MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

Decision Support for Dynamic Barrier Management for Offshore Operations

William R. Nelson†, Amar Ahluwalia, and Mia Matuszak
DNV GL
1400 Ravello Dr.
Katy, Texas 77449

†Presenter E-mail: bill.nelson@dnvgl.com

Abstract

Effective safety barrier management is a fundamental principle for prevention and mitigation of major accidents in offshore drilling and production operations. Barrier management methods such as bow tie diagrams are commonly used for identifying safety barriers in the development of safety case documentation and the performance of major accident risk assessments. In addition to such applications for establishing design baselines for offshore installations, some organizations are taking safety barrier management into the operational regime by establishing measures for assessing barrier health and assigning barrier owners to ensure that barriers are continuously maintained. The next step in effective safety barrier management is to develop and implement methods to continuously monitor barriers in real time and provide decision guidance for operations, maintenance, and management personnel regarding actions to be taken when barriers are degraded or failed. A systematic approach has been developed by DNV GL for identifying information requirements for dynamic barrier management, instrumentation or other sources of data for providing that information, decision criteria for determining when barriers are degraded or failed, and guidance for actions to be taken to restore degraded barriers and to prevent major accidents and mitigate their consequences. The resulting information framework can be used to support communication, consensus, decision making and action across technical disciplines and organizational boundaries. This paper summarizes the approach for the development of decision support tools for dynamic barrier management, and insights gained from application of the approach to offshore production and drilling operations with multiple industry partners. In addition, the paper summarizes industry research and development activities that are needed for effective implementation of dynamic barrier management in the offshore oil and gas industry.

Background and Need

Assessment of the occurrence and recurrence of catastrophic accidents such as Three Mile Island, Columbia, Macondo, Fukushima, and major pipeline leak accidents has indicated a number of shortcomings of current risk management approaches. First, in all these cases important safety barriers were missing, degraded, or failed, allowing the initiating event to progress to a major accident with catastrophic consequences. In all these industries the need to establish and maintain effective barriers is well recognized, but in each case the critical barriers failed in some way.

The second common element is that human decision making was not adequate to recognize the inadequacy of the critical barriers and to formulate effective corrective actions in time to prevent the accident or mitigate its consequences. In some cases the most obvious decision making errors occurred during the event itself:

- The Three Miles Island operators did not recognize that the primary coolant boundary had been breached and turned off the critical Emergency Core Cooling System.
- The Columbia mission managers did not recognize that the wing leading edge had been breached by the foam impact, even though NASA engineers deep within the organization were analyzing that very scenario.
- The personnel aboard the Deepwater Horizon drilling rig did not recognize the symptoms of a flowing well and take action in time to activate the blowout preventer (BOP) to prevent the blowout, fire, loss of the rig, 11 fatalities, and a major oil spill.
- Numerous major pipeline leak accidents have occurred because control center operators did not recognize the symptoms of a leak, delaying the response to isolate the leak and resulting in major spills and environmental damages.

An interesting variation of barrier management decision making during the course of a major accident is the Fukushima nuclear power plant accident, where once the critical emergency electrical power supplies were engulfed by the tsunami, plant operators worked heroically in an effort restore and maintain the critical barriers for preventing the release of radioactive materials into the sea and the atmosphere.

As tempting as it is, each of these types of “industry defining” catastrophic events cannot be completely described by focusing on decision making failures of the operating personnel during the “heat of the moment.” In all cases, there were major shortcomings that occurred earlier in the project lifetime that “set the stage” for the barrier failures and decision making errors that occurred during the events.

- The designers of the Three Mile Island nuclear plant did not provide instrumentation to conclusively indicate the position of the pilot operated relief valve or the level of liquid water in the pressurizer. In addition, they did not provide adequate training and analysis tools to ensure that control room operators could clearly differentiate between liquid water and steam in the pressurizer.
- Designers and mission management for the Columbia space shuttle did not provide adequate imaging systems and analysis tools to conclusively determine whether the Thermal Protection System of the wing’s leading edge had been breached.

- The Deepwater Horizon blowout preventer was not designed to shear drill pipe that moved to an off-center position in the ram cavity.
- Designers of the Fukushima nuclear plant did not design the location and protection of the emergency electrical power supplies to account for the effects of historically recorded tsunami events.
- Pipeline operating companies did not provide procedures with clear guidance and decision criteria for recognizing symptoms of a leak and taking prompt action to isolate the leak before the occurrence of a major spill.

Regardless of whether the critical decision making errors occur before or during the event that leads to a major accident, the common thread of all these events is that management personnel, engineers, and/or operators made incorrect or inadequate decisions regarding the design, maintenance, activation, or operation of critical safety barriers. One possible contributing factor is that operations personnel and management may have a false sense of security and reduced vigilance because of their belief that robust barriers have been established, when in reality missing or degraded barriers could fail to prevent the progression of an accident when required. This observation leads to the conclusion that it is not only essential to design effective barriers, but effective decision support must be provided to ensure that barriers are continuously monitored, accurate decision criteria are establish to identify when a barrier is degraded, and prompt and effective corrective action can be taken when required to prevent or mitigate the occurrence of a major accident.

As can be seen from the conclusions reached in multiple incident reports for major accidents, it is also tempting to place the primary blame for catastrophic accidents on a poor safety culture. Major efforts and resources have been devoted to measure and improve safety culture; yet major accidents continue to happen within the same organization, as evidenced by the occurrence of the Challenger and Columbia space shuttle accidents only 17 years apart.

The authors believe that the critical element that is missing to effectively manage offshore risks is to provide effective decision support for dynamic barrier management, so that all personnel have the information and tools they need to make effective risk informed decisions.

Dynamic Barrier Management Concept

Figure 1 shows the basic concepts for dynamic barrier management. During the design of an offshore process or installation, barriers are established to prevent the occurrence of threats from leading to a major accident. These barriers are included in the design baseline for regulatory approval and operation of the installation, and establish the baseline level of risk. However, if barriers are not continuously monitored and maintained over time, the barriers can degrade or fail, leading to an increased level of risk. This can be very dangerous and lead to major accidents if the degradation or failure of the barrier is not detected.

Dynamic barrier management establishes the information structure and processes for continuously monitoring the status of the barriers, detecting when barriers are degraded or failed, and determining what actions should be taken to restore the degraded barriers or add additional barriers if needed. This allows the risk to be reduced back to the baseline level or lower.

Dynamic barrier management can be applied in different ways depending on the timescales over which barriers can degrade, and the type of monitoring or instrumentation that is used to track the barrier status over time. The examples of dynamic barrier management that are described in this paper focus on real-time decision support for components, systems, and barriers that are monitored using active sensors. However, the concepts are equally applicable for other types of barriers that are continuously monitored over time using other methods such as periodic samples or auditing procedures. The systematic information requirements analysis can be used to identify the requirements for barrier monitoring that are needed to support the decisions made by the relevant users.

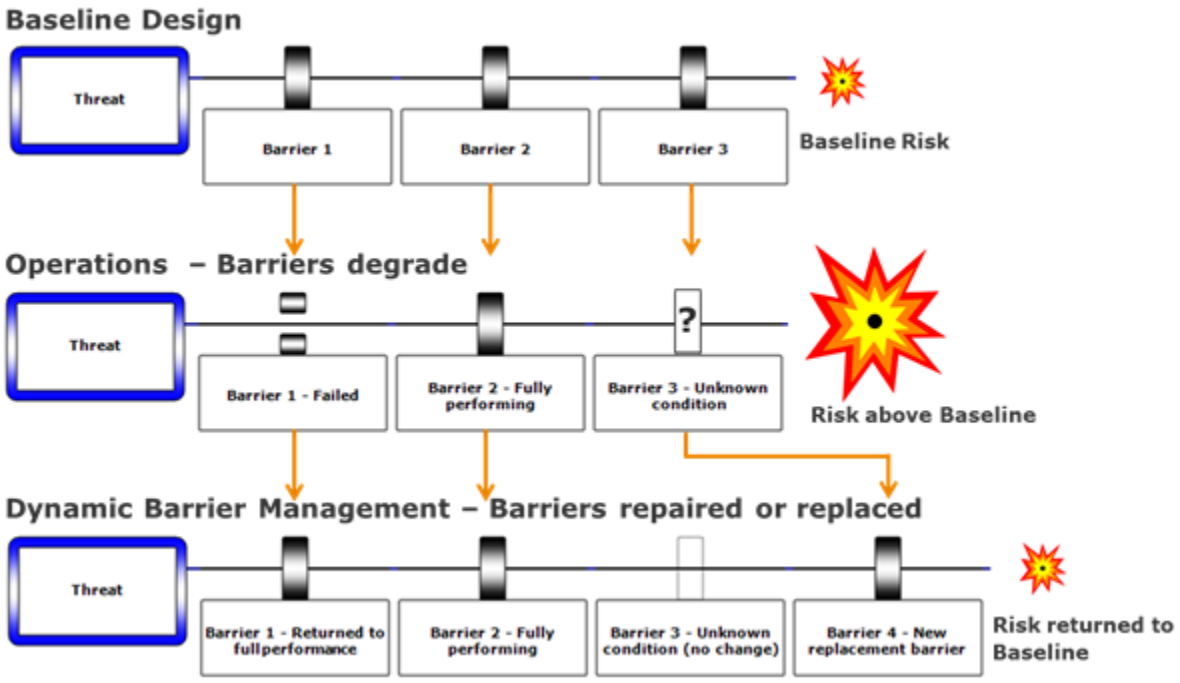

Figure 1. Dynamic barrier management

Decision Support for Dynamic Barrier Management

The DNV GL approach for decision support for dynamic barrier management combines bow tie diagrams from the offshore industry with the success path concept from the nuclear power industry. By combining bow tie diagrams - which provide information about the barriers that can intervene in the progression of an accident, with response trees - which provide information on actions needed to maintain or restore the barriers, a comprehensive, robust approach for dynamic barrier management can be realized.

Bow tie diagrams for barrier management

A bow tie diagram shows the barriers that can be used to prevent a major accident or to mitigate its consequences. Figure 2 shows an example bow tie diagram for deepwater drilling. The orange circle at the center of the diagram is the major accident or "Top Event" that is the focus of the assessment - in this case Loss of Containment for the drilling operation. The blue rectangle on the left is the Threat - i.e. Pressurized Hydrocarbons - that can lead to Loss of Containment. The rectangles between the Threat and the Top event are the barriers that can be used to prevent the Threat from leading to the Top Event - i.e. the Fluid Column, Blowout Preventer (BOP), and the Drilling Riser. Barriers on the left side of the bow tie diagram are referred to as prevention barriers.

Similarly, the red rectangles on the right hand side of the bow tie diagram are Potential Consequences that can result if Loss of Containment occurs. Barriers are shown that can prevent or reduce the magnitude of the consequences. Barriers on the right hand side of the bow tie diagram are called mitigation barriers.

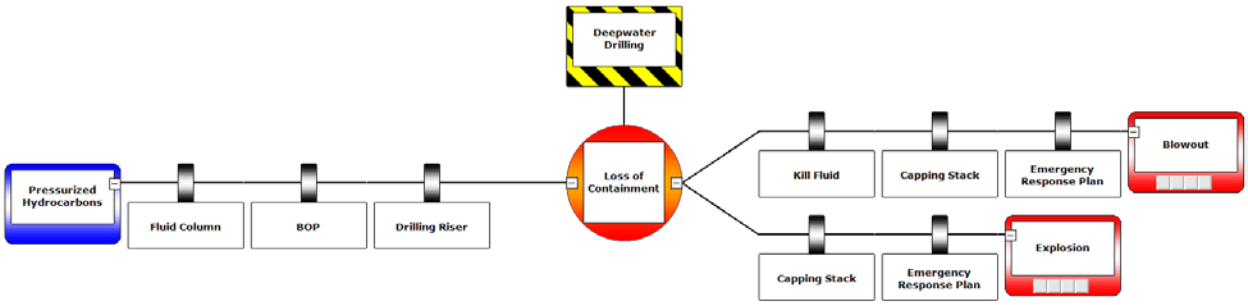

Figure 2. Bow tie diagram for deepwater drilling

Success paths and response trees

A success path is a combination of equipment and processes (e.g. hardware, software, and human actions) that are necessary for a barrier to perform its intended function. The success path and critical safety function concepts were developed in the nuclear power industry following the accident at Three Mile Island in 1979 [1]. A response tree is a graphical representation of the alternative success paths that can be used to maintain or restore a barrier, and provides guidance for selecting the best success path to use when equipment failures degrade the barrier. Response trees were developed at the Department of Energy's Idaho National Engineering Laboratory (INEL) in 1978 for use in the severe accident procedures for a nuclear test reactor [2].

Figure 3 shows a simplified response tree for the BOP barrier for deepwater drilling. Each pathway from the bottom of the tree to the top is a success path for implementing the BOP barrier. In this case, a success path represents a pathway for hydraulic fluid from the source (e.g. surface or subsea accumulators) to flow to the port of a BOP ram in order to close it to maintain well integrity when required by a well kick or other conditions indicating potential well flow.

The response tree is evaluated for failure of the yellow pod and the crossover line between the pods, as indicated by the boxes with the orange color. Because of these failures, the success paths coded with the red color are no longer available for implementing the BOP barrier, while success paths colored green are available. Decision criteria have been established to select the recommended success path that is preferred for this failure scenario, as shown by the boxes colored light blue. This preferred path can be implemented either by manual action or by automated reconfiguration of the BOP control system.

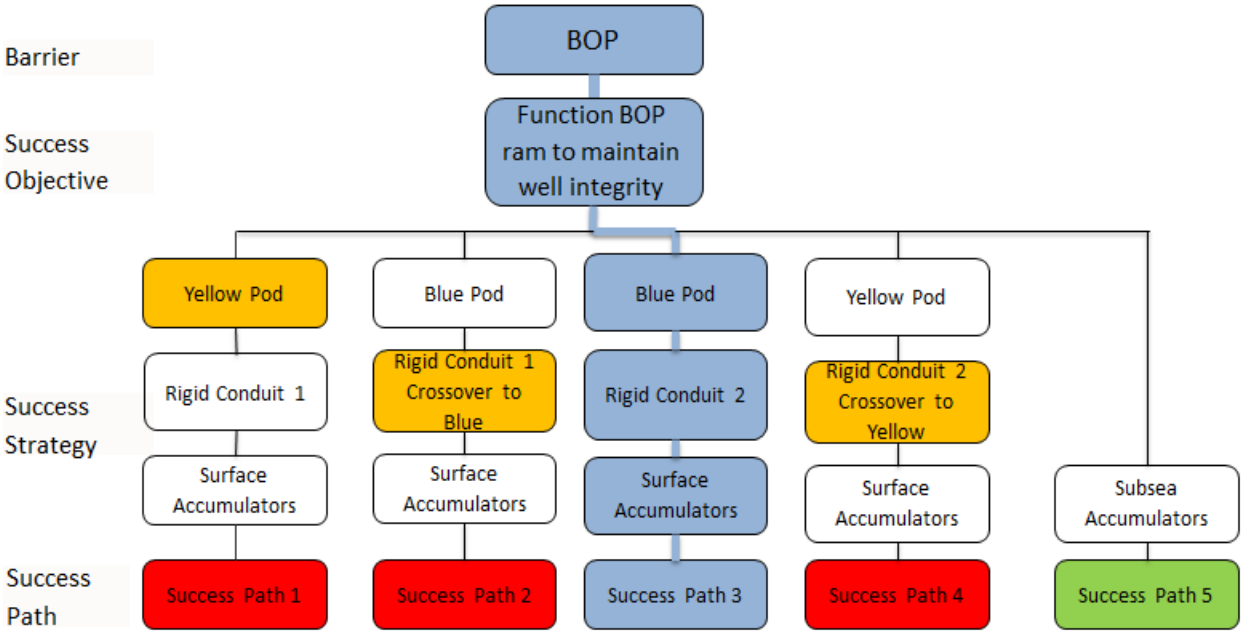

Figure 3. Response tree for the blowout preventer barrier for well integrity

The response tree shown represents a simplified picture of the multiple success paths available for a current two-pod blowout preventer with a crossover pathway. The response tree approach can also be used to explore the potential benefits of alternative designs for BOP control systems, for example by providing additional redundancy or options for reconfiguration.

Figure 4 shows how the response trees and bow tie diagrams are combined to form the framework for decision support for dynamic barrier management. The BOP response tree is continuously monitored to determine the health of the BOP barrier for the Loss of Containment bow tie diagram. If a failure or degraded condition is detected in one of the elements of the BOP response tree, the tree is evaluated to determine which success paths are disabled due to the failure, which paths remain available, and based on the pre-established decision criteria, which success path should be used to reconfigure the BOP control system to restore the BOP barrier. Then the BOP control system is reconfigured to implement this success path, either through manual operator action or automatically using the automated functions of the BOP control system.

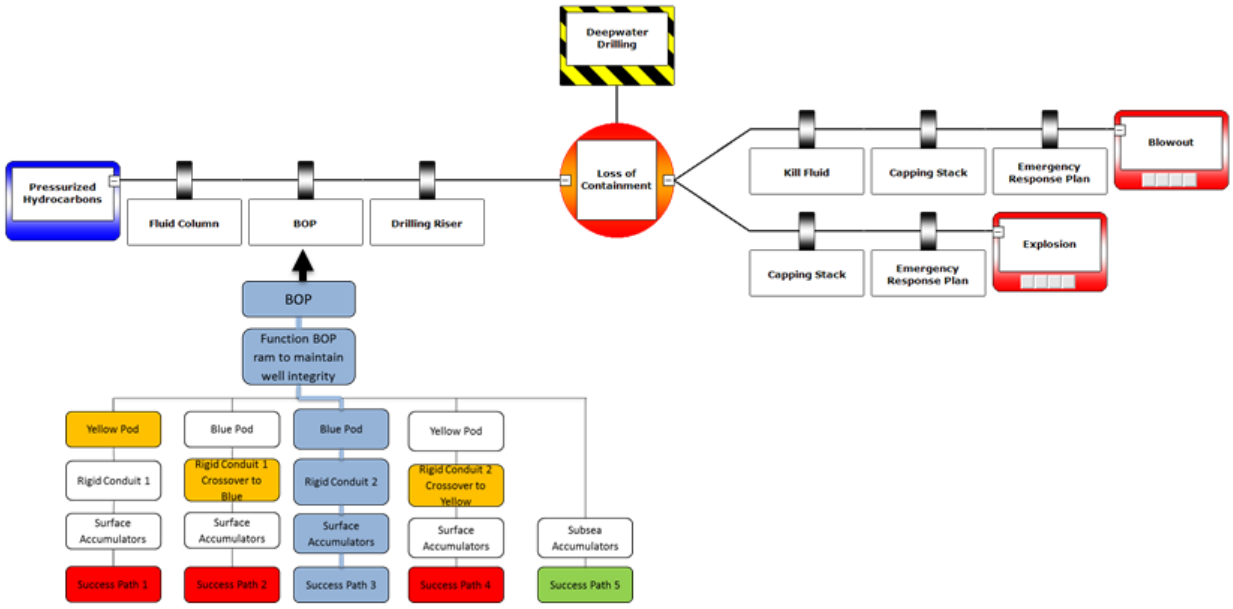

Figure 4. Combining bow tie diagrams and response trees for decision support for dynamic barrier management

Information requirements analysis

Table 1 shows how the information requirements, instrumentation requirements, and decision criteria are established for dynamic barrier management. The first column of the table shows the elements of the bow tie diagram, with the left to right flow of the bow tie diagram represented from the rows moving from the bottom to the top of the table:

- Threat
- Prevention barrier
- Prevention barrier success path
- Top event
- Mitigation barrier
- Mitigation barrier success path
- Consequence

The columns are then systematically filled out in a workshop setting as follows:

- **Information requirement** - The information that is needed to determine the current condition of the Threat, Prevention Barrier, Prevention Barrier Success Path, Top Event, Mitigation Barrier, Mitigation Barrier Success Path, and Consequence.
- **Source of information** - Potential sources of the required information. These sources of information can either be direct information sources (e.g. sensors that directly monitor the parameter) or indirect information sources (e.g. measurements that can be calculated or otherwise inferred from directly monitored parameters).
- **Decision criteria (IF)** - Specific combinations of the parameters that indicate:

- Occurrence or potential future occurrence of the threat
- Degradation or failure of a prevention barrier
- Occurrence or potential future occurrence of the Top Event
- Degradation or failure of a mitigation barrier
- Occurrence or potential future occurrence of the consequence

- **Response guidance (THEN)** - Actions to be taken when the decision criteria are satisfied.

The development of the information in this table forms the foundation for the decision support tool for dynamic barrier management.

Table 1. Framework for Defining Information Needs and Decision Guidance for Dynamic Barrier Management

	Information Requirement	Source of Information	Decision Criteria (IF)	Response Guidance (THEN)
Consequence : Oil Spill	Occurrence of oil spill	Visual observation	Oil on surface confirmed	Implement Emergency Response Plan
Mitigation Barrier Success Path: Inject kill fluid	Initiation criteria for kill fluid injection	- Volume and pressure of kill fluid source - Availability and position of valves in flow path	Uncontrolled well flow	Inject kill fluid
Mitigation Barrier: Kill Fluid	Functionality and Availability of Kill Fluid Flow Paths	- Availability of kill fluid source - Availability and position of valves in flow path	Loss of containment has occurred	Implement kill fluid success path
Top Event: Loss of Containment	Uncontrolled well flow	- Mud pit levels - Wellbore flow conditions	Uncontrolled well flow	- Function BOP ram control flow if possible - Inject kill fluid
Prevention Barrier Success Path: Function BOP ram to shear pipe and close well	Initiation criteria for BOP activation to shear pipe and close well	- Wellbore conditions - Kick margin	Underbalanced fluid column	Function BOP ram to shear pipe and close well
Prevention Barrier: BOP	Availability of hydraulic fluid pathways to function BOP rams	- Volume and pressure of hydraulic fluid source - Availability and position of valves in flow path	Availability of hydraulic fluid pathways does not meet operational and regulatory requirements	- Suspend drilling operations - Maintain BOP control system to restore required capability
Threat: Underbalanced fluid column	Hydrostatic pressure	Comparison of fluid column pressure to formation pressure	Inadequate kick margin	Restore kick margin

Visualization and communication of information for dynamic barrier management

The next step is to develop the displays for the Human Machine Interface (HMI) that will be used to present the information to operators, maintenance personnel, management, and (potentially) regulatory personnel. Figure 5 shows one concept for displaying the information for the loss of containment bow tie diagram. A dynamic well barrier schematic is used to show the current condition of the well control barriers including the BOP and the fluid column. The Compliance Level display shows the current level of compliance with company (e.g. the well control manual) or regulatory requirements, for example the requirement to maintain two barriers at all times during drilling, completion, production, and abandonment operations. The Barrier Status display shows the overall assessment of the current condition of a specific barrier such as the fluid column or the BOP. Finally, the success path status shows the current condition of the success paths for a particular barrier, in this case the fluid column barrier.

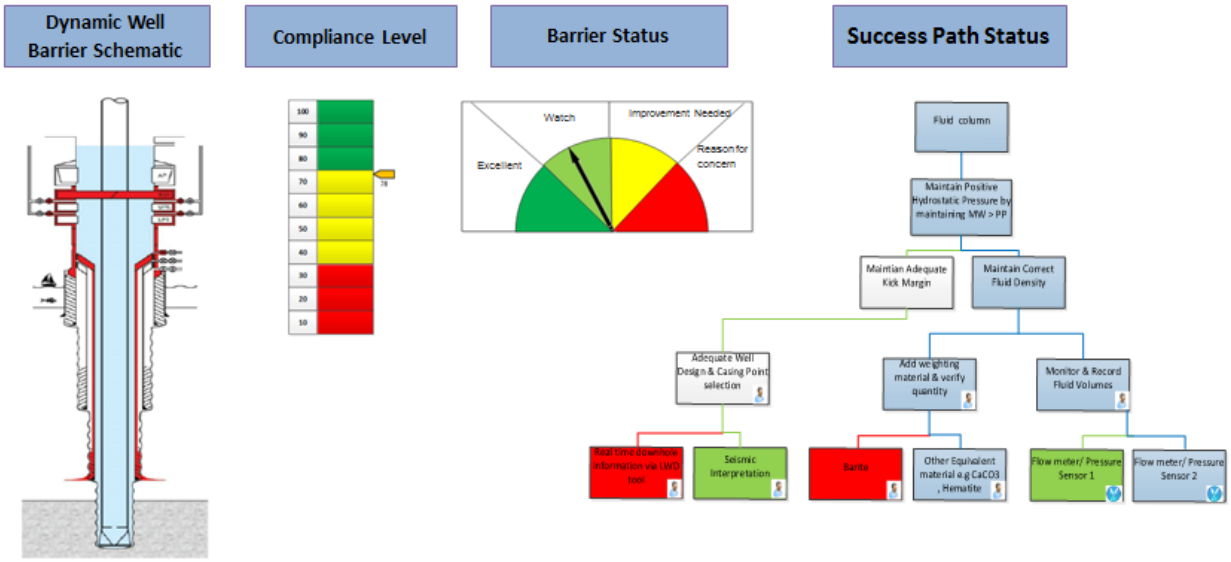

Figure 5. Concept for application of dynamic barrier management to well integrity

Figure 6 shows the overall strategy for dynamic barrier management for a specific process such as well integrity or for an entire installation. Once again, the rows of the table show the elements of the bow tie diagram. The columns of the diagram show the progression of the incident as and the actions to be taken follows:

- **Continuously monitor during standby conditions** - The parameters that should be monitored during normal operating conditions.
- **IF: Degraded barrier conditions are present** - Actions that should be taken if conditions of barrier degradation or failure are detected. If a prevention barrier is degraded or failed a success path should be implemented to restore the prevention barrier. Similarly, if a mitigation barrier is degraded or failed a success path should be implemented to restore the mitigation barrier.
- **IF: Threat conditions are present** - Actions that should be taken if one of the threats is detected or trends indicate that the threat might occur in the future.
- **IF: Top Event conditions are present** - Actions that should be taken if the Top Event is detected or trends indicate that it may occur in the future
- **If Consequence conditions are present** - Actions that should be taken if one of the Consequences is detected or trends indicate that it might occur in the future.

	Standby Conditions		Event Conditions		
Progression of the event → / Elements of the bow tie diagram ↓	Continuously Monitor During Standby Conditions	IF: Degraded Barrier Conditions are Present	IF: Threat Conditions are Present	IF: Top Event Conditions are Present	IF: Consequences Conditions are Present
Consequence	Consequence Precursors				Consequence Assessment and Response
Mitigation Barriers	Mitigation Barrier and Success Path Health	Restore Mitigation Barriers		Assess and Implement Mitigation Barrier Success Paths	
Top Event	Top Event Precursors			Top Event Assessment and Response	
Prevention Barriers	Prevention Barrier and Success Path Health	Restore Prevention Barriers	Assess and Implement Prevention Barrier Success Paths		
Threats	Threat Precursors		Threat Assessment and Response		

Figure 6. Overall strategy for dynamic barrier management

Figure 7 shows the overall long-term vision for dynamic barrier management. We believe that the approach combining bow tie diagrams (representing barriers to intervene in the progression of an event), response trees (to assess the current condition of the barriers), and information requirements analysis (to define the decision criteria and actions to be taken when barriers are degraded or fail), can be applied at all levels within an organization and even across the industry.

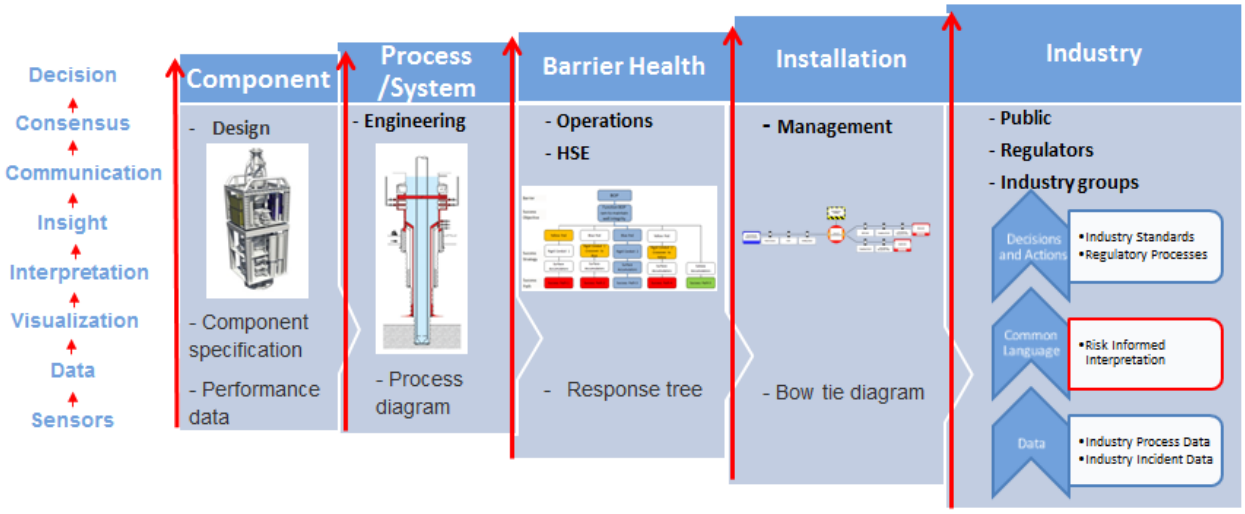

Figure 7. Vision for decision support for dynamic barrier management

The left side of the diagram shows the flow of information that is used in dynamic barrier management:

- **Sensors** - The instruments and other sources of information used to monitor barrier status.
- **Data** - The information that is collected from the instruments.
- **Visualization** - An intuitive representation is used to organize the data and present it to support human decision making.
- **Interpretation** - The process that individual operators or the team use to attach meaning to the information presented on the visualization displays.
- **Insight** - The process to understand how future conditions will be affected if current trends continue or alternative courses of action are taken.
- **Communication** - Sharing of understanding among the members of the team and other stakeholders across disciplines or organizations.
- **Consensus** - Reaching agreement on the assessment of the situation and selection of the best course of action to implement.
- **Decision** - The formal conclusion is formalized and instructions are given for carrying out the prescribed actions and monitoring the outcomes.

As shown in the columns across the diagram, a consistent approach can be applied to support decisions at each level of abstraction:

- **Component** - Enhanced instrumentation and condition based monitoring can be used to monitor the status and health of the critical components that are needed to maintain the barriers. Design personnel are the typical originators and users of information at this level.
- **Process/system** - This level monitors the overall status and health of processes and systems used to maintain or restore barriers. Engineering organizations are the typical users of this information.
- **Barrier health** - This level monitors the current condition of the barriers, determines whether actions are required to maintain or restore the barrier, and selects and implements the selected success path. Operations personnel and health, safety, and environment (HSE) personnel are typical users of the information at this level.
- **Installation** - This level monitors the overall status and health of all the barriers affecting the entire installation and the conduct of the overall mission of the installation, e.g. drilling or production operations. The information generated and applied at this level is similar to major accident risk assessments and safety case information. However, dynamic barrier management makes it possible to continuously monitor barrier conditions at this level rather than limiting barrier management to a static assessment at the design stage with periodic updates during facility life. Management personnel are the typical users of information at this level, and oversee the overall dynamic barrier management process for the installation.
- **Industry** - One of the most promising applications of decision support for dynamic barrier management is for communication across stakeholder groups including industry groups such as the American Petroleum Institute (API) and Ocean Energy Safety Institute (OESI) and regulatory bodies such as the Bureau of Safety and Environmental Enforcement (BSEE). The framework for organizing and visualizing information for dynamic barrier management and the process for making decisions can form a “common language” for communicating information and reaching consensus about required actions. For example, the new well control rule proposed by BSEE will require real time

monitoring of offshore parameters, transmission of the data to an onshore monitoring facility, and sharing the data with BSEE at their request. A common structure or language will be needed to organize this information for sharing in a way that will allow meaningful discussion and common understanding among the stakeholders. We believe that the framework for decision support for dynamic barrier management could be used to form the foundation for such a common language for discussion among industry stakeholders in the application of regulatory process and development of risk-informed industry standards.

Applications of decision support for dynamic barrier management

The DNV GL approach for decision support for dynamic barrier management has been under development for four years in projects assessing safety culture for a nuclear power plant and control room management for two different pipeline companies. In the nuclear power studies the approach was applied to multiple past incidents to determine which barriers had failed and where corrective actions were needed to strengthen existing barriers or add new barriers to prevent the occurrences of similar incidents in the future.

The studies of pipeline control room management were required by regulatory bodies as part of the process for approval for continued operation following the occurrence of major pipeline leak accidents. In both accidents pipeline operators had failed to diagnose the occurrence of the pipeline leaks, and major oil spills occurred before the failed pipeline segments were isolated. The dynamic barrier management approach was used to evaluate the team decision making processes that had led to the failure to diagnose the failure of the pipeline integrity barrier, and the actions that had been taken since the accident to strengthen the existing barriers or add additional barriers. The application of the dynamic barrier management approach in a workshop setting helped the control room management personnel understand how inadequate decision processes led to the failure to diagnose and correct the leaks. In addition, the bow tie diagrams that were annotated to highlight the improvements that had been made since the accident proved to be excellent communication tools to convey the assessment results to the regulatory authorities.

Since these early applications of the dynamic barrier management approach for the assessment of past incidents and accidents, we have extended the focus to the development of real-time decision support tools. The first application was for erosion integrity management for an offshore production facility. We are currently supporting the development of a real-time decision support tool for well integrity barrier management in partnership with a drilling company and an offshore operator. In addition to supporting real time operation, the dynamic barrier management framework for this application will also be used to communicate with regulators for initial approval of the new technology and assessment of operational decisions during drilling activities.

Looking Ahead

Based on the encouraging results that have been experienced in the projects described above, we are currently organizing a Joint Industry Project (JIP) to further develop concepts of decision support for dynamic barrier management. We anticipate that the JIP participants will work together to develop methods, best practices, data sources and pilot-scale decision support systems that can then be adapted for targeted application within their home organizations. This will help the industry move toward the long range vision to apply dynamic barrier management to reduce operational costs, decrease downtime, and increase safety for offshore operations.

Summary and Conclusions

An approach for decision support for dynamic barrier management has been developed that combines proven methods for operational risk management from the offshore industry and nuclear power industry. The combination of bow tie diagrams for barrier management and response trees for selecting success paths to restore degraded barriers provides an effective framework to organize information for managing risks of offshore operations. The systematic approach for information requirements analysis is then applied to identify information needs and develop decision criteria for managing safety barriers throughout the operational life of an offshore process or installation. In the future, the information framework for dynamic barrier management could support the development of a common risk-informed language for communication, consensus, and action among operators, suppliers, industry groups, regulatory bodies, and external stakeholders, allowing them to work together towards the common goal of improved offshore safety.

References

1. W.R. Corcoran, D.J. Finnicum, F.R. Hubbard III, C.R. Musick, and P.F. Walzer, Nuclear Power-Plant Safety Functions, Nuclear Safety, Vol. 22, No. 2, March - April 1981.
2. W. R. Nelson, "Response Trees for Emergency Operator Action at the LOFT Facility, "ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, TN, April 7-11, 1980.