control structure of the organization or industry. Figure 1 shows the control structure for operations at the Macondo well in particular and offshore oil drilling in general. The system-level hazard is uncontrolled methane gas surging up the well. Similar control structures, not shown, exist for engineering development and licensing of the well equipment and for emergency response

Each of the components in this structure plays different roles and has different responsibilities for ensuring safe behavior of the physical process and the organizational components of the structure. Between components there are feedback control loops where control actions are used to achieve the system and component goals (see Figure 2). Feedback provides information about how successful the control actions have been. For example, the cementer pours cement and receives feedback about how the process is proceeding.

Decisions about providing control actions is partly based on a model the controller has of the controlled process. Every controller must contain a model of the process it is controlling. For human controllers, this model is usually called a mental model. Accidents often result from the process models being inconsistent with the actual state of the process. For example, managers use occupational safety data to make decisions about the state of process safety or an engineering manager believes the cementing process was effective and provides a command to remove the mud.

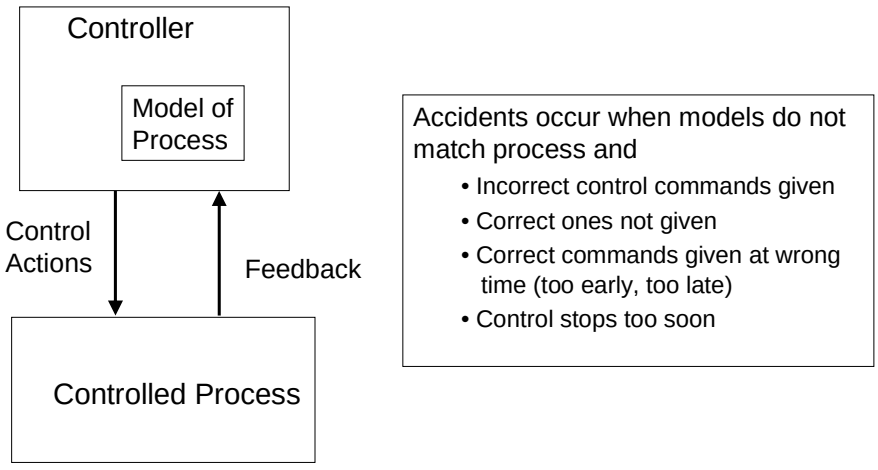

Figure 2: The General Form for a Control Loop in the Safety Control Structure

Control decisions are also influenced by the social and environmental context in which the controller operates. To understand individual behavior requires understanding the pressures and influences of the environment in which that behavior occurs as well as the model of the process that was used.

Losses occur when this control structure does not enforce appropriate behavioral safety constraints to prevent the hazard. In Figure 1, there are physical controls on the well such as the blowout preventer, mud, and cement. Each of the other components of the safety control structure has assigned responsibilities related to the overall system hazard and controls they can exercise to implement those responsibilities. These controls may involve physical design, technical processes, social (cultural, regulatory, industry, company) processes, or individual self interest. For example, part of the responsibility of the MMS was to approve plans and issue drilling permits. Partial control over the safety of operations in the GOM could, at least theoretically, be implemented by appropriate use of the approval and permitting processes.

Determining why an accident occurred requires understanding what role each part of the safety control structure played in the events. Accidents can result from poor design of the control structure, individual components not implementing their responsibilities (which may involve

oversight of the behavior of other components), communication flaws, conflicts between multiple controllers controlling the same component, systemic environmental factors influencing the behavior of the individual components, etc. Major accidents, such as the Deepwater Horizon explosion and oil spill, usually result from flawed behavior of most of the system components.

Preventing accidents requires designing an effective safety control structure that eliminates or reduces such adverse events.

An important consideration in preventing accidents is that the control structure itself and the individual behavior of the components is very likely to change over time, often in ways that weaken the safety controls. For example, a common occurrence is for people to assume that risk is decreasing after a period of time in which nothing unsafe occurs. As a result, they may change their behavior to respond to other conflicting goals. Migration toward states of higher risk may also occur due to financial and competitive pressures. Controls must be established to prevent or at least to detect when such migration has occurred.

There is not just one correct or best safety control structure. Responsibilities may be assigned to different components depending on the culture of the industry, history, or even politics. It is important to note that all responsibility for safety should not necessarily rest in the government or a regulatory authority. Because the lower levels of the structure can more directly impact the behavior of the controlled process, it is much more effective for primary safety responsibility to be assigned to the companies with the regulatory authorities providing oversight to ensure that the proper safety practices are being used. In some industries, however, the companies are unable or unwilling to shoulder the bulk of the safety control responsibilities and the regulatory authorities must provide more control.

The safety control structure as defined here is often called the safety management system.

Establishing Controls to Prevent Future Oil Spills

Given this system and control view of safety, we can identify the flaws in the safety control structure that allowed the Deepwater Horizon accident to occur and what can be done to strengthen the overall offshore oil and gas industry safety control structure. Many of the recommendations below appear in the Presidential Oil Spill Commission report, which is not surprising as I played a role in writing it, particularly Chapter 8. The general key to preventing such occurrences in the future is to provide better information for decision making, not just for the government regulators but for those operating the oil rigs.

There are many changes that would be useful in strengthening the safety control structure and preventing future oil spills. Focus should not just be on BOEMRE but on all the components of the control structure. Some general recommendations follow.

- *Providing appropriate incentives to change the safety culture*: Participants in industries like commercial aviation understand the direct relationship between safety and their profits and future viability. The relationship is not so clear in the off-shore oil industry. The moratorium on GOM drilling was a very strong signal to the industry that those companies with strong safety cultures and practices can be hurt by those without them and that they need to participate in industry initiatives for self-policing and cooperation in improving safety. There also need to be incentives to update safety technology. The standard BOP design was less effective as exploration moved into deeper water and other technology changes occurred, but the industry ignored the many previous BOP failures and insisted that the design could not be improved. A similar example occurred with the Refrigerator Safety Act of 1956, which was passed because children were being trapped and suffocated while playing in unused refrigerators. Manufacturers insisted that they could not afford to design safer latches, but when forced to do so, they substituted magnetic latches for the old mechanical latches. The magnetic latches permit the door to be opened from the inside without major effort. The new latches not only eliminate the hazard, but are cheaper and more reliable than the older type [Martin and Schinzinger, 1989]. A similar example occurred when an improved BOP was designed quickly after the Macondo well blowout. BOEMRE needs to keep on top of needed technical incentives as oil exploration and extraction conditions change and ensure that incentives exist to update safety technology that has become less effective.
- *Industry standards*: One of the surprises that emerged in the investigation of the accident was the lack of standards in the industry, for example standards for cementing operations. Even

weak guidelines, like API Recommended Practice 75 (Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities), have been unable to get consensus. Having the API lead standards efforts may be a mistake. In commercial aviation, an independent group called the RTCA performs this role. RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions. RTCA acts as the honest broker and has been very effective in producing strong aviation industry standards.

- *Industry self-policing*: Any government regulatory agency is limited in what it can accomplish. After Three Mile Island, the nuclear power industry created an industry organization, called INPO, to provide shared oversight of safety in nuclear power plants. INPO is described in the Presidential Oil Spill Commission report and recommended as a model for the oil and gas industry to help ensure that the best technologies and practices are used. The tie of INPO reviews to insurance coverage adds extra incentive.
- *Safety management systems*: The industry safety control structure in Figure 1 is an example of a safety management system at the industry level. Safety management systems (safety control structures) also exist within each company although some are not well designed. For example, one of the findings of the Baker Panel was that the BP safety management system for oil refineries needed improvement. The FAA has recently decided that more responsibility for safety needs to be assumed by the airlines and others in the industry and is requiring safety management systems in the companies for which they provide oversight. Safety management systems are also being created for internal FAA activities, such as air traffic control. The Presidential Oil Spill Commission Report recommended that SEMS (Safety and Environment Management Systems) be required by BOEMRE as a prerequisite for issuing licenses and permits for exploration and drilling activities.
- *Integration of safety engineers into operational decision making*: One of the surprises to me personally in the Deepwater Horizon investigations was the lack of any operational safety group advising the decision makers on the platforms. If such a group existed, it did not play an important enough role to be mentioned in the description of the events that occurred. Industries with strong safety programs include a person or group that is responsible for advising management at all levels of the organization on both long-term decisions during engineering design and development of new platforms and on the safety implications of decisions during operations. In most other industries, a safety engineer would have been resident on the platform and involved in all the real time safety-related decision making. This change needs to be put in place by any companies that do not already have such a process safety engineering group.
- *Certification and training*: Another lesson learned from the investigation of the Deepwater Horizon accident is that some workers have minimal training and little certification is required. The changes needed here are obvious.
- *Learning from events*. A systems approach to accident and incident investigation needs to be implemented by everyone in the industry in order to improve the learning and continual improvement process [Leveson, 2011].
- *Hazard analysis*: While the process industry has a very powerful hazard analysis technique, called HAZOP, the use of this technique is not as prevalent as it should be. The results from HAZOP need to be used to improve technological design and also passed to operations to guide maintenance and performance audits.
- *Maintenance*: For the Macondo well, maintenance of safety-critical equipment, for example on the BOP, was not performed as required for safety and as specified in the equipment standards. Regulatory agencies can only spot-check compliance. Ensuring that proper maintenance activities are performed is an important activity for the company Safety Management System.

- *Third Party Certification*: Oversight of complex activities is difficult for any regulatory agency. The Designated Engineering Representative (DER) model used by the FAA may be appropriate for BOEMRE. The FAA cannot possibly provide detailed oversight of the design and manufacturing of all the millions of parts on a commercial aircraft. The problem is solved by the use of DERs, who may be independent experts or may actually work for the company in which oversight is being applied. DERs exist for individual technical engineering specialties, such as propulsion, structures, for general system engineering, and for manufacturing. The DER works under the oversight of an FAA employee and has the power to approve technical data and activities in companies. Various types of mechanisms are used to ensure that DERs are technically well-qualified and execute their responsibilities with appropriate care, diligence, and independence from conflicts of interest. The details of how this program works are beyond the scope of this testimony, but the DER program could provide a model for devising something similar for BOEMRE.
- *Management of change*: As noted earlier, accidents often occur after changes. Any change that has safety implications should be carefully evaluated, including performing a hazard analysis, before it is allowed. Most companies have policies for management of change, but the implementation and enforcement of these policies can vary greatly. One of the unique aspects of the off-shore oil and gas industry is the need for changes to procedures quickly based on information uncovered about the particular geological conditions encountered. It may be impractical for BOEMRE to approve all these changes in a timely enough manner. The importance of the safety engineering function within the companies enters here. BP used a decision tree to make real-time decisions about activities on the platform. Such decision trees can and should be analyzed prior to use for the safety of each of the branches. In addition, the consultation with a safety engineering expert during operations can also improve decisions about required changes, which is another reason why a strong process safety engineering group needs to be tightly integrated into operations and operational decision making.

There is one recommendation in the Presidential Oil Spill Commission report about which I have some reservations and that is the use of safety cases. While what is in a safety case will determine its efficacy, the common definition of a safety case as an argument for why the system will be safe has some serious drawbacks. There is surprisingly little evidence for the efficacy of the safety case approach to regulation. In fact, the use of safety cases has been highlighted in accident reports as a major causal factor, most notably the Nimrod accident mentioned earlier. A major problem with safety cases is what psychologists call “confirmation bias.” In simple terms, people look for evidence that supports the goal they are trying to achieve. So when making a safety case, focus is on evidence that supports that goal and the safety of the system. People do not usually look for evidence that contradicts the goal and often ignore such contradictory evidence when it presents itself. A paperwork, compliance-oriented culture can be created where safety efforts focus on proving the system is safe rather then designing it to be safe. Safety must be designed into a system from the beginning, it cannot be argued in after the fact.

References:

Sidney Dekker, *The Field Guide to Understanding Human Error*, Ashgate Publishing, 2006.

Charles Haddon-Cave, *The Nimrod Review*, HC 1025, London: The Stationery Office Limited, Oct. 28, 2009.

Nancy Leveson, Safeware, Addison-Wesley Publishers, 1995.

Nancy Leveson, Engineering a Safer World, MIT Press, to appear fall 2011. In the meantime, a final draft can be downloaded from http://sunnyday.mit.edu/safer-world.

Mike Martin and Roland Schinzinger, *Ethics in Engineering*, McGraw-Hill Book Company, 1989.